Privacy Act 1988
No. 119, 1988

Compilation No. 78

Compilation date: 1 July 2018
Includes amendments up to: Act No. 25, 2018
Registered: 30 July 2018

Prepared by the Office of Parliamentary Counsel, Canberra
About this compilation

This compilation

This is a compilation of the Privacy Act 1988 that shows the text of the law as amended and in force on 1 July 2018 (the compilation date).

The notes at the end of this compilation (the endnotes) include information about amending laws and the amendment history of provisions of the compiled law.

Uncommenced amendments

The effect of uncommenced amendments is not shown in the text of the compiled law. Any uncommenced amendments affecting the law are accessible on the Legislation Register (www.legislation.gov.au). The details of amendments made up to, but not commenced at, the compilation date are underlined in the endnotes. For more information on any uncommenced amendments, see the series page on the Legislation Register for the compiled law.

Application, saving and transitional provisions for provisions and amendments

If the operation of a provision or amendment of the compiled law is affected by an application, saving or transitional provision that is not included in this compilation, details are included in the endnotes.

Editorial changes

For more information about any editorial changes made in this compilation, see the endnotes.

Modifications

If the compiled law is modified by another law, the compiled law operates as modified but the modification does not amend the text of the law. Accordingly, this compilation does not show the text of the compiled law as modified. For more information on any modifications, see the series page on the Legislation Register for the compiled law.

Self-repealing provisions

If a provision of the compiled law has been repealed in accordance with a provision of the law, details are included in the endnotes.
## Contents

### Part I—Preliminary

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Short title ................................................................. 1</td>
</tr>
<tr>
<td>2</td>
<td>Commencement ............................................................. 1</td>
</tr>
<tr>
<td>2A</td>
<td>Objects of this Act ...................................................... 1</td>
</tr>
<tr>
<td>3</td>
<td>Saving of certain State and Territory laws .......................... 2</td>
</tr>
<tr>
<td>3A</td>
<td>Application of the <em>Criminal Code</em> ................................... 2</td>
</tr>
<tr>
<td>4</td>
<td>Act to bind the Crown .................................................... 3</td>
</tr>
<tr>
<td>5A</td>
<td>Extension to external Territories ..................................... 3</td>
</tr>
<tr>
<td>5B</td>
<td>Extra-territorial operation of Act ..................................... 3</td>
</tr>
</tbody>
</table>

### Part II—Interpretation

#### Division 1—General definitions

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Interpretation ............................................................ 5</td>
</tr>
<tr>
<td>6AA</td>
<td>Meaning of <em>responsible person</em> .................................... 32</td>
</tr>
<tr>
<td>6B</td>
<td>Breach of an Australian Privacy Principle .......................... 33</td>
</tr>
<tr>
<td>6B</td>
<td>Breach of a registered APP code ...................................... 34</td>
</tr>
<tr>
<td>6BA</td>
<td>Breach of the registered CR code .................................... 35</td>
</tr>
<tr>
<td>6C</td>
<td>Organisations ............................................................. 36</td>
</tr>
<tr>
<td>6D</td>
<td>Small business and small business operators ..................... 38</td>
</tr>
<tr>
<td>6DA</td>
<td>What is the <em>annual turnover</em> of a business? ....................... 41</td>
</tr>
<tr>
<td>6E</td>
<td>Small business operator treated as organisation .................. 42</td>
</tr>
<tr>
<td>6EA</td>
<td>Small business operators choosing to be treated as organisations .................................................. 44</td>
</tr>
<tr>
<td>6F</td>
<td>State instrumentalities etc. treated as organisations ........... 45</td>
</tr>
<tr>
<td>6FA</td>
<td>Meaning of <em>health information</em> ..................................... 46</td>
</tr>
<tr>
<td>6FB</td>
<td>Meaning of <em>health service</em> ........................................... 46</td>
</tr>
</tbody>
</table>

#### Division 2—Key definitions relating to credit reporting

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6G</td>
<td>Meaning of <em>credit provider</em> .......................................... 48</td>
</tr>
<tr>
<td>6H</td>
<td>Agents of credit providers ............................................. 49</td>
</tr>
<tr>
<td>6J</td>
<td>Securitisation arrangements etc. ..................................... 50</td>
</tr>
<tr>
<td>6K</td>
<td>Acquisition of the rights of a credit provider .................... 51</td>
</tr>
</tbody>
</table>

#### Subdivision B—Other definitions

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6L</td>
<td>Meaning of <em>access seeker</em> .......................................... 52</td>
</tr>
<tr>
<td>6M</td>
<td>Meaning of <em>credit and amount of credit</em> ......................... 52</td>
</tr>
<tr>
<td>6N</td>
<td>Meaning of <em>credit information</em> ..................................... 53</td>
</tr>
</tbody>
</table>
Division 3—Other matters

7 Acts and practices of agencies, organisations etc. ........................... 61
7A Acts of certain agencies treated as acts of organisation ............... 64
7B Exempt acts and exempt practices of organisations ................... 64
7C Political acts and practices are exempt ....................................... 66
8 Acts and practices of, and disclosure of information to, staff of agency, organisation etc. .................................................. 68
10 Agencies that are taken to hold a record .................................. 70
11 File number recipients ............................................................. 71
12A Act not to apply in relation to State banking or insurance within that State ................................................................. 72
12B Severability—additional effect of this Act ................................ 72

Part III—Information privacy

Division 1—Interferences with privacy

13 Interferences with privacy .......................................................... 75
13B Related bodies corporate ......................................................... 77
13C Change in partnership because of change in partners ............... 78
13D Overseas act required by foreign law ..................................... 79
13E Effect of sections 13B, 13C and 13D ....................................... 79
13F Act or practice not covered by section 13 is not an interference with privacy .......................................................... 79
13G Serious and repeated interferences with privacy ..................... 79

Division 2—Australian Privacy Principles

14 Australian Privacy Principles ...................................................... 80
15 APP entities must comply with Australian Privacy Principles .......... 80
16 Personal, family or household affairs ....................................... 80
16A Permitted general situations in relation to the collection, use or disclosure of personal information ........................................ 80
16B Permitted health situations in relation to the collection, use or disclosure of health information ...................................... 83
Part IIA—Credit reporting

Division 1—Introduction

Guide to this Part

Division 2—Credit reporting bodies

Subdivision A—Introduction and application of this Division etc.

Guide to this Division

Subdivision B—Consideration of information privacy

Open and transparent management of credit reporting information

Subdivision C—Collection of credit information

Collection of solicited credit information

Subdivision D—Dealing with credit reporting information etc.

Use or disclosure of credit reporting information

Permitted CRB disclosures in relation to individuals

Use or disclosure of credit reporting information for the purposes of direct marketing

Use or disclosure of pre-screening assessments

DeSTRUCTION OF pre-screenING assesseMent

No use or disclosure of credit reporting information during a ban period

Adoption of government related identifiers

Use or disclosure of credit reporting information that is de-identified

Subdivision E—Integrity of credit reporting information

Quality of credit reporting information

False or misleading credit reporting information

Security of credit reporting information

Subdivision F—Access to, and correction of, information

Access to credit reporting information
Subdivision G—Dealing with credit reporting information after the retention period ends etc.

20S Correction of credit reporting information .............................................. 107
20T Individual may request the correction of credit information etc. .................. 108
20U Notice of correction etc. must be given .................................................... 109

Division 3—Credit providers

Subdivision A—Introduction and application of this Division

21 Guide to this Division .............................................................................. 120
21A Application of this Division to credit providers ...................................... 120

Subdivision B—Consideration of information privacy

21B Open and transparent management of credit information etc. .............. 121

Subdivision C—Dealing with credit information

21C Additional notification requirements for the collection of personal information etc. ............................................................... 123
21D Disclosure of credit information to a credit reporting body ..................... 124
21E Payment information must be disclosed to a credit reporting body .......... 126
21F Limitation on the disclosure of credit information during a ban period ......... 126

Subdivision D—Dealing with credit eligibility information etc.

21G Use or disclosure of credit eligibility information .................................... 127
21H Permitted CP uses in relation to individuals ......................................... 129
21J Permitted CP disclosures between credit providers .................................. 131
21K Permitted CP disclosures relating to guarantees etc. ................................ 133
21L Permitted CP disclosures to mortgage insurers ...................................... 134
21M Permitted CP disclosures to debt collectors ......................................... 135
21N Permitted CP disclosures to other recipients ....................................... 136
21NA Disclosures to certain persons and bodies that do not have an
Australian link .............................................................................. 137
21P Notification of a refusal of an application for consumer
credit ............................................................................................... 138

Subdivision E—Integrity of credit information and credit
eligibility information

21Q Quality of credit eligibility information ........................................ 139
21R False or misleading credit information or credit eligibility
information ........................................................................................ 140
21S Security of credit eligibility information ......................................... 141

Subdivision F—Access to, and correction of, information

21T Access to credit eligibility information ........................................ 141
21U Correction of credit information or credit eligibility
information ........................................................................................ 143
21V Individual may request the correction of credit information
e tc ................................................................................................. 144
21W Notice of correction etc. must be given ......................................... 146

Division 4—Affected information recipients

22 Guide to this Division .................................................................... 148

Subdivision A—Consideration of information privacy

22A Open and transparent management of regulated information .... 148

Subdivision B—Dealing with regulated information

22B Additional notification requirements for affected information
recipients .......................................................................................... 150
22C Use or disclosure of information by mortgage insurers or
trade insurers ................................................................................ 150
22D Use or disclosure of information by a related body corporate ...... 152
22E Use or disclosure of information by credit managers etc. .......... 153
22F Use or disclosure of information by advisers etc. ....................... 154

Division 5—Complaints

23 Guide to this Division .................................................................... 156
23A Individual may complain about a breach of a provision of
this Part etc. .................................................................................. 156
23B Dealing with complaints ................................................................ 157
23C Notification requirements relating to correction complaints ....... 158

Division 6—Unauthorised obtaining of credit reporting
information etc.

24 Obtaining credit reporting information from a credit
reporting body .................................................................................. 161
24A Obtaining credit eligibility information from a credit provider

Division 7—Court orders
25 Compensation orders
25A Other orders to compensate loss or damage

Part IIIB—Privacy codes
Division 1—Introduction
26 Guide to this Part

Division 2—Registered APP codes
Subdivision A—Compliance with registered APP codes etc.
26A APP entities to comply with binding registered APP codes
26B What is a registered APP code
26C What is an APP code
26D Extension of Act to exempt acts or practices covered by registered APP codes

Subdivision B—Development and registration of APP codes
26E Development of APP codes by APP code developers
26F Application for registration of APP codes
26G Development of APP codes by the Commissioner
26H Commissioner may register APP codes

Subdivision C—Variation and removal of registered APP codes
26J Variation of registered APP codes
26K Removal of registered APP codes

Division 3—Registered CR code
Subdivision A—Compliance with the registered CR code
26L Entities to comply with the registered CR code if bound by the code
26M What is the registered CR code
26N What is a CR code

Subdivision B—Development and registration of CR code
26P Development of CR code by CR code developers
26Q Application for registration of CR code
26R Development of CR code by the Commissioner
26S Commissioner may register CR code

Subdivision C—Variation of the registered CR code
26T Variation of the registered CR code
Division 4—General matters

26U Codes Register.................................................................................. 180
26V Guidelines relating to codes.............................................................. 180
26W Review of operation of registered codes......................................... 181

Part IIIC—Notification of eligible data breaches

Division 1—Introduction

26WA Simplified outline of this Part.......................................................... 182
26WB Entity ............................................................................................. 182
26WC Deemed holding of information...................................................... 182
26WD Exception—notification under the My Health Records Act 2012 .............................................................................. 183

Division 2—Eligible data breach

26WE Eligible data breach ...................................................................... 185
26WF Exception—remedial action ............................................................. 186
26WG Whether access or disclosure would be likely, or would not be likely, to result in serious harm—relevant matters ....................... 189

Division 3—Notification of eligible data breaches

Subdivision A—Suspected eligible data breaches

26WH Assessment of suspected eligible data breach .............................. 191
26WJ Exception—eligible data breaches of other entities ....................... 191

Subdivision B—General notification obligations

26WK Statement about eligible data breach.......................................... 192
26WL Entity must notify eligible data breach........................................... 193
26WM Exception—eligible data breaches of other entities ..................... 194
26WN Exception—enforcement related activities .................................... 194
26WP Exception—inconsistency with secrecy provisions ....................... 195
26WQ Exception—declaration by Commissioner .................................. 196

Subdivision C—Commissioner may direct entity to notify eligible data breach

26WR Commissioner may direct entity to notify eligible data breach .................. 199
26WS Exception—enforcement related activities .................................... 201
26WT Exception—inconsistency with secrecy provisions ....................... 201

Part IV—Functions of the Information Commissioner

Division 2—Functions of Commissioner

27 Functions of the Commissioner......................................................... 203

Privacy Act 1988
28  Guidance related functions of the Commissioner .......................... 204
28A Monitoring related functions of the Commissioner .................... 204
28B Advice related functions of the Commissioner .............................. 206
29  Commissioner must have due regard to the objects of the Act ...... 207

Division 3—Reports by Commissioner ........................................... 208
30  Reports following investigation of act or practice ..................... 208
31  Report following examination of proposed enactment ............... 210
32  Commissioner may report to the Minister if the Commissioner has monitored certain activities etc. ............... 210
33  Exclusion of certain matters from reports ................................. 211

Division 3A—Assessments by, or at the direction of, the Commissioner 213
33C Commissioner may conduct an assessment relating to the Australian Privacy Principles etc. .................. 213
33D Commissioner may direct an agency to give a privacy impact assessment .................................................. 213

Division 3B—Enforceable undertakings ........................................... 215
33E Commissioner may accept undertakings ................................. 215
33F Enforcement of undertakings ..................................................... 215

Division 4—Miscellaneous .............................................................. 217
34  Provisions relating to documents exempt under the Freedom of Information Act 1982 ........................................ 217
35  Direction where refusal or failure to amend exempt document ......................................................... 217
35A Commissioner may recognise external dispute resolution schemes ......................................................... 219

Part V—Investigations etc. .............................................................. 220
Division 1A—Introduction .............................................................. 220
36A Guide to this Part ........................................................................ 220

Division 1—Investigation of complaints and investigations on the Commissioner’s initiative ........................................... 222
36  Complaints ................................................................................ 222
37  Principal executive of agency .................................................... 223
38  Conditions for making a representative complaint .................... 224
38A Commissioner may determine that a complaint is not to continue as a representative complaint .................. 225
38B Additional rules applying to the determination of representative complaints .................................................. 226
38C Amendment of representative complaints ......................................... 226
39 Class member for representative complaint not entitled to
lodge individual complaint ................................................................ 226
40 Investigations .................................................................................. 227
40A Conciliation of complaints ............................................................... 227
41 Commissioner may or must decide not to investigate etc. in
certain circumstances ....................................................................... 228
42 Preliminary inquiries ....................................................................... 230
43 Conduct of investigations .................................................................. 230
43A Interested party may request a hearing ........................................... 232
44 Power to obtain information and documents .................................... 233
45 Power to examine witnesses .............................................................. 234
46 Directions to persons to attend compulsory conference ................. 234
47 Conduct of compulsory conference .................................................. 235
48 Complainant and certain other persons to be informed of
various matters .................................................................................. 236
49 Investigation under section 40 to cease if certain offences
may have been committed ................................................................... 236
49A Investigation under section 40 to cease if civil penalty
 provision under Personal Property Securities Act 2009 may
have been contravened ....................................................................... 238
50 Reference of matters to other authorities ....................................... 239
50A Substitution of respondent to complaint ......................................... 241
51 Effect of investigation by Auditor-General ...................................... 242

Division 2—Determinations following investigation of
complaints .................................................................................................. 243
52 Determination of the Commissioner .................................................. 243
53 Determination must identify the class members who are to
be affected by the determination ......................................................... 245
53A Notice to be given to outsourcing agency ....................................... 246
53B Substituting an agency for a contracted service provider ............... 246

Division 3—Enforcement ........................................................................ 248
54 Application of Division .................................................................... 248
55 Obligations of organisations and small business operators .......... 248
55A Proceedings in the Federal Court or Federal Circuit Court to
enforce a determination .................................................................... 248
55B Evidentiary certificate ..................................................................... 250
Division 4—Review and enforcement of determinations involving Commonwealth agencies 251
57 Application of Division ................................................................. 251
58 Obligations of agencies ............................................................... 251
59 Obligations of principal executive of agency ............................ 251
60 Compensation and expenses ......................................................... 252
62 Enforcement of determination against an agency ....................... 253

Division 5—Miscellaneous 254
63 Legal assistance ............................................................................... 254
64 Commissioner etc. not to be sued ................................................ 255
65 Failure to attend etc. before Commissioner .................................... 255
66 Failure to give information etc. ....................................................... 256
67 Protection from civil actions ............................................................ 259
68 Power to enter premises ................................................................. 259
68A Identity cards .............................................................................. 261
70 Certain documents and information not required to be disclosed .......................................................... 261
70B Application of this Part to former organisations ....................... 263

Part VI—Public interest determinations and temporary public interest determinations 264
Division 1—Public interest determinations 264
71 Interpretation .................................................................................. 264
72 Power to make, and effect of, determinations ................................ 264
73 Application by APP entity ............................................................... 265
74 Publication of application etc. ........................................................ 266
75 Draft determination ......................................................................... 266
76 Conference .................................................................................... 267
77 Conduct of conference ................................................................. 267
78 Determination of application ......................................................... 268
79 Making of determination ............................................................... 268

Division 2—Temporary public interest determinations 269
80A Temporary public interest determinations .................................. 269
80B Effect of temporary public interest determination .................... 269
80D Commissioner may continue to consider application ............... 270

Division 3—Register of determinations 271
80E Register of determinations .......................................................... 271
Part VIA—Dealing with personal information in emergencies and disasters 272

Division 1—Object and interpretation 272

80F Object ........................................................................................................ 272
80G Interpretation .......................................................................................... 272
80H Meaning of permitted purpose .................................................................. 273

Division 2—Declaration of emergency 274

80J Declaration of emergency—events of national significance .................. 274
80K Declaration of emergency—events outside Australia ............................ 274
80L Form of declarations ................................................................................ 275
80M When declarations take effect ................................................................ 275
80N When declarations cease to have effect .................................................. 275

Division 3—Provisions dealing with the use and disclosure of personal information 276

80P Authorisation of collection, use and disclosure of personal information .............................................................. 276

Division 4—Other matters 279

80Q Disclosure of information—offence ..................................................... 279
80R Operation of Part .................................................................................... 280
80S Severability—additional effect of Part ............................................... 280
80T Compensation for acquisition of property—constitutional safety net ........................................................................ 282

Part VIB—Civil penalty orders 283

Division 1—Civil penalty provisions 283

80U Civil penalty provisions ........................................................................... 283
80V Ancillary contravention of civil penalty provisions .................................. 283

Division 2—Obtaining a civil penalty order 284

80W Civil penalty orders .................................................................................. 284
80X Civil enforcement of penalty .................................................................... 285
80Y Conduct contravening more than one civil penalty provision ............... 285
80Z Multiple contraventions ........................................................................... 285
80ZA Proceedings may be heard together ..................................................... 286
80ZB Civil evidence and procedure rules for civil penalty orders ................ 286
80ZC Contravening a civil penalty provision is not an offence ....................... 286

Division 3—Civil proceedings and criminal proceedings 287

80ZD Civil proceedings after criminal proceedings ..................................... 287
80ZE Criminal proceedings during civil proceedings ............... 287
80ZF Criminal proceedings after civil proceedings .................. 287
80ZG Evidence given in proceedings for civil penalty order not admissible in criminal proceedings.......................... 288

Part VII—Privacy Advisory Committee ........................ 289
81 Interpretation ................................................................. 289
82 Establishment and membership ....................................... 289
83 Functions ................................................................. 290
84 Leave of absence .......................................................... 291
85 Removal and resignation of members ............................... 291
86 Disclosure of interests of members ................................. 291
87 Meetings of Advisory Committee ................................. 292
88 Travel allowance .......................................................... 292

Part VIII—Obligations of confidence ................................. 293
89 Obligations of confidence to which Part applies ............... 293
90 Application of Part .......................................................... 293
91 Effect of Part on other laws ............................................. 293
92 Extension of certain obligations of confidence ................. 294
93 Relief for breach etc. of certain obligations of confidence ....... 294
94 Jurisdiction of courts ..................................................... 294

Part IX—Miscellaneous ......................................................... 295
95 Medical research guidelines ........................................... 295
95A Guidelines for Australian Privacy Principles about health information ................................................... 295
95AA Guidelines for Australian Privacy Principles about genetic information ..................................................... 297
95B Requirements for Commonwealth contracts .................. 297
95C Disclosure of certain provisions of Commonwealth contracts .......................................................... 298
96 Review by the Administrative Appeals Tribunal .................. 298
98 Injunctions ................................................................. 299
98A Treatment of partnerships ............................................ 301
98B Treatment of unincorporated associations ...................... 302
98C Treatment of trusts .................................................... 303
99A Conduct of directors, employees and agents .................... 303
100 Regulations ............................................................... 305

Schedule 1—Australian Privacy Principles ......................... 307
Overview of the Australian Privacy Principles ..................... 307
Part 1—Consideration of personal information privacy

1 Australian Privacy Principle 1—open and transparent management of personal information ............................................ 309

2 Australian Privacy Principle 2—anonymity and pseudonymity .............................................................. 310

Part 2—Collection of personal information

3 Australian Privacy Principle 3—collection of solicited personal information ......................................................... 312

4 Australian Privacy Principle 4—dealing with unsolicited personal information ...................................................... 314

5 Australian Privacy Principle 5—notification of the collection of personal information .................................................. 315

Part 3—Dealing with personal information

6 Australian Privacy Principle 6—use or disclosure of personal information .......................................................... 317

7 Australian Privacy Principle 7—direct marketing ...................................................................................... 319

8 Australian Privacy Principle 8—cross-border disclosure of personal information ......................................................... 322

9 Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers ........................................ 324

Part 4—Integrity of personal information

10 Australian Privacy Principle 10—quality of personal information ........................................................................ 326

11 Australian Privacy Principle 11—security of personal information ........................................................................ 326

Part 5—Access to, and correction of, personal information

12 Australian Privacy Principle 12—access to personal information ........................................................................ 327

13 Australian Privacy Principle 13—correction of personal information ........................................................................ 330

Endnotes

Endnote 1—About the endnotes

Endnote 2—Abbreviation key

Endnote 3—Legislation history

Endnote 4—Amendment history

xiii

Privacy Act 1988

Compilation No. 78

Compilation date: 1/7/18

Registered: 30/7/18

Authorised Version C2018C00292 registered 30/07/2018
An Act to make provision to protect the privacy of individuals, and for related purposes

WHEREAS Australia is a party to the International Covenant on Civil and Political Rights, the English text of which is set out in Schedule 2 to the Australian Human Rights Commission Act 1986:

AND WHEREAS, by that Covenant, Australia has undertaken to adopt such legislative measures as may be necessary to give effect to the right of persons not to be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence:

AND WHEREAS Australia is a member of the Organisation for Economic Co-operation and Development:

AND WHEREAS the Council of that Organisation has recommended that member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in Guidelines annexed to the recommendation:

AND WHEREAS Australia has informed that Organisation that it will participate in the recommendation concerning those Guidelines:

BE IT THEREFORE ENACTED by the Queen, and the Senate and the House of Representatives of the Commonwealth of Australia, as follows:

Part I—Preliminary

1 Short title

This Act may be cited as the Privacy Act 1988.

2 Commencement

This Act commences on a day to be fixed by Proclamation.

2A Objects of this Act

The objects of this Act are:

(a) to promote the protection of the privacy of individuals; and
Part I Preliminary

Section 3

(b) to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities; and
(c) to provide the basis for nationally consistent regulation of privacy and the handling of personal information; and
(d) to promote responsible and transparent handling of personal information by entities; and
(e) to facilitate an efficient credit reporting system while ensuring that the privacy of individuals is respected; and
(f) to facilitate the free flow of information across national borders while ensuring that the privacy of individuals is respected; and
(g) to provide a means for individuals to complain about an alleged interference with their privacy; and
(h) to implement Australia’s international obligation in relation to privacy.

3 Saving of certain State and Territory laws

It is the intention of the Parliament that this Act is not to affect the operation of a law of a State or of a Territory that makes provision with respect to the collection, holding, use, correction or disclosure of personal information (including such a law relating to credit reporting or the use of information held in connection with credit reporting) and is capable of operating concurrently with this Act.

Note: Such a law can have effect for the purposes of the provisions of the Australian Privacy Principles that regulate the handling of personal information by organisations by reference to the effect of other laws.

3A Application of the Criminal Code

Chapter 2 of the Criminal Code (except Part 2.5) applies to all offences against this Act.

Note: Chapter 2 of the Criminal Code sets out the general principles of criminal responsibility.
4 Act to bind the Crown

(1) This Act binds the Crown in right of the Commonwealth, of each of the States, of the Australian Capital Territory and of the Northern Territory.

(2) Nothing in this Act renders the Crown in right of the Commonwealth, of a State, of the Australian Capital Territory or of the Northern Territory liable to be prosecuted for an offence.

(3) Nothing in this Act shall be taken to have the effect of making the Crown in right of a State, of the Australian Capital Territory or of the Northern Territory an agency for the purposes of this Act.

5A Extension to external Territories

This Act extends to all external Territories.

5B Extra-territorial operation of Act

Agencies

(1) This Act, a registered APP code and the registered CR code extend to an act done, or practice engaged in, outside Australia and the external Territories by an agency.

Note: The act or practice overseas will not breach an Australian Privacy Principle or a registered APP code if the act or practice is required by an applicable foreign law (see sections 6A and 6B).

Organisations and small business operators

(1A) This Act, a registered APP code and the registered CR code extend to an act done, or practice engaged in, outside Australia and the external Territories by an organisation, or small business operator, that has an Australian link.

Note: The act or practice overseas will not breach an Australian Privacy Principle or a registered APP code if the act or practice is required by an applicable foreign law (see sections 6A and 6B).
Part I  Preliminary

Section 5B

Australian link

(2) An organisation or small business operator has an Australian link if the organisation or operator is:
   (a) an Australian citizen; or
   (b) a person whose continued presence in Australia is not subject to a limitation as to time imposed by law; or
   (c) a partnership formed in Australia or an external Territory; or
   (d) a trust created in Australia or an external Territory; or
   (e) a body corporate incorporated in Australia or an external Territory; or
   (f) an unincorporated association that has its central management and control in Australia or an external Territory.

(3) An organisation or small business operator also has an Australian link if all of the following apply:
   (a) the organisation or operator is not described in subsection (2);
   (b) the organisation or operator carries on business in Australia or an external Territory;
   (c) the personal information was collected or held by the organisation or operator in Australia or an external Territory, either before or at the time of the act or practice.

Power to deal with complaints about overseas acts and practices

(4) Part V of this Act has extra-territorial operation so far as that Part relates to complaints and investigation concerning acts and practices to which this Act extends because of subsection (1) or (1A).

Note: This lets the Commissioner take action overseas to investigate complaints and lets the ancillary provisions of Part V operate in that context.
Part II—Interpretation

Division 1—General definitions

6 Interpretation

(1) In this Act, unless the contrary intention appears:

*ACC* means the Australian Crime Commission.

*access seeker* has the meaning given by subsection 6L(1).

*ACT enactment* has the same meaning as *enactment* has in the *Australian Capital Territory (Self-Government) Act 1988*.

*advice related functions* has the meaning given by subsection 28B(1).

*affected information recipient* means:

(a) a mortgage insurer; or

(b) a trade insurer; or

(c) a body corporate referred to in paragraph 21G(3)(b); or

(d) a person referred to in paragraph 21G(3)(c); or

(e) an entity or adviser referred to in paragraph 21N(2)(a).

*agency* means:

(a) a Minister; or

(b) a Department; or

(c) a body (whether incorporated or not), or a tribunal, established or appointed for a public purpose by or under a Commonwealth enactment, not being:

(i) an incorporated company, society or association; or

(ii) an organisation that is registered under the *Fair Work (Registered Organisations) Act 2009* or a branch of such an organisation; or
(d) a body established or appointed by the Governor-General, or by a Minister, otherwise than by or under a Commonwealth enactment; or
(e) a person holding or performing the duties of an office established by or under, or an appointment made under, a Commonwealth enactment, other than a person who, by virtue of holding that office, is the Secretary of a Department; or
(f) a person holding or performing the duties of an appointment, being an appointment made by the Governor-General, or by a Minister, otherwise than under a Commonwealth enactment; or
(g) a federal court; or
(h) the Australian Federal Police; or
(ha) a Norfolk Island agency; or
(k) an eligible hearing service provider; or
(l) the service operator under the *Healthcare Identifiers Act 2010*.

*amount of credit* has the meaning given by subsection 6M(2).

*annual turnover* of a business has the meaning given by section 6DA.

*APP code* has the meaning given by section 26C.

*APP code developer* means:
(a) an APP entity; or
(b) a group of APP entities; or
(c) a body or association representing one or more APP entities.

*APP complaint* means a complaint about an act or practice that, if established, would be an interference with the privacy of an individual because it breached an Australian Privacy Principle.

*APP entity* means an agency or organisation.
APP privacy policy has the meaning given by Australian Privacy Principle 1.3.

at risk from an eligible data breach has the meaning given by section 26WE.

Australian law means:
   (a) an Act of the Commonwealth or of a State or Territory; or
   (b) regulations, or any other instrument, made under such an Act; or
   (c) a Norfolk Island enactment; or
   (d) a rule of common law or equity.

Australian link has the meaning given by subsections 5B(2) and (3).

Australian Privacy Principle has the meaning given by section 14.

authorised agent of a reporting entity means a person authorised to act on behalf of the reporting entity as mentioned in section 37 of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006.

bank means:
   (a) the Reserve Bank of Australia; or
   (b) a body corporate that is an ADI (authorised deposit-taking institution) for the purposes of the Banking Act 1959; or
   (c) a person who carries on State banking within the meaning of paragraph 51(xiii) of the Constitution.

Bankruptcy Act means the Bankruptcy Act 1966.

ban period has the meaning given by subsection 20K(3).

Board of the ACC means the Board of the Australian Crime Commission established under section 7B of the Australian Crime Commission Act 2002.
Part II Interpretation
Division 1 General definitions

Section 6

(a) in relation to an Australian Privacy Principle, has the meaning given by section 6A; and
(b) in relation to a registered APP code, has the meaning given by section 6B; and
(c) in relation to the registered CR code, has the meaning given by section 6BA.

civil penalty order has the meaning given by subsection 80W(4).

civil penalty provision has the meaning given by section 80U.

class member, in relation to a representative complaint, means any of the persons on whose behalf the complaint was lodged, but does not include a person who has withdrawn under section 38B.

code complaint means a complaint about an act or practice that, if established, would be an interference with the privacy of an individual because it breached a registered APP code.

Codes Register has the meaning given by subsection 26U(1).

collects: an entity collects personal information only if the entity collects the personal information for inclusion in a record or generally available publication.

commercial credit means credit (other than consumer credit) that is applied for by, or provided to, a person.

commercial credit related purpose of a credit provider in relation to a person means the purpose of:
(a) assessing an application for commercial credit made by the person to the provider; or
(b) collecting payments that are overdue in relation to commercial credit provided by the provider to the person.

Commissioner means the Information Commissioner within the meaning of the Australian Information Commissioner Act 2010.

Commissioner of Police means the Commissioner of Police appointed under the Australian Federal Police Act 1979.
Interpretation  Part II
General definitions  Division 1

Section 6

**Commission of inquiry** means:
(a) the Commission of inquiry within the meaning of the *Quarantine Act 1908* (as in force immediately before its repeal); or
(b) a Commission of inquiry within the meaning of the *Offshore Petroleum and Greenhouse Gas Storage Act 2006*.

**committee of management** of an unincorporated association means a body (however described) that governs, manages or conducts the affairs of the association.

**Commonwealth contract** means a contract, to which the Commonwealth or an agency is or was a party, under which services are to be, or were to be, provided to an agency.

Note: See also subsection (9) about provision of services to an agency.

**Commonwealth enactment** means:
(a) an Act other than:
   (i) the *Northern Territory (Self-Government) Act 1978*; or
   (ii) an Act providing for the administration or government of an external Territory; or
   (iii) the *Australian Capital Territory (Self-Government) Act 1988*;
(b) an Ordinance of the Australian Capital Territory;
(c) an instrument (including rules, regulations or by-laws) made under an Act to which paragraph (a) applies or under an Ordinance to which paragraph (b) applies; or
(d) any other legislation that applies as a law of the Commonwealth (other than legislation in so far as it is applied by an Act referred to in subparagraph (a)(i) or (ii)) or as a law of the Australian Capital Territory, to the extent that it operates as such a law.

**Commonwealth officer** means a person who holds office under, or is employed by, the Commonwealth, and includes:
(a) a person appointed or engaged under the *Public Service Act 1999*;

---

*Privacy Act 1988* 9

Compilation No. 78  Compilation date: 1/7/18  Registered: 30/7/18

Authorised Version C2018C00292 registered 30/07/2018
Part II Interpretation
Division 1 General definitions

Section 6

(b) a person (other than a person referred to in paragraph (a)) permanently or temporarily employed by, or in the service of, an agency;
(c) a member of the Defence Force; and
(d) a member, staff member or special member of the Australian Federal Police;

but does not include a person permanently or temporarily employed in the Australian Capital Territory Government Service or in the Public Service of the Northern Territory.

Commonwealth record has the same meaning as in the Archives Act 1983.

consent means express consent or implied consent.

consumer credit means credit:
(a) for which an application has been made by an individual to a credit provider, or that has been provided to an individual by a credit provider, in the course of the provider carrying on a business or undertaking as a credit provider; and
(b) that is intended to be used wholly or primarily:
   (i) for personal, family or household purposes; or
   (ii) to acquire, maintain, renovate or improve residential property for investment purposes; or
   (iii) to refinance consumer credit that has been provided wholly or primarily to acquire, maintain, renovate or improve residential property for investment purposes.

consumer credit liability information: if a credit provider provides consumer credit to an individual, the following information about the consumer credit is consumer credit liability information about the individual:
(a) the name of the provider;
(b) whether the provider is a licensee;
(c) the type of consumer credit;
(d) the day on which the consumer credit is entered into;
(e) the terms or conditions of the consumer credit:
(i) that relate to the repayment of the amount of credit; and
(ii) that are prescribed by the regulations;
(f) the maximum amount of credit available under the consumer credit;
(g) the day on which the consumer credit is terminated or otherwise ceases to be in force.

**consumer credit related purpose** of a credit provider in relation to an individual means the purpose of:
(a) assessing an application for consumer credit made by the individual to the provider; or
(b) collecting payments that are overdue in relation to consumer credit provided by the provider to the individual.

**contracted service provider**, for a government contract, means:
(a) an organisation that is or was a party to the government contract and that is or was responsible for the provision of services to an agency or a State or Territory authority under the government contract; or
(b) a subcontractor for the government contract.

**corporation** means a body corporate that:
(a) is a foreign corporation;
(b) is a trading corporation formed within the limits of Australia or is a financial corporation so formed; or
(c) is incorporated in a Territory, other than the Northern Territory.

**court proceedings information** about an individual means information about a judgement of an Australian court:
(a) that is made, or given, against the individual in proceedings (other than criminal proceedings); and
(b) that relates to any credit that has been provided to, or applied for by, the individual.

**court/tribunal order** means an order, direction or other instrument made by:
Part II Interpretation
Division 1 General definitions

Section 6

(a) a court; or
(b) a tribunal; or
(c) a judge (including a judge acting in a personal capacity) or a person acting as a judge; or
(d) a magistrate (including a magistrate acting in a personal capacity) or a person acting as a magistrate; or
(e) a member or an officer of a tribunal;
and includes an order, direction or other instrument that is of an interim or interlocutory nature.

CP derived information about an individual means any personal information (other than sensitive information) about the individual:
(a) that is derived from credit reporting information about the individual that was disclosed to a credit provider by a credit reporting body under Division 2 of Part IIA; and
(b) that has any bearing on the individual’s credit worthiness; and
(c) that is used, has been used or could be used in establishing the individual’s eligibility for consumer credit.

CRB derived information about an individual means any personal information (other than sensitive information) about the individual:
(a) that is derived by a credit reporting body from credit information about the individual that is held by the body; and
(b) that has any bearing on the individual’s credit worthiness; and
(c) that is used, has been used or could be used in establishing the individual’s eligibility for consumer credit.

CR code has the meaning given by section 26N.

CR code developer means:
(a) an entity that is subject to Part IIA; or
(b) a group of entities that are subject to Part IIA; or
(c) a body or association representing one or more entities that are subject to Part IIA.
Interpretation

Part II

General definitions

Division 1

Section 6

credit has the meaning given by subsections 6M(1) and (3).

credit card means any article of a kind commonly known as a credit card, charge card or any similar article intended for use in obtaining cash, goods or services by means of credit, and includes any article of a kind commonly issued by persons carrying on business to customers or prospective customers of those persons for use in obtaining goods or services from those persons by means of credit.

credit eligibility information about an individual means:
(a) credit reporting information about the individual that was disclosed to a credit provider by a credit reporting body under Division 2 of Part IIIA; or
(b) CP derived information about the individual.

credit enhancement, in relation to credit, means:
(a) the process of insuring risk associated with purchasing or funding the credit by means of a securitisation arrangement; or
(b) any other similar process related to purchasing or funding the credit by those means.

credit guarantee purpose of a credit provider in relation to an individual means the purpose of assessing whether to accept the individual as a guarantor in relation to:
(a) credit provided by the provider to a person other than the individual; or
(b) credit for which an application has been made to the provider by a person other than the individual.

credit information has the meaning given by section 6N.

credit provider has the meaning given by sections 6G to 6K, and, for the purposes of sections 7 and 8 and Parts III, IIIB, IV and V, is taken to include a mortgage insurer and a trade insurer.

credit reporting body means:
(a) an organisation; or
Part II Interpretation
Division 1 General definitions

Section 6

(b) an agency prescribed by the regulations; that carries on a credit reporting business.

credit reporting business has the meaning given by section 6P.

credit reporting complaint means a complaint about an act or practice that, if established, would be an interference with the privacy of an individual because:
(a) it breached the registered CR code; or
(b) it breached a provision of Part IIIA.

credit reporting information about an individual means credit information, or CRB derived information, about the individual.

credit worthiness of an individual means the individual’s:
(a) eligibility to be provided with consumer credit; or
(b) history in relation to consumer credit; or
(c) capacity to repay an amount of credit that relates to consumer credit.

de facto partner of an individual has the meaning given by the Acts Interpretation Act 1901.

default information has the meaning given by section 6Q.

Defence Department means the Department of State that deals with defence and that is administered by the Minister administering section 1 of the Defence Act 1903.

Defence Force includes the Australian Defence Force Cadets.

de-identified: personal information is de-identified if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.

Department means an Agency within the meaning of the Public Service Act 1999.

eligible data breach has the meaning given by Division 2 of Part IIIC.
**eligible hearing service provider** means an entity (within the meaning of the *Hearing Services Administration Act 1997*):

(a) that is, or has at any time been, engaged under Part 3 of the *Hearing Services Administration Act 1997* to provide hearing services; and

(b) that is not covered by paragraph (a), (b), (c), (d), (e), (f), (g) or (h) of the definition of *agency*.

**employee record**, in relation to an employee, means a record of personal information relating to the employment of the employee. Examples of personal information relating to the employment of the employee are health information about the employee and personal information about all or any of the following:

(a) the engagement, training, disciplining or resignation of the employee;

(b) the termination of the employment of the employee;

(c) the terms and conditions of employment of the employee;

(d) the employee’s personal and emergency contact details;

(e) the employee’s performance or conduct;

(f) the employee’s hours of employment;

(g) the employee’s salary or wages;

(h) the employee’s membership of a professional or trade association;

(i) the employee’s trade union membership;

(j) the employee’s recreation, long service, sick, personal, maternity, paternity or other leave;

(k) the employee’s taxation, banking or superannuation affairs.

**enactment** includes a Norfolk Island enactment.

**enforcement body** means:

(a) the Australian Federal Police; or

(aa) the Integrity Commissioner; or

(b) the ACC; or

(ca) the Immigration Department; or

(d) the Australian Prudential Regulation Authority; or
Part II  Interpretation
Division 1  General definitions

Section 6

(e) the Australian Securities and Investments Commission; or
(ea) the Office of the Director of Public Prosecutions, or a similar body established under a law of a State or Territory; or
(f) another agency, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law; or
(g) another agency, to the extent that it is responsible for administering a law relating to the protection of the public revenue; or
(h) a police force or service of a State or a Territory; or
(i) the New South Wales Crime Commission; or
(j) the Independent Commission Against Corruption of New South Wales; or
(k) the Law Enforcement Conduct Commission of New South Wales; or
(ka) the Independent Broad-based Anti-corruption Commission of Victoria; or
(l) the Crime and Corruption Commission of Queensland; or
(la) the Corruption and Crime Commission of Western Australia; or
(lb) the Independent Commissioner Against Corruption of South Australia; or
(m) another prescribed authority or body that is established under a law of a State or Territory to conduct criminal investigations or inquiries; or
(n) a State or Territory authority, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law; or
(o) a State or Territory authority, to the extent that it is responsible for administering a law relating to the protection of the public revenue.

enforcement related activity means:
(a) the prevention, detection, investigation, prosecution or punishment of:
Interpretation  
Part II  
General definitions  
Division 1  

Section 6

(i) criminal offences; or  
(ii) breaches of a law imposing a penalty or sanction; or  
(b) the conduct of surveillance activities, intelligence gathering activities or monitoring activities; or  
(c) the conduct of protective or custodial activities; or  
(d) the enforcement of laws relating to the confiscation of the proceeds of crime; or  
(e) the protection of the public revenue; or  
(f) the prevention, detection, investigation or remedying of misconduct of a serious nature, or other conduct prescribed by the regulations; or  
(g) the preparation for, or conduct of, proceedings before any court or tribunal, or the implementation of court/tribunal orders.

entity means:  
(a) an agency; or  
(b) an organisation; or  
(c) a small business operator.

Federal Circuit Court means the Federal Circuit Court of Australia.

Federal Court means the Federal Court of Australia.

file number complaint means a complaint about an act or practice that, if established, would be an interference with the privacy of an individual:  
(a) because it breached a rule issued under section 17; or  
(b) because it involved an unauthorised requirement or request for disclosure of a tax file number.

financial corporation means a financial corporation within the meaning of paragraph 51(xx) of the Constitution.

foreign corporation means a foreign corporation within the meaning of paragraph 51(xx) of the Constitution.
Part II  Interpretation

Division 1  General definitions

Section 6


generally available publication means a magazine, book, article, newspaper or other publication that is, or will be, generally available to members of the public:

(a) whether or not it is published in print, electronically or in any other form; and

(b) whether or not it is available on the payment of a fee.

genetic relative of an individual (the first individual) means another individual who is related to the first individual by blood, including but not limited to a sibling, a parent or a descendant of the first individual.

government contract means a Commonwealth contract or a State contract.

government related identifier of an individual means an identifier of the individual that has been assigned by:

(a) an agency; or

(b) a State or Territory authority; or

(c) an agent of an agency, or a State or Territory authority, acting in its capacity as agent; or

(d) a contracted service provider for a Commonwealth contract, or a State contract, acting in its capacity as contracted service provider for that contract.

guarantee includes an indemnity given against the default of a person in making a payment in relation to credit that has been applied for by, or provided to, the person.

guidance related functions has the meaning given by subsection 28(1).

healthcare identifier has the meaning given by the Healthcare Identifiers Act 2010.

healthcare identifier offence means:
Interpretation Part II
General definitions Division 1

Section 6

(a) an offence against section 26 of the Healthcare Identifiers Act 2010; or
(b) an offence against section 6 of the Crimes Act 1914 that relates to an offence mentioned in paragraph (a) of this definition.

Note: For ancillary offences, see section 11.6 of the Criminal Code.

health information has the meaning given by section 6FA.

health service has the meaning given by section 6FB.

hearing services has the same meaning as in the Hearing Services Administration Act 1997.

holds: an entity holds personal information if the entity has possession or control of a record that contains the personal information.

Note: See section 10 for when an agency is taken to hold a record.

identification information about an individual means:
(a) the individual’s full name; or
(b) an alias or previous name of the individual; or
(c) the individual’s date of birth; or
(d) the individual’s sex; or
(e) the individual’s current or last known address, and 2 previous addresses (if any); or
(f) the name of the individual’s current or last known employer; or
(g) if the individual holds a driver’s licence—the individual’s driver’s licence number.

identifier of an individual means a number, letter or symbol, or a combination of any or all of those things, that is used to identify the individual or to verify the identity of the individual, but does not include:
(a) the individual’s name; or
(b) the individual’s ABN (within the meaning of the A New Tax System (Australian Business Number) Act 1999); or
Part II Interpretation
Division 1 General definitions

Section 6

(c) anything else prescribed by the regulations.

*Immigration Department* means the Department administered by the Minister administering the *Migration Act 1958*.

*individual* means a natural person.

*information request* has the meaning given by section 6R.

*Integrity Commissioner* has the same meaning as in the *Law Enforcement Integrity Commissioner Act 2006*.

*intelligence agency* means:
(a) the Australian Security Intelligence Organisation;
(b) the Australian Secret Intelligence Service; or
(ba) the Australian Signals Directorate; or
(c) the Office of National Assessments.

*interested party* has the meaning given by subsections 20T(3) and 21V(3).

*interference with the privacy of an individual* has the meaning given by sections 13 to 13F.

*licensee* has the meaning given by the *National Consumer Credit Protection Act 2009*.

*managing credit* does not include the act of collecting overdue payments in relation to credit.

*media organisation* means an organisation whose activities consist of or include the collection, preparation for dissemination or dissemination of the following material for the purpose of making it available to the public:
(a) material having the character of news, current affairs, information or a documentary;
(b) material consisting of commentary or opinion on, or analysis of, news, current affairs, information or a documentary.

*medical research* includes epidemiological research.
Interpretation

Part II

General definitions Division 1

Section 6

misconduct includes fraud, negligence, default, breach of trust, breach of duty, breach of discipline or any other misconduct in the course of duty.

monitoring related functions has the meaning given by subsections 28A(1) and (2).

mortgage credit means consumer credit:

(a) that is provided in connection with the acquisition, maintenance, renovation or improvement of real property; and

(b) in relation to which the real property is security.

mortgage insurance purpose of a mortgage insurer in relation to an individual is the purpose of assessing:

(a) whether to provide insurance to, or the risk of providing insurance to, a credit provider in relation to mortgage credit:
   (i) provided by the provider to the individual; or
   (ii) for which an application to the provider has been made by the individual; or

(b) the risk of the individual defaulting on mortgage credit in relation to which the insurer has provided insurance to a credit provider; or

(c) the risk of the individual being unable to meet a liability that might arise under a guarantee provided, or proposed to be provided, in relation to mortgage credit provided by a credit provider to another person.

mortgage insurer means an organisation, or small business operator, that carries on a business or undertaking that involves providing insurance to credit providers in relation to mortgage credit provided by providers to other persons.

National Personal Insolvency Index has the meaning given by the Bankruptcy Act.

new arrangement information has the meaning given by section 6S.
Part II Interpretation
Division 1 General definitions

Section 6

**non-profit organisation** means an organisation:
(a) that is a non-profit organisation; and
(b) that engages in activities for cultural, recreational, political, religious, philosophical, professional, trade or trade union purposes.

**Norfolk Island agency** means:
(a) a Norfolk Island Minister; or
(b) a public sector agency (within the meaning of the Public Sector Management Act 2000 of Norfolk Island); or
(c) a body (whether incorporated or not), or a tribunal, established for a public purpose by or under a Norfolk Island enactment, other than a body established or registered under:
   (i) the Companies Act 1985 of Norfolk Island; or
   (ii) the Associations Incorporation Act 2005 of Norfolk Island; or
   (e) a person holding or performing the duties of:
      (i) an office established by or under a Norfolk Island enactment; or
      (ii) an appointment made under a Norfolk Island enactment; or
   (g) a court of Norfolk Island.

**Norfolk Island enactment** means:
(a) an enactment (within the meaning of the Norfolk Island Act 1979); or
(b) an instrument (including rules, regulations or by-laws) made under such an enactment;
and includes a Norfolk Island enactment as amended by another Norfolk Island enactment.

**offence against this Act** includes an offence against section 6 of the Crimes Act 1914, or section 11.1, 11.2, 11.2A, 11.4 or 11.5 of the Criminal Code, that relates to an offence against this Act.

**Ombudsman** means the Commonwealth Ombudsman.
Interpretation  Part II
General definitions  Division 1

Section 6

organisation has the meaning given by section 6C.

overseas recipient, in relation to personal information, has the meaning given by Australian Privacy Principle 8.1.

payment information has the meaning given by section 6T.

penalty unit has the meaning given by section 4AA of the Crimes Act 1914.

pending correction request in relation to credit information or CRB derived information means:
(a) a request made under subsection 20T(1) in relation to the information if a notice has not been given under subsection 20U(2) or (3) in relation to the request; or
(b) a request made under subsection 21V(1) in relation to the information if:
   (i) the credit reporting body referred to in subsection 20V(3) has been consulted about the request under subsection 21V(3); and
   (ii) a notice has not been given under subsection 21W(2) or (3) in relation to the request.

pending dispute in relation to credit information or CRB derived information means:
(a) a complaint made under section 23A that relates to the information if a decision about the complaint has not been made under subsection 23B(4); or
(b) a matter that relates to the information and that is still being dealt with by a recognised external dispute resolution scheme; or
(c) a complaint made to the Commissioner under Part V that relates to the information and that is still being dealt with.

permitted CP disclosure has the meaning given by sections 21J to 21N.

permitted CP use has the meaning given by section 21H.
Part II Interpretation
Division 1 General definitions

Section 6

permitted CRB disclosure has the meaning given by section 20F.

permitted general situation has the meaning given by section 16A.

permitted health situation has the meaning given by section 16B.

personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and
(b) whether the information or opinion is recorded in a material form or not.

Note: Section 187LA of the Telecommunications (Interception and Access) Act 1979 extends the meaning of personal information to cover information kept under Part 5-1A of that Act.

personal insolvency information has the meaning given by section 6U.

pre-screening assessment means an assessment made under paragraph 20G(2)(d).

principal executive, of an agency, has a meaning affected by section 37.

purchase, in relation to credit, includes the purchase of rights to receive payments relating to the credit.

recognised external dispute resolution scheme means an external dispute resolution scheme recognised under section 35A.

record includes:

(a) a document; or
(b) an electronic or other device;

but does not include:

(d) a generally available publication; or
(e) anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition; or
(f) Commonwealth records as defined by subsection 3(1) of the *Archives Act 1983* that are in the open access period for the purposes of that Act; or

(fa) records (as defined in the *Archives Act 1983*) in the care (as defined in that Act) of the National Archives of Australia in relation to which the Archives has entered into arrangements with a person other than a Commonwealth institution (as defined in that Act) providing for the extent to which the Archives or other persons are to have access to the records; or

(g) documents placed by or on behalf of a person (other than an agency) in the memorial collection within the meaning of the *Australian War Memorial Act 1980*; or

(h) letters or other articles in the course of transmission by post.

Note: For document, see section 2B of the *Acts Interpretation Act 1901*.

registered APP code has the meaning given by section 26B.

registered CR code has the meaning given by section 26M.

registered political party means a political party registered under Part XI of the *Commonwealth Electoral Act 1918*.

regulated information of an affected information recipient means:

(a) if the recipient is a mortgage insurer or trade insurer—
    personal information disclosed to the recipient under Division 2 or 3 of Part IIIA; or

(b) if the recipient is a body corporate referred to in paragraph 21G(3)(b)—credit eligibility information disclosed to the recipient under that paragraph; or

(c) if the recipient is a person referred to in paragraph 21G(3)(c)—credit eligibility information disclosed to the recipient under that paragraph; or

(d) if the recipient is an entity or adviser referred to in paragraph 21N(2)(a)—credit eligibility information disclosed to the recipient under subsection 21N(2).
Part II Interpretation
Division 1 General definitions

Section 6

**repayment history information** has the meaning given by subsection 6V(1).

**reporting entity** has the same meaning as in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.

**representative complaint** means a complaint where the persons on whose behalf the complaint was made include persons other than the complainant, but does not include a complaint that the Commissioner has determined should no longer be continued as a representative complaint.

**residential property** has the meaning given by section 204 of the National Credit Code (within the meaning of the *National Consumer Credit Protection Act 2009*).

**respondent** for a complaint made under section 23A means the credit reporting body or credit provider to which the complaint is made.

**responsible person** has the meaning given by section 6AA.

**retention period** has the meaning given by sections 20W and 20X.

**Secretary** means an Agency Head within the meaning of the *Public Service Act 1999*.

**securitisation arrangement** means an arrangement:

(a) involving the funding, or proposed funding, of:

(i) credit that has been, or is to be, provided by a credit provider; or

(ii) the purchase of credit by a credit provider; by issuing instruments or entitlements to investors; and

(b) under which payments to investors in respect of such instruments or entitlements are principally derived, directly or indirectly, from such credit.

**securitisation related purpose** of a credit provider in relation to an individual is the purpose of:
Section 6

(a) assessing the risk in purchasing, by means of a securitisation arrangement, credit that has been provided to, or applied for by:
   (i) the individual; or
   (ii) a person for whom the individual is, or is proposing to be, a guarantor; or
(b) assessing the risk in undertaking credit enhancement in relation to credit:
   (i) that is, or is proposed to be, purchased or funded by means of a securitisation arrangement; and
   (ii) that has been provided to, or applied for by, the individual or a person for whom the individual is, or is proposing to be, a guarantor.

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

**Serious credit infringement** means:
(a) an act done by an individual that involves fraudulently obtaining consumer credit, or attempting fraudulently to obtain consumer credit; or
(b) an act done by an individual that involves fraudulently evading the individual’s obligations in relation to consumer credit, or attempting fraudulently to evade those obligations; or
(c) an act done by an individual if:
   (i) a reasonable person would consider that the act indicates an intention, on the part of the individual, to no longer comply with the individual’s obligations in relation to consumer credit provided by a credit provider; and
   (ii) the provider has, after taking such steps as are reasonable in the circumstances, been unable to contact the individual about the act; and
   (iii) at least 6 months have passed since the provider last had contact with the individual.

small business has the meaning given by section 6D.

small business operator has the meaning given by section 6D.

solicits: an entity solicits personal information if the entity requests another entity to provide the personal information, or to provide a kind of information in which that personal information is included.

staff of the Ombudsman means the persons appointed or employed for the purposes of section 31 of the Ombudsman Act 1976.

State includes the Australian Capital Territory and the Northern Territory.

State contract means a contract, to which a State or Territory or State or Territory authority is or was a party, under which services are to be, or were to be, provided to a State or Territory authority.

Note: See also subsection (9) about provision of services to a State or Territory authority.
State or Territory authority has the meaning given by section 6C.

subcontractor, for a government contract, means an organisation:

(a) that is or was a party to a contract (the subcontract):
   (i) with a contracted service provider for the government contract (within the meaning of paragraph (a) of the definition of contracted service provider); or
   (ii) with a subcontractor for the government contract (under a previous application of this definition); and

(b) that is or was responsible under the subcontract for the provision of services to an agency or a State or Territory authority, or to a contracted service provider for the government contract, for the purposes (whether direct or indirect) of the government contract.

tax file number means a tax file number as defined in Part VA of the Income Tax Assessment Act 1936.

tax file number information means information, whether compiled lawfully or unlawfully, and whether recorded in a material form or not, that records the tax file number of a person in a manner connecting it with the person’s identity.

temporary public interest determination means a determination made under section 80A.

trade insurance purpose of a trade insurer in relation to an individual is the purpose of assessing:

(a) whether to provide insurance to, or the risk of providing insurance to, a credit provider in relation to commercial credit provided by the provider to the individual or another person; or

(b) the risk of a person defaulting on commercial credit in relation to which the insurer has provided insurance to a credit provider.

trade insurer means an organisation, or small business operator, that carries on a business or undertaking that involves providing
Part II Interpretation
Division 1 General definitions

Section 6

insurance to credit providers in relation to commercial credit provided by providers to other persons.

trading corporation means a trading corporation within the meaning of paragraph 51(xx) of the Constitution.

(1A) In order to avoid doubt, it is declared that an ACT enactment is not a Commonwealth enactment for the purposes of this Act.

(3) For the purposes of this Act, an act or practice breaches a rule issued under section 17 if, and only if, it is contrary to, or inconsistent with, the rule.

(4) The definition of individual in subsection (1) shall not be taken to imply that references to persons do not include persons other than natural persons.

(5) For the purposes of this Act, a person shall not be taken to be an agency merely because the person is the holder of, or performs the duties of:

(a) a prescribed office; or
(b) an office prescribed by regulations made for the purposes of subparagraph 4(3)(b)(i) of the Freedom of Information Act 1982; or
(c) an office established by or under a Commonwealth enactment for the purposes of an agency; or
(ca) an office established by or under a Norfolk Island enactment for the purposes of a Norfolk Island agency; or
(d) a judicial office or of an office of magistrate; or
(e) an office of member of a tribunal that is established by or under a law of the Commonwealth and that is prescribed for the purposes of this paragraph; or
(f) an office of member of a tribunal that is established by or under a Norfolk Island enactment and that is prescribed for the purposes of this paragraph.

(6) For the purposes of this Act, the Defence Department shall be taken to include the Defence Force.
(7) Nothing in this Act prevents a complaint from:
   (a) being both a file number complaint and an APP complaint; or
   (b) being both a file number complaint and a credit reporting complaint; or
   (c) being both a file number complaint and a code complaint; or
   (e) being both a file number complaint and a credit reporting complaint; or
   (f) being both an APP complaint and a credit reporting complaint; or
   (g) being both an APP complaint and a code complaint.

(8) For the purposes of this Act, the question whether bodies corporate are related to each other is determined in the manner in which that question is determined under the Corporations Act 2001.

(9) To avoid doubt, for the purposes of this Act, services provided to an agency or a State or Territory authority include services that consist of the provision of services to other persons in connection with the performance of the functions of the agency or State or Territory authority.

(10) For the purposes of this Act, a reference to family in the definition of consumer credit in subsection 6(1), and in sections 6D and 16, in relation to any individual is taken to include the following (without limitation):
   (a) a de facto partner of the individual;
   (b) someone who is the child of the person, or of whom the person is the child, because of the definition of child in subsection (11);
   (c) anyone else who would be a member of the individual’s family if someone mentioned in paragraph (a) or (b) is taken to be a member of the individual’s family.

(10A) For the purposes of this Act, the Supreme Court of Norfolk Island is taken not to be a federal court.

(11) In this section:
Part II Interpretation
Division 1 General definitions

Section 6AA

child: without limiting who is a child of a person for the purposes of subsection (10), someone is the child of a person if he or she is a child of the person within the meaning of the Family Law Act 1975.

6AA Meaning of responsible person

(1) A responsible person for an individual is:
(a) a parent of the individual; or
(b) a child or sibling of the individual if the child or sibling is at least 18 years old; or
(c) a spouse or de facto partner of the individual; or
(d) a relative of the individual if the relative is:
   (i) at least 18 years old; and
   (ii) a member of the individual’s household; or
(e) a guardian of the individual; or
(f) a person exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual’s health; or
(g) a person who has an intimate personal relationship with the individual; or
(h) a person nominated by the individual to be contacted in case of emergency.

(2) In this section:

child: without limiting who is a child of an individual for the purposes of subsection (1), each of the following is a child of an individual:
(a) an adopted child, stepchild, exnuptial child or foster child of the individual;
(b) someone who is a child of the individual within the meaning of the Family Law Act 1975.

parent: without limiting who is a parent of an individual for the purposes of subsection (1), someone is a parent of an individual if
the individual is his or her child because of the definition of *child* in this subsection.

*relative* of an individual (the *first individual*) means a grandparent, grandchild, uncle, aunt, nephew or niece of the first individual and for this purpose, relationships to the first individual may also be traced to or through another individual who is:

(a) a de facto partner of the first individual; or

(b) the child of the first individual because of the definition of *child* in this subsection.

*sibling* of an individual includes:

(a) a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister of the individual; and

(b) another individual if a relationship referred to in paragraph (a) can be traced through a parent of either or both of the individuals.

*stepchild*: without limiting who is a stepchild of an individual, someone is a *stepchild* of an individual if he or she would be the individual’s stepchild except that the individual is not legally married to the individual’s de facto partner.

### 6A Breach of an Australian Privacy Principle

(1) For the purposes of this Act, an act or practice *breaches* an Australian Privacy Principle if, and only if, it is contrary to, or inconsistent with, that principle.

*No breach—contracted service provider*

(2) An act or practice does not *breach* an Australian Privacy Principle if:

(a) the act is done, or the practice is engaged in:

(i) by an organisation that is a contracted service provider for a Commonwealth contract (whether or not the organisation is a party to the contract); and
Section 6B

(ii) for the purposes of meeting (directly or indirectly) an obligation under the contract; and
(b) the act or practice is authorised by a provision of the contract that is inconsistent with the principle.

No breach—disclosure to the National Archives of Australia

(3) An act or practice does not breach an Australian Privacy Principle if the act or practice involves the disclosure by an organisation of personal information in a record (as defined in the Archives Act 1983) solely for the purposes of enabling the National Archives of Australia to decide whether to accept, or to arrange, care (as defined in that Act) of the record.

No breach—act or practice outside Australia

(4) An act or practice does not breach an Australian Privacy Principle if:
(a) the act is done, or the practice is engaged in, outside Australia and the external Territories; and
(b) the act or practice is required by an applicable law of a foreign country.

Effect despite subsection (1)

(5) Subsections (2), (3) and (4) have effect despite subsection (1).

6B Breach of a registered APP code

Breach if contrary to, or inconsistent with, code

(1) For the purposes of this Act, an act or practice breaches a registered APP code if, and only if, it is contrary to, or inconsistent with, the code.

No breach—contracted service provider

(2) An act or practice does not breach a registered APP code if:
(a) the act is done, or the practice is engaged in:
Section 6BA

(i) by an organisation that is a contracted service provider for a Commonwealth contract (whether or not the organisation is a party to the contract); and

(ii) for the purposes of meeting (directly or indirectly) an obligation under the contract; and

(b) the act or practice is authorised by a provision of the contract that is inconsistent with the code.

No breach—disclosure to the National Archives of Australia

(3) An act or practice does not breach a registered APP code if the act or practice involves the disclosure by an organisation of personal information in a record (as defined in the Archives Act 1983) solely for the purposes of enabling the National Archives of Australia to decide whether to accept, or to arrange, care (as defined in that Act) of the record.

No breach—act or practice outside Australia

(4) An act or practice does not breach a registered APP code if:

(a) the act is done, or the practice is engaged in, outside Australia and the external Territories; and

(b) the act or practice is required by an applicable law of a foreign country.

Effect despite subsection (1)

(5) Subsections (2), (3) and (4) have effect despite subsection (1).

6BA Breach of the registered CR code

For the purposes of this Act, an act or practice breaches the registered CR code if, and only if, it is contrary to, or inconsistent with, the code.
Part II Interpretation
Division 1 General definitions

Section 6C

6C Organisations

What is an organisation?

(1) In this Act:

organisation means:
(a) an individual; or
(b) a body corporate; or
(c) a partnership; or
(d) any other unincorporated association; or
(e) a trust;

that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory.

Note 1: Under section 187LA of the Telecommunications (Interception and Access) Act 1979, service providers are, in relation to their activities relating to retained data, treated as organisations for the purposes of this Act.

Note 2: Regulations may prescribe an instrumentality by reference to one or more classes of instrumentality. See subsection 13(3) of the Legislation Act 2003.

Example: Regulations may prescribe an instrumentality of a State or Territory that is an incorporated company, society or association and therefore not a State or Territory authority.

Legal person treated as different organisations in different capacities

(2) A legal person can have a number of different capacities in which the person does things. In each of those capacities, the person is taken to be a different organisation.

Example: In addition to his or her personal capacity, an individual may be the trustee of one or more trusts. In his or her personal capacity, he or she is one organisation. As trustee of each trust, he or she is a different organisation.
What is a *State or Territory authority*?

(3) In this Act:

*State or Territory authority* means:

(a) a State or Territory Minister; or

(b) a Department of State of a State or Territory; or

(c) a body (whether incorporated or not), or a tribunal, established or appointed for a public purpose by or under a law of a State or Territory, other than:
   (i) an incorporated company, society or association; or
   (ii) an association of employers or employees that is registered or recognised under a law of a State or Territory dealing with the resolution of industrial disputes; or

(d) a body established or appointed, otherwise than by or under a law of a State or Territory, by:
   (i) a Governor of a State; or
   (ii) the Australian Capital Territory Executive; or
   (iii) the Administrator of the Northern Territory; or
   (v) a State or Territory Minister; or

(e) a person holding or performing the duties of an office established by or under, or an appointment made under, a law of a State or Territory, other than the office of head of a State or Territory Department (however described); or

(f) a person holding or performing the duties of an appointment made, otherwise than under a law of a State or Territory, by:
   (i) a Governor of a State; or
   (ii) the Australian Capital Territory Executive; or
   (iii) the Administrator of the Northern Territory; or
   (v) a State or Territory Minister; or

(g) a State or Territory court.
Part II Interpretation
Division 1 General definitions

Section 6D

Making regulations to stop instrumentalities being organisations

(4) Before the Governor-General makes regulations prescribing an instrumentality of a State or Territory for the purposes of the definition of organisation in subsection (1), the Minister must:
(a) be satisfied that the State or Territory has requested that the instrumentality be prescribed for those purposes; and
(b) consider:
   (i) whether treating the instrumentality as an organisation for the purposes of this Act adversely affects the government of the State or Territory; and
   (ii) the desirability of regulating under this Act the collection, holding, use, correction and disclosure of personal information by the instrumentality; and
   (iii) whether the law of the State or Territory regulates the collection, holding, use, correction and disclosure of personal information by the instrumentality to a standard that is at least equivalent to the standard that would otherwise apply to the instrumentality under this Act; and
(c) consult the Commissioner about the matters mentioned in subparagraphs (b)(ii) and (iii).

State does not include Territory

(5) In this section:

State does not include the Australian Capital Territory or the Northern Territory (despite subsection 6(1)).

6D Small business and small business operators

What is a small business?

(1) A business is a small business at a time (the test time) in a financial year (the current year) if its annual turnover for the previous financial year is $3,000,000 or less.
Test for new business

(2) However, if there was no time in the previous financial year when
the business was carried on, the business is a small business at the
test time only if its annual turnover for the current year is
$3,000,000 or less.

What is a small business operator?

(3) A small business operator is an individual, body corporate,
partnership, unincorporated association or trust that:
(a) carries on one or more small businesses; and
(b) does not carry on a business that is not a small business.

Entities that are not small business operators

(4) However, an individual, body corporate, partnership,
unincorporated association or trust is not a small business operator
if he, she or it:
(a) carries on a business that has had an annual turnover of more
than $3,000,000 for a financial year that has ended after the
later of the following:
   (i) the time he, she or it started to carry on the business;
   (ii) the commencement of this section; or
(b) provides a health service to another individual and holds any
   health information except in an employee record; or
(c) discloses personal information about another individual to
   anyone else for a benefit, service or advantage; or
(d) provides a benefit, service or advantage to collect personal
   information about another individual from anyone else; or
(e) is a contracted service provider for a Commonwealth contract
   (whether or not a party to the contract); or
(f) is a credit reporting body.
Part II Interpretation
Division 1 General definitions

Section 6D

*Private affairs of small business operators who are individuals*

(5) Subsection (4) does not prevent an individual from being a small business operator merely because he or she does something described in paragraph (4)(b), (c) or (d):  
(a) otherwise than in the course of a business he or she carries on; and  
(b) only for the purposes of, or in connection with, his or her personal, family or household affairs.

*Non-business affairs of other small business operators*

(6) Subsection (4) does not prevent a body corporate, partnership, unincorporated association or trust from being a small business operator merely because it does something described in paragraph (4)(b), (c) or (d) otherwise than in the course of a business it carries on.

*Disclosure compelled or made with consent*

(7) Paragraph (4)(c) does not prevent an individual, body corporate, partnership, unincorporated association or trust from being a small business operator only because he, she or it discloses personal information about another individual:  
(a) with the consent of the other individual; or  
(b) as required or authorised by or under legislation.

*Collection with consent or under legislation*

(8) Paragraph (4)(d) does not prevent an individual, body corporate, partnership, unincorporated association or trust from being a small business operator only because he, she or it:  
(a) collects personal information about another individual from someone else:  
(i) with the consent of the other individual; or  
(ii) as required or authorised by or under legislation; and  
(b) provides a benefit, service or advantage to be allowed to collect the information.
(9) Despite subsection (3), a body corporate is not a small business operator if it is related to a body corporate that carries on a business that is not a small business.

6DA What is the annual turnover of a business?

What is the annual turnover of a business for a financial year?

(1) The annual turnover of a business for a financial year is the total of the following that is earned in the year in the course of the business:
(a) the proceeds of sales of goods and/or services;
(b) commission income;
(c) repair and service income;
(d) rent, leasing and hiring income;
(e) government bounties and subsidies;
(f) interest, royalties and dividends;
(g) other operating income.

Note: The annual turnover for a financial year of a business carried on by an entity that does not carry on another business will often be similar to the total of the instalment income the entity notifies to the Commissioner of Taxation for the 4 quarters in the year (or for the year, if the entity pays tax in annual instalments).

(2) However, if a business has been carried on for only part of a financial year, its annual turnover for the financial year is the amount worked out using the formula:

\[
\text{Annual Turnover for Part of Year} = \left( \frac{\text{Annual Turnover for Whole Year}}{\text{Number of Days in Whole Year}} \right) \times \left( \frac{\text{Number of Days in Part}}{\text{Number of Days in Whole Year}} \right)
\]
Part II Interpretation
Division 1 General definitions

Section 6E

6E Small business operator treated as organisation

Small business operator that is a reporting entity

(1A) If a small business operator is a reporting entity or an authorised agent of a reporting entity because of anything done in the course of a small business carried on by the small business operator, this Act applies, with the prescribed modifications (if any), in relation to the activities carried on by the small business operator for the purposes of, or in connection with, activities relating to:

(a) the Anti-Money Laundering and Counter-Terrorism Financing Act 2006; or

(b) regulations or AML/CTF Rules under that Act;

as if the small business operator were an organisation.

Note: The regulations may prescribe different modifications of the Act for different small business operators. See subsection 33(3A) of the Acts Interpretation Act 1901.

Small business operator that is a protected action ballot agent under the Fair Work Act 2009

(1B) If a small business operator is the protected action ballot agent for a protected action ballot conducted under Part 3-3 of the Fair Work Act 2009, this Act applies, with the prescribed modifications (if any), in relation to the activities carried on by the small business operator for the purpose of, or in connection with, the conduct of the protected action ballot, as if the small business operator were an organisation.

Note: The regulations may prescribe different modifications of the Act for different small business operators. See subsection 33(3A) of the Acts Interpretation Act 1901.

Small business operator that is an association of employees that is registered or recognised under the Fair Work (Registered Organisations) Act 2009

(1C) If a small business operator is an association of employees that is registered or recognised under the Fair Work (Registered Organisations) Act 2009, this Act applies, with the prescribed
modifications (if any), in relation to the activities carried on by the small business operator, as if the small business operator were an organisation (within the meaning of this Act).

Note: The regulations may prescribe different modifications of the Act for different small business operators. See subsection 33(3A) of the *Acts Interpretation Act 1901*.

**Regulations treating a small business operator as an organisation**

(1) This Act applies, with the prescribed modifications (if any), in relation to a small business operator prescribed for the purposes of this subsection as if the small business operator were an organisation.

Note 1: The regulations may prescribe different modifications of the Act for different small business operators. See subsection 33(3A) of the *Acts Interpretation Act 1901*.

Note 2: Regulations may prescribe a small business operator by reference to one or more classes of small business operator. See subsection 13(3) of the *Legislation Act 2003*.

**Regulations treating a small business operator as an organisation for particular acts or practices**

(2) This Act also applies, with the prescribed modifications (if any), in relation to the prescribed acts or practices of a small business operator prescribed for the purposes of this subsection as if the small business operator were an organisation.

Note 1: The regulations may prescribe different modifications of the Act for different acts, practices or small business operators. See subsection 33(3A) of the *Acts Interpretation Act 1901*.

Note 2: Regulations may prescribe an act, practice or small business operator by reference to one or more classes of acts, practices or small business operators. See subsection 13(3) of the *Legislation Act 2003*. 
Part II  Interpretation
Division 1  General definitions

Section 6EA

Definition

(3) In this section:

*protected action ballot agent* means a person (other than the Australian Electoral Commission) that conducts a protected action ballot under Part 3-3 of the *Fair Work Act 2009*.

Making regulations

(4) Before the Governor-General makes regulations prescribing a small business operator, act or practice for the purposes of subsection (1) or (2), the Minister must:

(a) be satisfied that it is desirable in the public interest to regulate under this Act the small business operator, act or practice; and

(b) consult the Commissioner about the desirability of regulating under this Act the matters described in paragraph (a).

6EA  Small business operators choosing to be treated as organisations

(1) This Act applies in relation to a small business operator as if the operator were an organisation while a choice by the operator to be treated as an organisation is registered under this section.

(2) A small business operator may make a choice in writing given to the Commissioner to be treated as an organisation.

Note: A small business operator may revoke such a choice by writing given to the Commissioner. See subsection 33(3) of the *Acts Interpretation Act 1901*.

(3) If the Commissioner is satisfied that a small business operator has made the choice to be treated as an organisation, the Commissioner must enter in a register of operators who have made such a choice:

(a) the name or names under which the operator carries on business; and

(b) the operator’s ABN, if the operator has one under the *A New Tax System (Australian Business Number) Act 1999*. 
(4) If a small business operator revokes a choice to be treated as an organisation, the Commissioner must remove from the register the material relating to the operator.

(5) The Commissioner may decide the form of the register and how it is to be kept.

(6) The Commissioner must make the register available to the public in the way that the Commissioner determines. However, the Commissioner must not make available to the public in the register information other than that described in subsection (3).

6F State instrumentalities etc. treated as organisations

Regulations treating a State instrumentality etc. as an organisation

(1) This Act applies, with the prescribed modifications (if any), in relation to a prescribed State or Territory authority or a prescribed instrumentality of a State or Territory (except an instrumentality that is an organisation because of section 6C) as if the authority or instrumentality were an organisation.

Note 1: The regulations may prescribe different modifications of the Act for different authorities or instrumentalities. See subsection 33(3A) of the Acts Interpretation Act 1901.

Note 2: Regulations may prescribe an authority or instrumentality by reference to one or more classes of authority or instrumentality. See subsection 13(3) of the Legislation Act 2003.

Making regulations to treat instrumentality etc. as organisation

(3) Before the Governor-General makes regulations prescribing a State or Territory authority or instrumentality of a State or Territory for the purposes of subsection (1), the Minister must:

(a) be satisfied that the relevant State or Territory has requested that the authority or instrumentality be prescribed for those purposes; and

(b) consult the Commissioner about the desirability of regulating under this Act the collection, holding, use, correction and
Part II Interpretation
Division 1 General definitions

Section 6FA

disclosure of personal information by the authority or instrumentality.

6FA Meaning of health information

The following information is health information:

(a) information or an opinion about:
   (i) the health, including an illness, disability or injury, (at any time) of an individual; or
   (ii) an individual’s expressed wishes about the future provision of health services to the individual; or
   (iii) a health service provided, or to be provided, to an individual;
that is also personal information;

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

(c) other personal information collected in connection with the donation, or intended donation, by an individual of his or her body parts, organs or body substances;

(d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

6FB Meaning of health service

(1) An activity performed in relation to an individual is a health service if the activity is intended or claimed (expressly or otherwise) by the individual or the person performing it:
   (a) to assess, maintain or improve the individual’s health; or
   (b) where the individual’s health cannot be maintained or improved—to manage the individual’s health; or
   (c) to diagnose the individual’s illness, disability or injury; or
   (d) to treat the individual’s illness, disability or injury or suspected illness, disability or injury; or
(e) to record the individual’s health for the purposes of assessing, maintaining, improving or managing the individual’s health.

(2) The dispensing on prescription of a drug or medicinal preparation by a pharmacist is a health service.

(3) To avoid doubt:
   (a) a reference in this section to an individual’s health includes the individual’s physical or psychological health; and
   (b) an activity mentioned in subsection (1) or (2) that takes place in the course of providing aged care, palliative care or care for a person with a disability is a health service.

(4) The regulations may prescribe an activity that, despite subsections (1) and (2) is not to be treated as a health service for the purposes of this Act.
Division 2—Key definitions relating to credit reporting

Subdivision A—Credit provider

6G Meaning of credit provider

General

(1) Each of the following is a credit provider:

(a) a bank;

(b) an organisation or small business operator if:
   (i) the organisation or operator carries on a business or undertaking; and
   (ii) a substantial part of the business or undertaking is the provision of credit;

(c) an organisation or small business operator:
   (i) that carries on a retail business; and
   (ii) that, in the course of the business, issues credit cards to individuals in connection with the sale of goods, or the supply of services, by the organisation or operator (as the case may be);

(d) an agency, organisation or small business operator:
   (i) that carries on a business or undertaking that involves providing credit; and
   (ii) that is prescribed by the regulations.

Other credit providers

(2) If:

(a) an organisation or small business operator (the supplier) carries on a business or undertaking in the course of which the supplier provides credit in connection with the sale of goods, or the supply of services, by the supplier; and

(b) the repayment, in full or in part, of the amount of credit is deferred for at least 7 days; and
Section 6H

(c) the supplier is not a credit provider under subsection (1); then the supplier is a credit provider but only in relation to the credit.

(3) If:

(a) an organisation or small business operator (the lessor) carries on a business or undertaking in the course of which the lessor provides credit in connection with the hiring, leasing or renting of goods; and
(b) the credit is in force for at least 7 days; and
(c) no amount, or an amount less than the value of the goods, is paid as a deposit for the return of the goods; and
(d) the lessor is not a credit provider under subsection (1); then the lessor is a credit provider but only in relation to the credit.

(4) An organisation or small business operator is a credit provider if subsection 6H(1), 6J(1) or 6K(1) provides that the organisation or operator is a credit provider.

Exclusions

(5) Despite subsections (1) to (4) of this section, an organisation or small business operator acting in the capacity of:

(a) a real estate agent; or
(b) a general insurer (within the meaning of the Insurance Act 1973); or
(c) an employer of an individual; is not a credit provider while acting in that capacity.

(6) Despite subsections (1) to (4) of this section, an organisation or small business operator is not a credit provider if it is included in a class of organisations or operators prescribed by the regulations.

6H Agents of credit providers

(1) If an organisation or small business operator (the agent) is acting as an agent of a credit provider (the principal) in performing, on behalf of the principal, a task that is reasonably necessary:
Part II  Interpretation
Division 2  Key definitions relating to credit reporting

Section 6J

(a) in processing an application for credit made to the principal; or
(b) in managing credit provided by the principal;
then, while the agent is so acting, the agent is a credit provider.

(2) Subsection (1) does not apply if the principal is an organisation or small business operator that is a credit provider because of a previous application of that subsection.

(3) If subsection (1) applies in relation to credit that has been provided by the principal, the credit is taken, for the purposes of this Act, to have been provided by both the principal and the agent.

(4) If subsection (1) applies in relation to credit for which an application has been made to the principal, the application is taken, for the purposes of this Act, to have been made to both the principal and the agent.

6J Securitisation arrangements etc.

(1) If:

(a) an organisation or small business operator (the securitisation entity) carries on a business that is involved in either or both of the following:
   (i) a securitisation arrangement;
   (ii) managing credit that is the subject of a securitisation arrangement; and
(b) the securitisation entity performs a task that is reasonably necessary for:
   (i) purchasing, funding or managing, or processing an application for, credit by means of a securitisation arrangement; or
   (ii) undertaking credit enhancement in relation to credit; and
(c) the credit has been provided by, or is credit for which an application has been made to, a credit provider (the original credit provider);
then, while the securitisation entity performs such a task, the
securitisation entity is a **credit provider**.

(2) Subsection (1) does not apply if the original credit provider is an
organisation or small business operator that is a credit provider
because of a previous application of that subsection.

(3) If subsection (1) applies in relation to credit that has been provided
by the original credit provider, the credit is taken, for the purposes
of this Act, to have been provided by both the original credit
provider and the securitisation entity.

(4) If subsection (1) applies in relation to credit for which an
application has been made to the original credit provider, the
application is taken, for the purposes of this Act, to have been
made to both the original credit provider and the securitisation
entity.

**6K Acquisition of the rights of a credit provider**

(1) If:

(a) an organisation or small business operator (the **acquirer**) acquires, whether by assignment, subrogation or any other means, the rights of a credit provider (the **original credit provider**) in relation to the repayment of an amount of credit; and

(b) the acquirer is not a credit provider under subsection 6G(1);
then the acquirer is a **credit provider** but only in relation to the
credit.

(2) If subsection (1) of this section applies in relation to credit that has been provided by the original credit provider, the credit is taken, for the purposes of this Act, to have been provided by the acquirer.

(3) If subsection (1) of this section applies in relation to credit for which an application has been made to the original credit provider, the application is taken, for the purposes of this Act, to have been made to the acquirer.
Part II  Interpretation
Division 2  Key definitions relating to credit reporting

Section 6L

Subdivision B—Other definitions

6L  Meaning of access seeker

(1) An access seeker in relation to credit reporting information, or credit eligibility information, about an individual is:
   (a) the individual; or
   (b) a person:
      (i) who is assisting the individual to deal with a credit reporting body or credit provider; and
      (ii) who is authorised, in writing, by the individual to make a request in relation to the information under subsection 20R(1) or 21T(1).

(2) An individual must not authorise a person under subparagraph (1)(b)(ii) if the person is:
   (a) a credit provider; or
   (b) a mortgage insurer; or
   (c) a trade insurer; or
   (d) a person who is prevented from being a credit provider by subsection 6G(5) or (6).

(3) Subparagraph (1)(b)(ii) does not apply to a person who provides the National Relay Service or a person prescribed by the regulations.

6M  Meaning of credit and amount of credit

(1) Credit is a contract, arrangement or understanding under which:
   (a) payment of a debt owed by one person to another person is deferred; or
   (b) one person incurs a debt to another person and defers the payment of the debt.

(2) The amount of credit is the amount of the debt that is actually deferred, or that may be deferred, but does not include any fees or charges payable in connection with the deferral of the debt.
(3) Without limiting subsection (1), credit includes:

(a) a hire-purchase agreement; and

(b) a contract, arrangement or understanding of a kind referred to in that subsection that is for the hire, lease or rental of goods, or for the supply of services, other than a contract, arrangement or understanding under which:

(i) full payment is made before, or at the same time as, the goods or services are provided; and

(ii) in the case of goods—an amount greater than, or equal to, the value of the goods is paid as a deposit for the return of the goods.

6N Meaning of credit information

Credit information about an individual is personal information (other than sensitive information) that is:

(a) identification information about the individual; or

(b) consumer credit liability information about the individual; or

(c) repayment history information about the individual; or

(d) a statement that an information request has been made in relation to the individual by a credit provider, mortgage insurer or trade insurer; or

(e) the type of consumer credit or commercial credit, and the amount of credit, sought in an application:

(i) that has been made by the individual to a credit provider; and

(ii) in connection with which the provider has made an information request in relation to the individual; or

(f) default information about the individual; or

(g) payment information about the individual; or

(h) new arrangement information about the individual; or

(i) court proceedings information about the individual; or

(j) personal insolvency information about the individual; or

(k) publicly available information about the individual:
Part II Interpretation
Division 2 Key definitions relating to credit reporting

Section 6P

(i) that relates to the individual’s activities in Australia or the external Territories and the individual’s credit worthiness; and
(ii) that is not court proceedings information about the individual or information about the individual that is entered or recorded on the National Personal Insolvency Index; or
(l) the opinion of a credit provider that the individual has committed, in circumstances specified by the provider, a serious credit infringement in relation to consumer credit provided by the provider to the individual.

6P Meaning of credit reporting business

(1) A credit reporting business is a business or undertaking that involves collecting, holding, using or disclosing personal information about individuals for the purpose of, or for purposes including the purpose of, providing an entity with information about the credit worthiness of an individual.

(2) Subsection (1) applies whether or not the information about the credit worthiness of an individual is:
   (a) provided for profit or reward; or
   (b) provided, or intended to be provided, for the purposes of assessing an application for consumer credit.

(3) In determining whether a business or undertaking carried on by a credit provider is a credit reporting business, disregard the provision of information about the credit worthiness of an individual to a related body corporate by the provider.

(4) Despite subsection (1), a business or undertaking is not a credit reporting business if the business or undertaking is included in a class of businesses or undertakings prescribed by the regulations.
6Q Meaning of default information

Consumer credit defaults

(1) Default information about an individual is information about a payment (including a payment that is wholly or partly a payment of interest) that the individual is overdue in making in relation to consumer credit that has been provided by a credit provider to the individual if:

(a) the individual is at least 60 days overdue in making the payment; and
(b) the provider has given a written notice to the individual informing the individual of the overdue payment and requesting that the individual pay the amount of the overdue payment; and
(c) the provider is not prevented by a statute of limitations from recovering the amount of the overdue payment; and
(d) the amount of the overdue payment is equal to or more than:
   (i) $150; or
   (ii) such higher amount as is prescribed by the regulations.

Guarantor defaults

(2) Default information about an individual is information about a payment that the individual is overdue in making as a guarantor under a guarantee given against any default by a person (the borrower) in repaying all or any of the debt deferred under consumer credit provided by a credit provider to the borrower if:

(a) the provider has given the individual written notice of the borrower’s default that gave rise to the individual’s obligation to make the overdue payment; and
(b) the notice requests that the individual pay the amount of the overdue payment; and
(c) at least 60 days have passed since the day on which the notice was given; and
Part II Interpretation

Division 2 Key definitions relating to credit reporting

Section 6R

(d) in addition to giving the notice, the provider has taken other steps to recover the amount of the overdue payment from the individual; and
(e) the provider is not prevented by a statute of limitations from recovering the amount of the overdue payment.

6R Meaning of information request

Credit provider

(1) A credit provider has made an information request in relation to an individual if the provider has sought information about the individual from a credit reporting body:
   (a) in connection with an application for consumer credit made by the individual to the provider; or
   (b) in connection with an application for commercial credit made by a person to the provider; or
   (c) for a credit guarantee purpose of the provider in relation to the individual; or
   (d) for a securitisation related purpose of the provider in relation to the individual.

Mortgage insurer

(2) A mortgage insurer has made an information request in relation to an individual if:
   (a) the insurer has sought information about the individual from a credit reporting body; and
   (b) the information was sought in connection with the provision of insurance to a credit provider in relation to mortgage credit provided by the provider to:
      (i) the individual; or
      (ii) a person for whom the individual is, or is proposing to be, a guarantor.
Trade insurer

(3) A trade insurer has made an information request in relation to an individual if:

(a) the insurer has sought information about the individual from a credit reporting body; and

(b) the information was sought in connection with the provision of insurance to a credit provider in relation to commercial credit provided by the provider to the individual or another person.

6S Meaning of new arrangement information

Consumer credit defaults

(1) If:

(a) a credit provider has disclosed default information about an individual to a credit reporting body; and

(b) the default information relates to a payment that the individual is overdue in making in relation to consumer credit (the original consumer credit) that has been provided by the provider to the individual; and

(c) because of the individual being so overdue:

(i) the terms or conditions of the original consumer credit that relate to the repayment of the amount of credit are varied; or

(ii) the individual is provided with other consumer credit (the new consumer credit) by a credit provider that relates, wholly or in part, to that amount of credit;

then new arrangement information about the individual is a statement that those terms or conditions of the original consumer credit have been varied, or that the individual has been provided with the new consumer credit.

Serious credit infringements

(2) If:
Part II Interpretation
Division 2 Key definitions relating to credit reporting

Section 6T

(a) a credit provider is of the opinion that an individual has committed a serious credit infringement in relation to consumer credit (the *original consumer credit*) provided by the provider to the individual; and

(b) the provider has disclosed the opinion to a credit reporting body; and

(c) because of the provider having that opinion:
   (i) the terms or conditions of the original consumer credit that relate to the repayment of the amount of credit are varied; or
   (ii) the individual is provided with other consumer credit (the *new consumer credit*) by a credit provider that relates, wholly or in part, to that amount of credit;

then *new arrangement information* about the individual is a statement that those terms or conditions of the original consumer credit have been varied, or that the individual has been provided with the new consumer credit.

6T Meaning of payment information

If:

(a) a credit provider has disclosed default information about an individual to a credit reporting body; and

(b) on a day after the default information was disclosed, the amount of the overdue payment to which the information relates is paid;

then *payment information* about the individual is a statement that the amount of the overdue payment has been paid on that day.

6U Meaning of personal insolvency information

(1) *Personal insolvency information* about an individual is information:

(a) that is entered or recorded in the National Personal Insolvency Index; and

(b) that relates to:
(i) a bankruptcy of the individual; or
(ii) a debt agreement proposal given by the individual; or
(iii) a debt agreement made by the individual; or
(iv) a personal insolvency agreement executed by the individual; or
(v) a direction given, or an order made, under section 50 of the Bankruptcy Act that relates to the property of the individual; or
(vi) an authority signed under section 188 of that Act that relates to the property of the individual.

(2) Despite subparagraph (1)(b)(i), personal insolvency information about an individual must not relate to:
   (a) the presentation of a creditor’s petition against the individual; or
   (b) an administration under Part XI of the Bankruptcy Act of the individual’s estate.

(3) An expression used in paragraph (1)(b) or (2)(a) that is also used in the Bankruptcy Act has the same meaning in that paragraph as it has in that Act.

6V Meaning of repayment history information

(1) If a credit provider provides consumer credit to an individual, the following information about the consumer credit is repayment history information about the individual:
   (a) whether or not the individual has met an obligation to make a monthly payment that is due and payable in relation to the consumer credit;
   (b) the day on which the monthly payment is due and payable;
   (c) if the individual makes the monthly payment after the day on which the payment is due and payable—the day on which the individual makes that payment.

(2) The regulations may make provision in relation to:
Part II  Interpretation
Division 2  Key definitions relating to credit reporting

Section 6V

(a) whether or not an individual has met an obligation to make a monthly payment that is due and payable in relation to consumer credit; and
(b) whether or not a payment is a monthly payment.
Division 3—Other matters

7 Acts and practices of agencies, organisations etc.

(1) Except so far as the contrary intention appears, a reference in this Act (other than section 8) to an act or to a practice is a reference to:

(a) an act done, or a practice engaged in, as the case may be, by an agency (other than an eligible hearing service provider), a file number recipient, a credit reporting body or a credit provider other than:

(i) an agency specified in any of the following provisions of the *Freedom of Information Act 1982*:

(A) Schedule 1;
(B) Division 1 of Part I of Schedule 2;
(C) Division 1 of Part II of Schedule 2; or

(ii) a federal court; or
(iiia) a court of Norfolk Island; or

(iii) a Minister; or

(iiiia) the Integrity Commissioner; or

(iv) the ACC; or

(v) a Royal Commission; or

(vi) a Commission of inquiry; or

(b) an act done, or a practice engaged in, as the case may be, by a federal court or by an agency specified in Schedule 1 to the *Freedom of Information Act 1982*, being an act done, or a practice engaged in, in respect of a matter of an administrative nature; or

(ba) an act done, or a practice engaged in, as the case may be, by a court of Norfolk Island, being an act done, or a practice engaged in, in respect of a matter of an administrative nature; or

(bca) an act done, or a practice engaged in, as the case may be, by an agency specified in Division 1 of Part II of Schedule 2 to the *Freedom of Information Act 1982*, other than an act done,
Section 7

or a practice engaged in, in relation to a record in relation to which the agency is exempt from the operation of that Act; or

(ca) an act done, or a practice engaged in, as the case may be, by a part of the Defence Department specified in Division 2 of Part I of Schedule 2 to the *Freedom of Information Act 1982*, other than an act done, or a practice engaged in, in relation to the activities of that part of the Department; or

(cc) an act done, or a practice engaged in, as the case may be, by an eligible hearing service provider in connection with the provision of hearing services under an agreement made under Part 3 of the *Hearing Services Administration Act 1997*; or

(d) an act done, or a practice engaged in, as the case may be, by a Minister in relation to the affairs of an agency (other than a Norfolk Island agency or an eligible hearing service provider), not being an act done, or a practice engaged in, in relation to an existing record; or

(e) an act done, or a practice engaged in, as the case may be, by a Minister in relation to a record that is in the Minister’s possession in his or her capacity as a Minister and relates to the affairs of an agency (other than a Norfolk Island agency or an eligible hearing service provider); or

(ec) an act done, or a practice engaged in, as the case may be, by a Minister in relation to the affairs of an eligible hearing service provider, being affairs in connection with the provision of hearing services under an agreement made under Part 3 of the *Hearing Services Administration Act 1997*; or

(ed) an act done, or a practice engaged in, as the case may be, by a Minister in relation to a record that is in the Minister’s possession in his or her capacity as a Minister and relates to the affairs of an eligible hearing service provider, being affairs in connection with the provision of hearing services under an agreement made under Part 3 of the *Hearing Services Administration Act 1997*; or

(ee) an act done, or a practice engaged in, by an organisation, other than an exempt act or exempt practice (see sections 7B and 7C);
Interpretation  Part II
Other matters  Division 3

Section 7

but does not include a reference to an act done, or a practice engaged in, in relation to a record that has originated with, or has been received from:

(f) an intelligence agency;
(g) the Defence Intelligence Organisation or the Australian Geospatial-Intelligence Organisation; or
(ga) the Integrity Commissioner or a staff member of ACLEI (within the meaning of the Law Enforcement Integrity Commissioner Act 2006); or
(h) the ACC or the Board of the ACC.

(1A) Despite subsections (1) and (2), a reference in this Act (other than section 8) to an act or to a practice does not include a reference to the act or practice so far as it involves the disclosure of personal information to:

(a) the Australian Security Intelligence Organisation; or
(b) the Australian Secret Intelligence Service; or
(c) the Australian Signals Directorate.

(2) Except so far as the contrary intention appears, a reference in this Act (other than section 8) to an act or to a practice includes, in the application of this Act otherwise than in respect of the Australian Privacy Principles, a registered APP code and the performance of the Commissioner’s functions in relation to the principles and such a code, a reference to an act done, or a practice engaged in, as the case may be, by an agency specified in Part I of Schedule 2 to the Freedom of Information Act 1982 or in Division 1 of Part II of that Schedule other than:

(a) an intelligence agency;
(b) the Defence Intelligence Organisation or the Australian Geospatial-Intelligence Organisation; or
(c) the ACC or the Board of the ACC.

(3) Except so far as the contrary intention appears, a reference in this Act to doing an act includes a reference to:

(a) doing an act in accordance with a practice; or
(b) refusing or failing to do an act.
Part II Interpretation
Division 3 Other matters

Section 7A

(4) For the purposes of section 28, of paragraphs 28A(2)(a) to (e), of subsection 31(2) and of Part VI, this section has effect as if a reference in subsection (1) of this section to an act done, or to a practice engaged in, included a reference to an act that is proposed to be done, or to a practice that is proposed to be engaged in, as the case may be.

7A Acts of certain agencies treated as acts of organisation

(1) This Act applies, with the prescribed modifications (if any), in relation to an act or practice described in subsection (2) or (3) as if:
   (a) the act or practice were an act done, or practice engaged in, by an organisation; and
   (b) the agency mentioned in that subsection were the organisation.

(2) Subsection (1) applies to acts done, and practices engaged in, by a prescribed agency. Regulations for this purpose may prescribe an agency only if it is specified in Part I of Schedule 2 to the Freedom of Information Act 1982.

(3) Subsection (1) also applies to acts and practices that:
   (a) are done or engaged in by an agency specified in Division 1 of Part II of Schedule 2 to the Freedom of Information Act 1982 in relation to documents in respect of its commercial activities or the commercial activities of another entity; and
   (b) relate to those commercial activities.

(4) This section has effect despite subparagraph 7(1)(a)(i), paragraph 7(1)(c) and subsection 7(2).

7B Exempt acts and exempt practices of organisations

Individuals in non-business capacity

(1) An act done, or practice engaged in, by an organisation that is an individual is exempt for the purposes of paragraph 7(1)(ee) if the
act is done, or the practice is engaged in, other than in the course of a business carried on by the individual.

Note: See also section 16 which provides that the Australian Privacy Principles do not apply for the purposes of, or in connection with, an individual’s personal, family or household affairs.

**Organisation acting under Commonwealth contract**

(2) An act done, or practice engaged in, by an organisation is *exempt* for the purposes of paragraph 7(1)(ee) if:

(a) the organisation is a contracted service provider for a Commonwealth contract (whether or not the organisation is a party to the contract); and

(b) the organisation would be a small business operator if it were not a contracted service provider for a Commonwealth contract; and

(c) the act is done, or the practice is engaged in, otherwise than for the purposes of meeting (directly or indirectly) an obligation under a Commonwealth contract for which the organisation is the contracted service provider.

Note: This puts the organisation in the same position as a small business operator as far as its activities that are not for the purposes of a Commonwealth contract are concerned, so the organisation need not comply with the Australian Privacy Principles, or a registered APP code that binds the organisation, in relation to those activities.

**Employee records**

(3) An act done, or practice engaged in, by an organisation that is or was an employer of an individual, is *exempt* for the purposes of paragraph 7(1)(ee) if the act or practice is directly related to:

(a) a current or former employment relationship between the employer and the individual; and

(b) an employee record held by the organisation and relating to the individual.
Part II Interpretation
Division 3 Other matters

Section 7C

Journalism

(4) An act done, or practice engaged in, by a media organisation is exempt for the purposes of paragraph 7(1)(ee) if the act is done, or the practice is engaged in:
(a) by the organisation in the course of journalism; and
(b) at a time when the organisation is publicly committed to observe standards that:
   (i) deal with privacy in the context of the activities of a media organisation (whether or not the standards also deal with other matters); and
   (ii) have been published in writing by the organisation or a person or body representing a class of media organisations.

Organisation acting under State contract

(5) An act done, or practice engaged in, by an organisation is exempt for the purposes of paragraph 7(1)(ee) if:
(a) the organisation is a contracted service provider for a State contract (whether or not the organisation is a party to the contract); and
(b) the act is done, or the practice is engaged in for the purposes of meeting (directly or indirectly) an obligation under the contract.

7C Political acts and practices are exempt

Members of a Parliament etc.

(1) An act done, or practice engaged in, by an organisation (the political representative) consisting of a member of a Parliament, or a councillor (however described) of a local government authority, is exempt for the purposes of paragraph 7(1)(ee) if the act is done, or the practice is engaged in, for any purpose in connection with:
(a) an election under an electoral law; or
(b) a referendum under a law of the Commonwealth or a law of a State or Territory; or

Privacy Act 1988

Compilation No. 78 Compilation date: 1/7/18 Registered: 30/7/18

Authorised Version C2018C00292 registered 30/07/2018
(c) the participation by the political representative in another aspect of the political process.

Contracts for political representatives etc.

(2) An act done, or practice engaged in, by an organisation (the contractor) is exempt for the purposes of paragraph 7(1)(ee) if the act is done or the practice is engaged in:

(a) for the purposes of meeting an obligation under a contract between the contractor and a registered political party or a political representative described in subsection (1); and

(b) for any purpose in connection with one or more of the following:

(i) an election under an electoral law;

(ii) a referendum under a law of the Commonwealth or a law of a State or Territory;

(iii) the participation in another aspect of the political process by the registered political party or political representative;

(iv) facilitating acts or practices of the registered political party or political representative for a purpose mentioned in subparagraph (i), (ii) or (iii) of this paragraph.

Subcontractors for organisations covered by subsection (1) etc.

(3) An act done, or practice engaged in, by an organisation (the subcontractor) is exempt for the purposes of paragraph 7(1)(ee) if the act is done or the practice is engaged in:

(a) for the purposes of meeting an obligation under a contract between the subcontractor and a contractor described in subsection (2); and

(b) for a purpose described in paragraph (2)(b).

Volunteers for registered political parties

(4) An act done voluntarily, or practice engaged in voluntarily, by an organisation for or on behalf of a registered political party and with the authority of the party is exempt for the purposes of...
Part II Interpretation
Division 3 Other matters

Section 8

paragraph 7(1)(ee) if the act is done or the practice is engaged in for any purpose in connection with one or more of the following:

(a) an election under an electoral law;
(b) a referendum under a law of the Commonwealth or a law of a State or Territory;
(c) the participation in another aspect of the political process by the registered political party;
(d) facilitating acts or practices of the registered political party for a purpose mentioned in paragraph (a), (b) or (c).

Effect of subsection (4) on other operation of Act

(5) Subsection (4) does not otherwise affect the operation of the Act in relation to agents or principals.

Meaning of electoral law and Parliament

(6) In this section:

electoral law means a law of the Commonwealth, or a law of a State or Territory, relating to elections to a Parliament or to a local government authority.

Parliament means:

(a) the Parliament of the Commonwealth; or
(b) a State Parliament; or
(c) the legislature of a Territory.

Note: To avoid doubt, this section does not make exempt for the purposes of paragraph 7(1)(ee) an act or practice of the political representative, contractor, subcontractor or volunteer for a registered political party involving the use or disclosure (by way of sale or otherwise) of personal information in a way not covered by subsection (1), (2), (3) or (4) (as appropriate). The rest of this Act operates normally in relation to that act or practice.

8 Acts and practices of, and disclosure of information to, staff of agency, organisation etc.

(1) For the purposes of this Act:
(a) an act done or practice engaged in by, or information disclosed to, a person employed by, or in the service of, an agency, organisation, file number recipient, credit reporting body or credit provider in the performance of the duties of the person’s employment shall be treated as having been done or engaged in by, or disclosed to, the agency, organisation, recipient, credit reporting body or credit provider;

(b) an act done or practice engaged in by, or information disclosed to, a person on behalf of, or for the purposes of the activities of, an unincorporated body, being a board, council, committee, sub-committee or other body established by or under a Commonwealth enactment or a Norfolk Island enactment for the purpose of assisting, or performing functions in connection with, an agency or organisation, shall be treated as having been done or engaged in by, or disclosed to, the agency or organisation; and

(c) an act done or practice engaged in by, or information disclosed to, a member, staff member or special member of the Australian Federal Police in the performance of his or her duties as such a member, staff member or special member shall be treated as having been done or engaged in by, or disclosed to, the Australian Federal Police.

(2) Where:

(a) an act done or a practice engaged in by a person, in relation to a record, is to be treated, under subsection (1), as having been done or engaged in by an agency; and

(b) that agency does not hold that record;

that act or practice shall be treated as the act or the practice of the agency that holds that record.

(3) For the purposes of the application of this Act in relation to an organisation that is a partnership:

(a) an act done or practice engaged in by a partner is taken to have been done or engaged in by the organisation; and
Part II Interpretation
Division 3 Other matters

Section 10

(b) a communication (including a complaint, notice, request or disclosure of information) made to a partner is taken to have been made to the organisation.

(4) For the purposes of the application of this Act in relation to an organisation that is an unincorporated association:
   (a) an act done or practice engaged in by a member of the committee of management of the association is taken to have been done or engaged in by the organisation; and
   (b) a communication (including a complaint, notice, request or disclosure of information) made to a member of the committee of management of the association is taken to have been made to the organisation.

(5) For the purposes of the application of this Act in relation to an organisation that is a trust:
   (a) an act done or practice engaged in by a trustee is taken to have been done or engaged in by the organisation; and
   (b) a communication (including a complaint, notice or request or disclosure of information) made to a trustee is taken to have been made to the organisation.

10 Agencies that are taken to hold a record

(4) Where:
   (a) a record of personal information (not being a record relating to the administration of the National Archives of Australia) is in the care (within the meaning of the *Archives Act 1983*) of the National Archives of Australia; or
   (b) a record of personal information (not being a record relating to the administration of the Australian War Memorial) is in the custody of the Australian War Memorial;
   the agency by or on behalf of which the record was placed in that care or custody or, if that agency no longer exists, the agency to whose functions the contents of the record are most closely related, shall be regarded, for the purposes of this Act, to be the agency that holds that record.
(5) Where a record of personal information was placed by or on behalf of an agency in the memorial collection within the meaning of the Australian War Memorial Act 1980, that agency or, if that agency no longer exists, the agency to whose functions the contents of the record are most closely related, shall be regarded, for the purposes of this Act, to be the agency that holds that record.

11 File number recipients

(1) A person who is (whether lawfully or unlawfully) in possession or control of a record that contains tax file number information shall be regarded, for the purposes of this Act, as a file number recipient.

(2) Subject to subsection (3), where a record that contains tax file number information is in the possession or under the control of a person:

(a) in the course of the person’s employment in the service of or by a person or body other than an agency;
(b) in the course of the person’s employment in the service of or by an agency other than the Australian Federal Police; or
(c) as a member, staff member or special member of the Australian Federal Police in the performance of his or her duties as such a member, staff member or special member;

then, for the purposes of this Act, the file number recipient in relation to that record shall be taken to be:

(d) if paragraph (a) applies—the person’s employer;
(e) if paragraph (b) applies—the agency first referred to in that paragraph; and
(f) if paragraph (c) applies—the Australian Federal Police.

(3) Where a record that contains tax file number information is in the possession or under the control of a person for the purposes of the activities of an unincorporated body, being a board, council, committee, sub-committee or other body established by or under a Commonwealth enactment or a Norfolk Island enactment for the purpose of assisting, or performing functions connected with, an agency, that agency shall be treated, for the purposes of this Act, as the file number recipient in relation to that record.
Section 12A

12A Act not to apply in relation to State banking or insurance within that State

Where, but for this section, a provision of this Act:

(a) would have a particular application; and

(b) by virtue of having that application, would be a law with respect to, or with respect to matters including:

(i) State banking not extending beyond the limits of the State concerned; or

(ii) State insurance not extending beyond the limits of the State concerned;

the provision is not to have that application.

12B Severability—additional effect of this Act

(1) Without limiting its effect apart from this section, this Act has effect in relation to the following (the regulated entities) as provided by this section:

(a) an agency;

(b) an organisation;

(c) a small business operator;

(d) a body politic.

Note: Subsection 27(4) applies in relation to an investigation of an act or practice referred to in subsection 29(1) of the Healthcare Identifiers Act 2010.

(2) This Act also has the effect it would have if its operation in relation to regulated entities were expressly confined to an operation to give effect to the following:

(a) the International Covenant on Civil and Political Rights done at New York on 16 December 1966 ([1980] ATS 23), and in particular Articles 17 and 24(1) of the Covenant;


Note: In 2012, the text of the Covenant and Convention in the Australian Treaty Series was accessible through the Australian Treaties Library on the AustLII website (www.austlii.edu.au).
(3) This Act also has the effect it would have if its operation in relation to regulated entities were expressly confined to acts or practices covered by section 5B (which deals with acts and practices outside Australia and the external Territories).

(4) This Act also has the effect it would have if its operation in relation to regulated entities were expressly confined to regulated entities that are corporations.

(5) This Act also has the effect it would have if its operation in relation to regulated entities were expressly confined to acts or practices of regulated entities taking place in the course of, or in relation to, trade or commerce:
   (a) between Australia and places outside Australia; or
   (b) among the States; or
   (c) within a Territory, between a State and a Territory or between 2 Territories.

(5A) This Act also has the effect it would have if its operation in relation to regulated entities were expressly confined to acts or practices engaged in by regulated entities in the course of:
   (a) banking (other than State banking not extending beyond the limits of the State concerned); or
   (b) insurance (other than State insurance not extending beyond the limits of the State concerned).

(6) This Act also has the effect it would have if its operation in relation to regulated entities were expressly confined to acts or practices of regulated entities taking place using a postal, telegraphic, telephonic or other like service within the meaning of paragraph 51(v) of the Constitution.

(7) This Act also has the effect it would have if its operation in relation to regulated entities were expressly confined to acts or practices of regulated entities taking place in a Territory.

(8) This Act also has the effect it would have if its operation in relation to regulated entities were expressly confined to acts or practices of
Part II Interpretation
Division 3 Other matters

Section 12B

regulated entities taking place in a place acquired by the Commonwealth for public purposes.
Part III—Information privacy

Division 1—Interferences with privacy

13 Interferences with privacy

APP entities

(1) An act or practice of an APP entity is an interference with the privacy of an individual if:
   (a) the act or practice breaches an Australian Privacy Principle in relation to personal information about the individual; or
   (b) the act or practice breaches a registered APP code that binds the entity in relation to personal information about the individual.

Credit reporting

(2) An act or practice of an entity is an interference with the privacy of an individual if:
   (a) the act or practice breaches a provision of Part IIIA in relation to personal information about the individual; or
   (b) the act or practice breaches the registered CR code in relation to personal information about the individual and the code binds the entity.

Contracted service providers

(3) An act or practice of an organisation is an interference with the privacy of an individual if:
   (a) the act or practice relates to personal information about the individual; and
   (b) the organisation is a contracted service provider for a Commonwealth contract (whether or not the organisation is a party to the contract); and
   (c) the act or practice does not breach:
Part III  Information privacy
Division 1  Interferences with privacy

Section 13

(i) an Australian Privacy Principle; or
(ii) a registered APP code that binds the organisation;
in relation to the personal information because of a provision
of the contract that is inconsistent with the principle or code;
and
(d) the act is done, or the practice is engaged in, in a manner
contrary to, or inconsistent with, that provision.

Note: See subsections 6A(2) and 6B(2) for when an act or practice does not
breach an Australian Privacy Principle or a registered APP code.

Tax file numbers

(4) An act or practice is an interference with the privacy of an
individual if:
(a) it is an act or practice of a file number recipient and the act or
practice breaches a rule issued under section 17 in relation to
tax file number information that relates to the individual; or
(b) the act or practice involves an unauthorised requirement or
request for disclosure of the tax file number of the individual.

Notification of eligible data breaches etc.

(4A) If an entity (within the meaning of Part IIIC) contravenes
subsection 26WH(2), 26WK(2), 26WL(3) or 26WR(10), the
contravention is taken to be an act that is an interference with the
privacy of an individual.

Other interferences with privacy

(5) An act or practice is an interference with the privacy of an
individual if the act or practice:
(a) constitutes a breach of Part 2 of the Data-matching Program
(Assistance and Tax) Act 1990 or the rules issued under
section 12 of that Act; or
(b) constitutes a breach of the rules issued under section 135AA
of the National Health Act 1953.

Note: Other Acts may provide that an act or practice is an interference with
the privacy of an individual. For example, see the Healthcare
13B Related bodies corporate

Acts or practices that are not interferences with privacy

(1) Despite subsection 13(1), each of the following acts or practices of an organisation that is a body corporate is not an interference with the privacy of an individual:

(a) the collection of personal information (other than sensitive information) about the individual by the body corporate from a related body corporate;

(b) the disclosure of personal information (other than sensitive information) about the individual by the body corporate to a related body corporate.

Note: Subsection (1) lets related bodies corporate share personal information. However, in using or holding the information, they must comply with the Australian Privacy Principles and a registered APP code that binds them. For example, there is an interference with privacy if:

(a) a body corporate uses personal information it has collected from a related body corporate; and

(b) the use breaches Australian Privacy Principle 6 (noting that the collecting body’s primary purpose of collection will be taken to be the same as that of the related body).

(1A) However, paragraph (1)(a) does not apply to the collection by a body corporate of personal information (other than sensitive information) from:

(a) a related body corporate that is not an organisation; or

(b) a related body corporate whose disclosure of the information to the body corporate is an exempt act or exempt practice for the purposes of paragraph 7(1)(ee); or

(c) a related body corporate whose disclosure of the information to the body corporate is not an interference with privacy because of section 13D.
Part III Information privacy
Division 1 Interferences with privacy

Section 13C

Note: The effect of subsection (1A) is that a body corporate’s failure to comply with the Australian Privacy Principles, or a registered APP code that binds the body, in collecting personal information about an individual from a related body corporate covered by that subsection is an interference with the privacy of the individual.

Relationship with subsection 13(3)

(2) Subsection (1) does not prevent an act or practice of an organisation from being an interference with the privacy of an individual under subsection 13(3).

13C Change in partnership because of change in partners

Acts or practices that are not interferences with privacy

(1) If:

(a) an organisation (the new partnership) that is a partnership forms at the same time as, or immediately after, the dissolution of another partnership (the old partnership); and

(b) at least one person who was a partner in the old partnership is a partner in the new partnership; and

(c) the new partnership carries on a business that is the same as, or similar to, a business carried on by the old partnership; and

(d) the new partnership holds, immediately after its formation, personal information about an individual that the old partnership held immediately before its dissolution;

neither the disclosure (if any) by the old partnership, nor the collection (if any) by the new partnership, of the information that was necessary for the new partnership to hold the information immediately after its formation constitutes an interference with the privacy of the individual.

Note: Subsection (1) lets personal information be passed on from an old to a new partnership. However, in using or holding the information, they must comply with the Australian Privacy Principles and a registered APP code that binds them. For example, the new partnership’s use of personal information collected from the old partnership may constitute an interference with privacy if it breaches Australian Privacy Principle 6.
Section 13D

Effect of subsection (1)

(2) Subsection (1) has effect despite subsections 13(1) and (3).

13D Overseas act required by foreign law

Acts or practices that are not interferences with privacy

(1) An act or practice of an organisation done or engaged in outside Australia and an external Territory is not an interference with the privacy of an individual if the act or practice is required by an applicable law of a foreign country.

Effect of subsection (1)

(2) Subsection (1) has effect despite subsections 13(1) and (3).

13E Effect of sections 13B, 13C and 13D

Sections 13B, 13C and 13D do not prevent an act or practice of an organisation from being an interference with the privacy of an individual under subsection 13(2), (4) or (5).

13F Act or practice not covered by section 13 is not an interference with privacy

An act or practice that is not covered by section 13 is not an interference with the privacy of an individual.

13G Serious and repeated interferences with privacy

An entity contravenes this subsection if:

(a) the entity does an act, or engages in a practice, that is a serious interference with the privacy of an individual; or

(b) the entity repeatedly does an act, or engages in a practice, that is an interference with the privacy of one or more individuals.

Civil penalty: 2,000 penalty units.
Part III  Information privacy
Division 2  Australian Privacy Principles

Section 14

Division 2—Australian Privacy Principles

14 Australian Privacy Principles

(1) The Australian Privacy Principles are set out in the clauses of Schedule 1.

(2) A reference in any Act to an Australian Privacy Principle by a number is a reference to the Australian Privacy Principle with that number.

15 APP entities must comply with Australian Privacy Principles

An APP entity must not do an act, or engage in a practice, that breaches an Australian Privacy Principle.

16 Personal, family or household affairs

Nothing in the Australian Privacy Principles applies to:

(a) the collection, holding, use or disclosure of personal information by an individual; or
(b) personal information held by an individual; only for the purposes of, or in connection with, his or her personal, family or household affairs.

16A Permitted general situations in relation to the collection, use or disclosure of personal information

(1) A permitted general situation exists in relation to the collection, use or disclosure by an APP entity of personal information about an individual, or of a government related identifier of an individual, if:

(a) the entity is an entity of a kind specified in an item in column 1 of the table; and
(b) the item in column 2 of the table applies to the information or identifier; and
Section 16A

(c) such conditions as are specified in the item in column 3 of the table are satisfied.

<table>
<thead>
<tr>
<th>Item</th>
<th>Column 1</th>
<th>Column 2</th>
<th>Column 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>APP entity</td>
<td>(a) personal information; or (b) a government related identifier.</td>
<td>(a) it is unreasonable or impracticable to obtain the individual’s consent to the collection, use or disclosure; and (b) the entity reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.</td>
</tr>
<tr>
<td>2</td>
<td>APP entity</td>
<td>(a) personal information; or (b) a government related identifier.</td>
<td>(a) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity’s functions or activities has been, is being or may be engaged in; and (b) the entity reasonably believes that the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter.</td>
</tr>
<tr>
<td>3</td>
<td>APP entity</td>
<td>Personal information</td>
<td>(a) the entity reasonably believes that the collection, use or disclosure is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing; and (b) the collection, use or disclosure complies with the rules made under subsection (2).</td>
</tr>
</tbody>
</table>
### Section 16A

#### Permitted general situations

<table>
<thead>
<tr>
<th>Item</th>
<th>Column 1</th>
<th>Column 2 Item applies to</th>
<th>Column 3 Condition(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>APP entity</td>
<td>Personal information</td>
<td>The collection, use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim.</td>
</tr>
<tr>
<td>5</td>
<td>APP entity</td>
<td>Personal information</td>
<td>The collection, use or disclosure is reasonably necessary for the purposes of a confidential alternative dispute resolution process.</td>
</tr>
<tr>
<td>6</td>
<td>Agency</td>
<td>Personal information</td>
<td>The entity reasonably believes that the collection, use or disclosure is necessary for the entity’s diplomatic or consular functions or activities.</td>
</tr>
<tr>
<td>7</td>
<td>Defence Force</td>
<td>Personal information</td>
<td>The entity reasonably believes that the collection, use or disclosure is necessary for any of the following occurring outside Australia and the external Territories: (a) war or warlike operations; (b) peacekeeping or peace enforcement; (c) civil aid, humanitarian assistance, medical or civil emergency or disaster relief.</td>
</tr>
</tbody>
</table>

(2) The Commissioner may, by legislative instrument, make rules relating to the collection, use or disclosure of personal information that apply for the purposes of item 3 of the table in subsection (1).
16B Permitted health situations in relation to the collection, use or disclosure of health information

Collection—provision of a health service

(1) A permitted health situation exists in relation to the collection by an organisation of health information about an individual if:

(a) the information is necessary to provide a health service to the individual; and

(b) either:

(i) the collection is required or authorised by or under an Australian law (other than this Act); or

(ii) the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

(1A) A permitted health situation exists in relation to the collection by an organisation of health information about an individual (the third party) if:

(a) it is necessary for the organisation to collect the family, social or medical history of an individual (the patient) to provide a health service to the patient; and

(b) the health information about the third party is part of the family, social or medical history necessary for the organisation to provide the health service to the patient; and

(c) the health information is collected by the organisation from the patient or, if the patient is physically or legally incapable of giving the information, a responsible person for the patient.

Collection—research etc.

(2) A permitted health situation exists in relation to the collection by an organisation of health information about an individual if:

(a) the collection is necessary for any of the following purposes:

(i) research relevant to public health or public safety;
Part III  Information privacy
Division 2  Australian Privacy Principles

Section 16B

(ii) the compilation or analysis of statistics relevant to public health or public safety;

(iii) the management, funding or monitoring of a health service; and

(b) that purpose cannot be served by the collection of information about the individual that is de-identified information; and

(c) it is impracticable for the organisation to obtain the individual’s consent to the collection; and

(d) any of the following apply:

(i) the collection is required by or under an Australian law (other than this Act);

(ii) the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation;

(iii) the information is collected in accordance with guidelines approved under section 95A for the purposes of this subparagraph.

Use or disclosure—research etc.

(3) A permitted health situation exists in relation to the use or disclosure by an organisation of health information about an individual if:

(a) the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety; and

(b) it is impracticable for the organisation to obtain the individual’s consent to the use or disclosure; and

(c) the use or disclosure is conducted in accordance with guidelines approved under section 95A for the purposes of this paragraph; and

(d) in the case of disclosure—the organisation reasonably believes that the recipient of the information will not disclose the information, or personal information derived from that information.
Use or disclosure—genetic information

(4) A permitted health situation exists in relation to the use or disclosure by an organisation of genetic information about an individual (the first individual) if:

(a) the organisation has obtained the information in the course of providing a health service to the first individual; and

(b) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another individual who is a genetic relative of the first individual; and

(c) the use or disclosure is conducted in accordance with guidelines approved under section 95AA; and

(d) in the case of disclosure—the recipient of the information is a genetic relative of the first individual.

Disclosure—responsible person for an individual

(5) A permitted health situation exists in relation to the disclosure by an organisation of health information about an individual if:

(a) the organisation provides a health service to the individual; and

(b) the recipient of the information is a responsible person for the individual; and

(c) the individual:

(i) is physically or legally incapable of giving consent to the disclosure; or

(ii) physically cannot communicate consent to the disclosure; and

(d) another individual (the carer) providing the health service for the organisation is satisfied that either:

(i) the disclosure is necessary to provide appropriate care or treatment of the individual; or

(ii) the disclosure is made for compassionate reasons; and

(e) the disclosure is not contrary to any wish:
Part III  Information privacy  
Division 2  Australian Privacy Principles 

Section 16C 

(i) expressed by the individual before the individual became unable to give or communicate consent; and  
(ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware; and  
(f) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (d). 

16C Acts and practices of overseas recipients of personal information  

(1) This section applies if:  
(a) an APP entity discloses personal information about an individual to an overseas recipient; and  
(b) Australian Privacy Principle 8.1 applies to the disclosure of the information; and  
(c) the Australian Privacy Principles do not apply, under this Act, to an act done, or a practice engaged in, by the overseas recipient in relation to the information; and  
(d) the overseas recipient does an act, or engages in a practice, in relation to the information that would be a breach of the Australian Privacy Principles (other than Australian Privacy Principle 1) if those Australian Privacy Principles so applied to that act or practice. 

(2) The act done, or the practice engaged in, by the overseas recipient is taken, for the purposes of this Act:  
(a) to have been done, or engaged in, by the APP entity; and  
(b) to be a breach of those Australian Privacy Principles by the APP entity.
Division 4—Tax file number information

17 Rules relating to tax file number information

The Commissioner must, by legislative instrument, issue rules concerning the collection, storage, use and security of tax file number information.

18 File number recipients to comply with rules

A file number recipient shall not do an act, or engage in a practice, that breaches a rule issued under section 17.
Part IIIA—Credit reporting

Division 1—Introduction

19 Guide to this Part

In general, this Part deals with the privacy of information relating to credit reporting.

Divisions 2 and 3 contain rules that apply to credit reporting bodies and credit providers in relation to their handling of information relating to credit reporting.

Division 4 contains rules that apply to affected information recipients in relation to their handling of their regulated information.

Division 5 deals with complaints to credit reporting bodies or credit providers about acts or practices that may be a breach of certain provisions of this Part or the registered CR code.

Division 6 deals with entities that obtain credit reporting information or credit eligibility information by false pretence, or when they are not authorised to do so under this Part.

Division 7 provides for compensation orders, and other orders, to be made by the Federal Court or Federal Circuit Court.
Division 2—Credit reporting bodies

Subdivision A—Introduction and application of this Division etc.

20 Guide to this Division

This Division sets out rules that apply to credit reporting bodies in relation to their handling of the following:

(a) credit reporting information;
(b) CP derived information;
(c) credit reporting information that is de-identified;
(d) a pre-screening assessment.

The rules apply in relation to that kind of information or assessment instead of the Australian Privacy Principles.

20A Application of this Division and the Australian Privacy Principles to credit reporting bodies

(1) This Division applies to a credit reporting body in relation to the following:
(a) credit reporting information;
(b) CP derived information;
(c) credit reporting information that is de-identified;
(d) a pre-screening assessment.

(2) The Australian Privacy Principles do not apply to a credit reporting body in relation to personal information that is:
(a) credit reporting information; or
(b) CP derived information; or
Part IIIA Credit reporting
Division 2 Credit reporting bodies

Section 20B

(c) a pre-screening assessment.

Note: The Australian Privacy Principles apply to the credit reporting body in relation to other kinds of personal information.

Subdivision B—Consideration of information privacy

20B Open and transparent management of credit reporting information

(1) The object of this section is to ensure that credit reporting bodies manage credit reporting information in an open and transparent way.

Compliance with this Division etc.

(2) A credit reporting body must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the credit reporting business of the body that:
   (a) will ensure that the body complies with this Division and the registered CR code; and
   (b) will enable the body to deal with inquiries or complaints from individuals about the body’s compliance with this Division or the registered CR code.

Policy about the management of credit reporting information

(3) A credit reporting body must have a clearly expressed and up-to-date policy about the management of credit reporting information by the body.

(4) Without limiting subsection (3), the policy of the credit reporting body must contain the following information:
   (a) the kinds of credit information that the body collects and how the body collects that information;
   (b) the kinds of credit reporting information that the body holds and how the body holds that information;
   (c) the kinds of personal information that the body usually derives from credit information that the body holds;
(d) the purposes for which the body collects, holds, uses and
discloses credit reporting information;
(e) information about the effect of section 20G (which deals with
direct marketing) and how the individual may make a request
under subsection (5) of that section;
(f) how an individual may access credit reporting information
about the individual that is held by the body and seek the
correction of such information;
(g) information about the effect of section 20T (which deals with
individuals requesting the correction of credit information
etc.);
(h) how an individual may complain about a failure of the body
to comply with this Division or the registered CR code and
how the body will deal with such a complaint.

Availability of policy etc.

(5) A credit reporting body must take such steps as are reasonable in
the circumstances to make the policy available:

(a) free of charge; and

(b) in such form as is appropriate.

Note: A credit reporting body will usually make the policy available on the
body’s website.

(6) If a person or body requests a copy, in a particular form, of the
policy of a credit reporting body, the credit reporting body must
take such steps as are reasonable in the circumstances to give the
person or body a copy in that form.

Subdivision C—Collection of credit information

20C Collection of solicited credit information

Prohibition on collection

(1) A credit reporting body must not collect credit information about
an individual.
Part IIIA Credit reporting

Division 2 Credit reporting bodies

Section 20C

Civil penalty: 2,000 penalty units.

Exceptions

(2) Subsection (1) does not apply if the collection of the credit information is required or authorised by or under an Australian law or a court/tribunal order.

(3) Subsection (1) does not apply if:
   (a) the credit reporting body collects the credit information about the individual from a credit provider who is permitted under section 21D to disclose the information to the body; and
   (b) the body collects the information in the course of carrying on a credit reporting business; and
   (c) if the information is identification information about the individual—the body also collects from the provider, or already holds, credit information of another kind about the individual.

(4) Subsection (1) does not apply if:
   (a) the credit reporting body:
      (i) collects the credit information about the individual from an entity (other than a credit provider) in the course of carrying on a credit reporting business; and
      (ii) knows, or believes on reasonable grounds, that the individual is at least 18 years old; and
   (b) the information does not relate to an act, omission, matter or thing that occurred or existed before the individual turned 18; and
   (c) if the information relates to consumer credit or commercial credit—the credit is or has been provided, or applied for, in Australia; and
   (d) if the information is identification information about the individual—the body also collects from the entity, or already holds, credit information of another kind about the individual; and
(e) if the information is repayment history information about the individual—the body collects the information from another credit reporting body that has an Australian link.

(5) Paragraph (4)(b) does not apply to identification information about the individual.

(6) Despite paragraph (4)(b), consumer credit liability information about the individual may relate to consumer credit that was entered into on a day before the individual turned 18, so long as the consumer credit was not terminated, or did not otherwise cease to be in force, on a day before the individual turned 18.

Means of collection

(7) A credit reporting body must collect credit information only by lawful and fair means.

Solicited credit information

(8) This section applies to the collection of credit information that is solicited by a credit reporting body.

20D Dealing with unsolicited credit information

(1) If:
   
   (a) a credit reporting body receives credit information about an individual; and
   
   (b) the body did not solicit the information;

the body must, within a reasonable period after receiving the information, determine whether or not the body could have collected the information under section 20C if the body had solicited the information.

(2) The credit reporting body may use or disclose the credit information for the purposes of making the determination under subsection (1).
(3) If the credit reporting body determines that it could have collected the credit information, sections 20E to 20ZA apply in relation to the information as if the body had collected the information under section 20C.

(4) If the credit reporting body determines that it could not have collected the credit information, the body must, as soon as practicable, destroy the information.

Civil penalty: 1,000 penalty units.

(5) Subsection (4) does not apply if the credit reporting body is required by or under an Australian law, or a court/tribunal order, to retain the credit information.

Subdivision D—Dealing with credit reporting information etc.

20E Use or disclosure of credit reporting information

Prohibition on use or disclosure

(1) If a credit reporting body holds credit reporting information about an individual, the body must not use or disclose the information.

Civil penalty: 2,000 penalty units.

Permitted uses

(2) Subsection (1) does not apply to the use of credit reporting information about the individual if:
   (a) the credit reporting body uses the information in the course of carrying on the body’s credit reporting business; or
   (b) the use is required or authorised by or under an Australian law or a court/tribunal order; or
   (c) the use is a use prescribed by the regulations.
Permitted disclosures

(3) Subsection (1) does not apply to the disclosure of credit reporting information about the individual if:
   (a) the disclosure is a permitted CRB disclosure in relation to the individual; or
   (b) the disclosure is to another credit reporting body that has an Australian link; or
   (c) both of the following apply:
      (i) the disclosure is for the purposes of a recognised external dispute resolution scheme;
      (ii) a credit reporting body or credit provider is a member of the scheme; or
   (d) both of the following apply:
      (i) the disclosure is to an enforcement body;
      (ii) the credit reporting body is satisfied that the body, or another enforcement body, believes on reasonable grounds that the individual has committed a serious credit infringement; or
   (e) the disclosure is required or authorised by or under an Australian law or a court/tribunal order; or
   (f) the disclosure is a disclosure prescribed by the regulations.

(4) However, if the credit reporting information is, or was derived from, repayment history information about the individual, the credit reporting body must not disclose the information under paragraph (3)(a) or (f) unless the recipient of the information is:
   (a) a credit provider who is a licensee or is prescribed by the regulations; or
   (b) a mortgage insurer.

Civil penalty: 2,000 penalty units.

(5) If a credit reporting body discloses credit reporting information under this section, the body must make a written note of that disclosure.

Civil penalty: 500 penalty units.
Part IIIA Credit reporting  
Division 2 Credit reporting bodies

Section 20F

Note: Other Acts may provide that the note must not be made (see for example the Australian Crime Commission Act 2002 and the Law Enforcement Integrity Commissioner Act 2006).

No use or disclosure for the purposes of direct marketing

(6) This section does not apply to the use or disclosure of credit reporting information for the purposes of direct marketing.

Note: Section 20G deals with the use or disclosure of credit reporting information for the purposes of direct marketing.

20F Permitted CRB disclosures in relation to individuals

(1) A disclosure by a credit reporting body of credit reporting information about an individual is a permitted CRB disclosure in relation to the individual if:

(a) the disclosure is to an entity that is specified in an item of the table and that has an Australian link; and

(b) such conditions as are specified for the item are satisfied.

<table>
<thead>
<tr>
<th>Permitted CRB disclosures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Item</strong></td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>Item</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
</tbody>
</table>

(2) The consent of the individual under paragraph (b) of item 2 of the table in subsection (1) must be given in writing unless:

(a) the credit provider referred to in that item requests the information for the purpose of assessing an application for commercial credit made by a person to the provider; and
(b) the application has not been made in writing.
Part IIIA  Credit reporting
Division 2  Credit reporting bodies

Section 20G

20G  Use or disclosure of credit reporting information for the purposes of direct marketing

Prohibition on direct marketing

(1) If a credit reporting body holds credit reporting information about an individual, the body must not use or disclose the information for the purposes of direct marketing.

Civil penalty: 2,000 penalty units.

Permitted use for pre-screening

(2) Subsection (1) does not apply to the use by the credit reporting body of credit information about the individual for the purposes of direct marketing by, or on behalf of, a credit provider if:

(a) the provider has an Australian link and is a licensee; and

(b) the direct marketing is about consumer credit that the provider provides in Australia; and

(c) the information is not consumer credit liability information, or repayment history information, about the individual; and

(d) the body uses the information to assess whether or not the individual is eligible to receive the direct marketing communications of the credit provider; and

(e) the individual has not made a request under subsection (5); and

(f) the body complies with any requirements that are set out in the registered CR code.

(3) In assessing under paragraph (2)(d) whether or not the individual is eligible to receive the direct marketing communications of the credit provider, the credit reporting body must have regard to the eligibility requirements nominated by the provider.

(4) An assessment under paragraph (2)(d) is not credit reporting information about the individual.
Request not to use information for pre-screening

(5) An individual may request a credit reporting body that holds credit information about the individual not to use the information under subsection (2).

(6) If the individual makes a request under subsection (5), the credit reporting body must not charge the individual for the making of the request or to give effect to the request.

Written note of use

(7) If a credit reporting body uses credit information under subsection (2), the body must make a written note of that use.

Civil penalty: 500 penalty units.

20H Use or disclosure of pre-screening assessments

Use or disclosure by credit reporting bodies

(1) If a credit reporting body makes a pre-screening assessment in relation to direct marketing by, or on behalf of, a credit provider, the body must not use or disclose the assessment.

Civil penalty: 2,000 penalty units.

(2) Subsection (1) does not apply if:
   (a) the credit reporting body discloses the pre-screening assessment for the purposes of the direct marketing by, or on behalf of, the credit provider; and
   (b) the recipient of the assessment is an entity (other than the provider) that has an Australian link.

(3) If the credit reporting body discloses the pre-screening assessment under subsection (2), the body must make a written note of that disclosure.

Civil penalty: 500 penalty units.
Part IIIA Credit reporting

Division 2 Credit reporting bodies

Section 20J

Use or disclosure by recipients

(4) If the credit reporting body discloses the pre-screening assessment under subsection (2), the recipient must not use or disclose the assessment.

Civil penalty: 1,000 penalty units.

(5) Subsection (4) does not apply if the recipient uses the pre-screening assessment for the purposes of the direct marketing by, or on behalf of, the credit provider.

(6) If the recipient uses the pre-screening assessment under subsection (5), the recipient must make a written note of that use.

Civil penalty: 500 penalty units.

Interaction with the Australian Privacy Principles

(7) If the recipient is an APP entity, Australian Privacy Principles 6, 7 and 8 do not apply to the recipient in relation to a pre-screening assessment.

20J Destruction of pre-screening assessment

(1) If an entity has possession or control of a pre-screening assessment, the entity must destroy the assessment if:

(a) the entity no longer needs the assessment for any purpose for which it may be used or disclosed under section 20H; and

(b) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the assessment.

Civil penalty: 1,000 penalty units.

(2) If the entity is an APP entity but not a credit reporting body, Australian Privacy Principle 11.2 does not apply to the entity in relation to the pre-screening assessment.
20K No use or disclosure of credit reporting information during a ban period

(1) If:
   (a) a credit reporting body holds credit reporting information about an individual; and
   (b) the individual believes on reasonable grounds that the individual has been, or is likely to be, a victim of fraud (including identity fraud); and
   (c) the individual requests the body not to use or disclose the information under this Division;
then, despite any other provision of this Division, the body must not use or disclose the information during the ban period for the information.

Civil penalty: 2,000 penalty units.

(2) Subsection (1) does not apply if:
   (a) the individual expressly consents, in writing, to the use or disclosure of the credit reporting information under this Division; or
   (b) the use or disclosure of the credit reporting information is required by or under an Australian law or a court/tribunal order.

Ban period

(3) The ban period for credit reporting information about an individual is the period that:
   (a) starts when the individual makes a request under paragraph (1)(c); and
   (b) ends:
      (i) 21 days after the day on which the request is made; or
      (ii) if the period is extended under subsection (4)—on the day after the extended period ends.

(4) If:
Part IIIA  Credit reporting  
Division 2  Credit reporting bodies

Section 20L

(a) there is a ban period for credit reporting information about an individual that is held by a credit reporting body; and 
(b) before the ban period ends, the individual requests the body to extend that period; and 
(c) the body believes on reasonable grounds that the individual has been, or is likely to be, a victim of fraud (including identity fraud);

the body must:

(d) extend the ban period by such period as the body considers is reasonable in the circumstances; and 
(e) give the individual written notification of the extension.

Civil penalty: 1,000 penalty units.

(5) A ban period for credit reporting information may be extended more than once under subsection (4).

No charge for request etc.

(6) If an individual makes a request under paragraph (1)(c) or (4)(b), a credit reporting body must not charge the individual for the making of the request or to give effect to the request.

20L. Adoption of government related identifiers

(1) If:

(a) a credit reporting body holds credit reporting information about an individual; and
(b) the information is a government related identifier of the individual;

the body must not adopt the government related identifier as its own identifier of the individual.

Civil penalty: 2,000 penalty units.

(2) Subsection (1) does not apply if the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order.
20M Use or disclosure of credit reporting information that is de-identified

Use or disclosure

(1) If:
(a) a credit reporting body holds credit reporting information; and
(b) the information (the de-identified information) is de-identified;
the body must not use or disclose the de-identified information.

(2) Subsection (1) does not apply to the use or disclosure of the de-identified information if:
(a) the use or disclosure is for the purposes of conducting research in relation to credit; and
(b) the credit reporting body complies with the rules made under subsection (3).

Commissioner may make rules

(3) The Commissioner may, by legislative instrument, make rules relating to the use or disclosure by a credit reporting body of de-identified information for the purposes of conducting research in relation to credit.

(4) Without limiting subsection (3), the rules may relate to the following matters:
(a) the kinds of de-identified information that may or may not be used or disclosed for the purposes of conducting the research;
(b) whether or not the research is research in relation to credit;
(c) the purposes of conducting the research;
(d) consultation about the research;
(e) how the research is conducted.
Subdivision E—Integrity of credit reporting information

20N Quality of credit reporting information

(1) A credit reporting body must take such steps as are reasonable in the circumstances to ensure that the credit information the body collects is accurate, up-to-date and complete.

(2) A credit reporting body must take such steps as are reasonable in the circumstances to ensure that the credit reporting information the body uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

(3) Without limiting subsections (1) and (2), a credit reporting body must:
   (a) enter into agreements with credit providers that require the providers to ensure that credit information that they disclose to the body under section 21D is accurate, up-to-date and complete; and
   (b) ensure that regular audits are conducted by an independent person to determine whether those agreements are being complied with; and
   (c) identify and deal with suspected breaches of those agreements.

20P False or misleading credit reporting information

Offence

(1) A credit reporting body commits an offence if:
   (a) the body uses or discloses credit reporting information under this Division (other than subsections 20D(2) and 20T(4)); and
   (b) the information is false or misleading in a material particular.

Penalty: 200 penalty units.
Civil penalty

(2) A credit reporting body must not use or disclose credit reporting information under this Division (other than subsections 20D(2) and 20T(4)) if the information is false or misleading in a material particular.

Civil penalty: 2,000 penalty units.

20Q  Security of credit reporting information

(1) If a credit reporting body holds credit reporting information, the body must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and
(b) from unauthorised access, modification or disclosure.

(2) Without limiting subsection (1), a credit reporting body must:

(a) enter into agreements with credit providers that require the providers to protect credit reporting information that is disclosed to them under this Division:

(i) from misuse, interference and loss; and
(ii) from unauthorised access, modification or disclosure;

and

(b) ensure that regular audits are conducted by an independent person to determine whether those agreements are being complied with; and

(c) identify and deal with suspected breaches of those agreements.

Subdivision F—Access to, and correction of, information

20R  Access to credit reporting information

Access

(1) If a credit reporting body holds credit reporting information about an individual, the body must, on request by an access seeker in
relation to the information, give the access seeker access to the information.

Exceptions to access

(2) Despite subsection (1), the credit reporting body is not required to give the access seeker access to the credit reporting information to the extent that:
   (a) giving access would be unlawful; or
   (b) denying access is required or authorised by or under an Australian law or a court/tribunal order; or
   (c) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Dealing with requests for access

(3) The credit reporting body must respond to the request within a reasonable period, but not longer than 10 days, after the request is made.

Means of access

(4) If the credit reporting body gives access to the credit reporting information, the access must be given in the manner set out in the registered CR code.

Access charges

(5) If a request under subsection (1) in relation to the individual has not been made to the credit reporting body in the previous 12 months, the body must not charge the access seeker for the making of the request or for giving access to the information.

(6) If subsection (5) does not apply, any charge by the credit reporting body for giving access to the information must not be excessive and must not apply to the making of the request.
Refusal to give access

(7) If the credit reporting body refuses to give access to the information because of subsection (2), the body must give the access seeker a written notice that:

(a) sets out the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

(b) states that, if the access seeker is not satisfied with the response to the request, the access seeker may:
   (i) access a recognised external dispute resolution scheme of which the body is a member; or
   (ii) make a complaint to the Commissioner under Part V.

20S Correction of credit reporting information

(1) If:

(a) a credit reporting body holds credit reporting information about an individual; and

(b) the body is satisfied that, having regard to a purpose for which the information is held by the body, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading;

the body must take such steps (if any) as are reasonable in the circumstances to correct the information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.

(2) If:

(a) the credit reporting body corrects credit reporting information under subsection (1); and

(b) the body has previously disclosed the information under this Division (other than subsections 20D(2) and 20T(4));

the body must, within a reasonable period, give each recipient of the information written notice of the correction.

(3) Subsection (2) does not apply if:
Part IIIA Credit reporting
Division 2 Credit reporting bodies

Section 20T

(a) it is impracticable for the credit reporting body to give the notice under that subsection; or
(b) the credit reporting body is required by or under an Australian law, or a court/tribunal order, not to give the notice under that subsection.

20T Individual may request the correction of credit information etc.

Request

(1) An individual may request a credit reporting body to correct personal information about the individual if:
(a) the personal information is:
   (i) credit information about the individual; or
   (ii) CRB derived information about the individual; or
   (iii) CP derived information about the individual; and
(b) the body holds at least one kind of the personal information referred to in paragraph (a).

Correction

(2) If the credit reporting body is satisfied that the personal information is inaccurate, out-of-date, incomplete, irrelevant or misleading, the body must take such steps (if any) as are reasonable in the circumstances to correct the information within:
(a) the period of 30 days that starts on the day on which the request is made; or
(b) such longer period as the individual has agreed to in writing.

Consultation

(3) If the credit reporting body considers that the body cannot be satisfied of the matter referred to in subsection (2) in relation to the personal information without consulting either or both of the following (the interested party):
(a) another credit reporting body that holds or held the information and that has an Australian link;

Privacy Act 1988

Compilation No. 78 Compilation date: 1/7/18 Registered: 30/7/18

Authorised Version C2018C00292 registered 30/07/2018
(b) a credit provider that holds or held the information and that has an Australian link;
the body must consult that interested party, or those interested parties, about the individual’s request.

(4) The use or disclosure of personal information about the individual for the purposes of the consultation is taken, for the purposes of this Act, to be a use or disclosure that is authorised by this subsection.

No charge

(5) The credit reporting body must not charge the individual for the making of the request or for correcting the information.

20U Notice of correction etc. must be given

(1) This section applies if an individual requests a credit reporting body to correct personal information under subsection 20T(1).

Notice of correction etc.

(2) If the credit reporting body corrects the personal information under subsection 20T(2), the body must, within a reasonable period:
(a) give the individual written notice of the correction; and
(b) if the body consulted an interested party under subsection 20T(3) about the individual’s request—give the party written notice of the correction; and
(c) if the correction relates to information that the body has previously disclosed under this Division (other than subsections 20D(2) and 20T(4))—give each recipient of the information written notice of the correction.

(3) If the credit reporting body does not correct the personal information under subsection 20T(2), the body must, within a reasonable period, give the individual written notice that:
(a) states that the correction has not been made; and
Part IIIA  Credit reporting
Division 2  Credit reporting bodies

Section 20V

(b) sets out the body’s reasons for not correcting the information (including evidence substantiating the correctness of the information); and
(c) states that, if the individual is not satisfied with the response to the request, the individual may:
   (i) access a recognised external dispute resolution scheme of which the body is a member; or
   (ii) make a complaint to the Commissioner under Part V.

Exceptions

(4) Paragraph (2)(c) does not apply if it is impracticable for the credit reporting body to give the notice under that paragraph.

(5) Subsection (2) or (3) does not apply if the credit reporting body is required by or under an Australian law, or a court/tribunal order, not to give the notice under that subsection.

Subdivision G—Dealing with credit reporting information after the retention period ends etc.

20V  Destruction etc. of credit reporting information after the retention period ends

(1) This section applies if:
   (a) a credit reporting body holds credit information about an individual; and
   (b) the retention period for the information ends.

Note: There is no retention period for identification information or credit information of a kind referred to in paragraph 6N(k).

Destruction etc. of credit information

(2) The credit reporting body must destroy the credit information, or ensure that the information is de-identified, within 1 month after the retention period for the information ends.

Civil penalty: 1,000 penalty units.
(3) Despite subsection (2), the credit reporting body must neither destroy the credit information nor ensure that the information is de-identified, if immediately before the retention period ends:
   (a) there is a pending correction request in relation to the information; or
   (b) there is a pending dispute in relation to the information.

Civil penalty: 500 penalty units.

(4) Subsection (2) does not apply if the credit reporting body is required by or under an Australian law, or a court/tribunal order, to retain the credit information.

Destruction etc. of CRB derived information

(5) The credit reporting body must destroy any CRB derived information about the individual that was derived from the credit information, or ensure that the CRB derived information is de-identified:
   (a) if:
      (i) the CRB derived information was derived from 2 or more kinds of credit information; and
      (ii) the body is required to do a thing referred to in subsection (2) to one of those kinds of credit information;
          at the same time that the body does that thing to that credit information; or
      (b) otherwise—at the same time that the body is required to do a thing referred to in subsection (2) to the credit information from which the CRB derived information was derived.

Civil penalty: 1,000 penalty units.

(6) Despite subsection (5), the credit reporting body must neither destroy the CRB derived information nor ensure that the information is de-identified, if immediately before the retention period ends:
Part IIIA  Credit reporting  
Division 2  Credit reporting bodies

Section 20W

(a) there is a pending correction request in relation to the information; or

(b) there is a pending dispute in relation to the information.

Civil penalty: 500 penalty units.

(7) Subsection (5) does not apply if the credit reporting body is required by or under an Australian law, or a court/tribunal order, to retain the CRB derived information.

20W  Retention period for credit information—general

The following table sets out the retention period for credit information:

(a) that is information of a kind referred to in an item of the table; and

(b) that is held by a credit reporting body.

<table>
<thead>
<tr>
<th>Item</th>
<th>If the credit information is ...</th>
<th>the retention period for the information is ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>consumer credit liability information</td>
<td>the period of 2 years that starts on the day on which the consumer credit to which the information relates is terminated or otherwise ceases to be in force.</td>
</tr>
<tr>
<td>2</td>
<td>repayment history information</td>
<td>the period of 2 years that starts on the day on which the monthly payment to which the information relates is due and payable.</td>
</tr>
<tr>
<td>3</td>
<td>information of a kind referred to in paragraph 6N(d) or (e)</td>
<td>the period of 5 years that starts on the day on which the information request to which the information relates is made.</td>
</tr>
<tr>
<td>4</td>
<td>default information</td>
<td>the period of 5 years that starts on the day on which the credit reporting body collects the information.</td>
</tr>
</tbody>
</table>

Privacy Act 1988

Compilation No. 78  Compilation date: 1/7/18  Registered: 30/7/18
### Section 20X

#### Retention period for credit information

<table>
<thead>
<tr>
<th>Item</th>
<th>If the credit information is ...</th>
<th>the retention period for the information is ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>payment information</td>
<td>the period of 5 years that starts on the day on which the credit reporting body collects the default information to which the payment information relates.</td>
</tr>
<tr>
<td>6</td>
<td>new arrangement information within the meaning of subsection 6S(1)</td>
<td>the period of 2 years that starts on the day on which the credit reporting body collects the default information referred to in that subsection.</td>
</tr>
<tr>
<td>7</td>
<td>new arrangement information within the meaning of subsection 6S(2)</td>
<td>the period of 2 years that starts on the day on which the credit reporting body collects the information about the opinion referred to in that subsection.</td>
</tr>
<tr>
<td>8</td>
<td>court proceedings information</td>
<td>the period of 5 years that starts on the day on which the judgement to which the information relates is made or given.</td>
</tr>
<tr>
<td>9</td>
<td>information of a kind referred to in paragraph 6N(1)</td>
<td>the period of 7 years that starts on the day on which the credit reporting body collects the information.</td>
</tr>
</tbody>
</table>

#### 20X Retention period for credit information—personal insolvency information

(1) The following table has effect:

<table>
<thead>
<tr>
<th>Item</th>
<th>If personal insolvency information relates to ...</th>
<th>the retention period for the information is whichever of the following periods ends later ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>a bankruptcy of an individual</td>
<td>(a) the period of 5 years that starts on the day on which the individual becomes a bankrupt; (b) the period of 2 years that starts on the day the bankruptcy ends.</td>
</tr>
</tbody>
</table>
### Section 20X

<table>
<thead>
<tr>
<th>Item</th>
<th>If personal insolvency information relates to ...</th>
<th>the retention period for the information is whichever of the following periods ends later ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>a personal insolvency agreement to which item 3 of this table does not apply</td>
<td>(a) the period of 5 years that starts on the day on which the agreement is executed; (b) the period of 2 years that starts on the day the agreement is terminated or set aside under the Bankruptcy Act.</td>
</tr>
<tr>
<td>3</td>
<td>a personal insolvency agreement in relation to which a certificate has been signed under section 232 of the Bankruptcy Act</td>
<td>(a) the period of 5 years that starts on the day on which the agreement is executed; (b) the period that ends on the day on which the certificate is signed.</td>
</tr>
<tr>
<td>4</td>
<td>a debt agreement to which item 5 of this table does not apply</td>
<td>(a) the period of 5 years that starts on the day on which the agreement is made; (b) the period of 2 years that starts on the day: (i) the agreement is terminated under the Bankruptcy Act; or (ii) an order declaring that all the agreement is void is made under that Act.</td>
</tr>
<tr>
<td>5</td>
<td>a debt agreement that ends under section 185N of the Bankruptcy Act</td>
<td>(a) the period of 5 years that starts on the day on which the agreement is made; (b) the period that ends on the day on which the agreement ends.</td>
</tr>
</tbody>
</table>

**Debt agreement proposals**

(2) If personal insolvency information relates to a debt agreement proposal, the retention period for the information is the period that ends on the day on which:

(a) the proposal is withdrawn; or
(b) the proposal is not accepted under section 185EC of the Bankruptcy Act; or
(c) the acceptance of the proposal for processing is cancelled under section 185ED of that Act; or
(d) the proposal lapses under section 185G of that Act.

Control of property

(3) If personal insolvency information relates to a direction given, or an order made, under section 50 of the Bankruptcy Act, the retention period for the information is the period that ends on the day on which the control of the property to which the direction or order relates ends.

Note: See subsection 50(1B) of the Bankruptcy Act for when the control of the property ends.

(4) If the personal insolvency information relates to an authority signed under section 188 of the Bankruptcy Act, the retention period for the information is the period that ends on the day on which the property to which the authority relates is no longer subject to control under Division 2 of Part X of that Act.

Interpretation

(5) An expression used in this section that is also used in the Bankruptcy Act has the same meaning in this section as it has in that Act.

20Y Destruction of credit reporting information in cases of fraud

(1) This section applies if:
(a) a credit reporting body holds credit reporting information about an individual; and
(b) the information relates to consumer credit that has been provided by a credit provider to the individual, or a person purporting to be the individual; and
(c) the body is satisfied that:
   (i) the individual has been a victim of fraud (including identity fraud); and

Privacy Act 1988

Compilation No. 78   Compilation date: 1/7/18   Registered: 30/7/18

Authorised Version C2018C00292 registered 30/07/2018
Section 20Y

(ii) the consumer credit was provided as a result of that fraud.

Destruction of credit reporting information

(2) The credit reporting body must:
   (a) destroy the credit reporting information; and
   (b) within a reasonable period after the information is destroyed:
      (i) give the individual a written notice that states that the information has been destroyed and sets out the effect of subsection (4); and
      (ii) give the credit provider a written notice that states that the information has been destroyed.

Civil penalty: 1,000 penalty units.

(3) Subsection (2) does not apply if the credit reporting body is required by or under an Australian law, or a court/tribunal order, to retain the credit reporting information.

Notification of destruction to third parties

(4) If:
   (a) a credit reporting body destroys credit reporting information about an individual under subsection (2); and
   (b) the body has previously disclosed the information to one or more recipients under Subdivision D of this Division;
the body must, within a reasonable period after the destruction, notify those recipients of the destruction and the matters referred to in paragraph (1)(c).

Civil penalty: 500 penalty units.

(5) Subsection (4) does not apply if the credit reporting body is required by or under an Australian law, or a court/tribunal order, not to give the notification.
20Z Dealing with information if there is a pending correction request etc.

(1) This section applies if a credit reporting body holds credit reporting information about an individual and either:
   (a) subsection 20V(3) applies in relation to the information; or
   (b) subsection 20V(6) applies in relation to the information.

Notification of Commissioner

(2) The credit reporting body must, as soon as practicable, notify in writing the Commissioner of the matter referred to in paragraph (1)(a) or (b) of this section.

   Civil penalty: 1,000 penalty units.

Use or disclosure

(3) The credit reporting body must not use or disclose the information under Subdivision D of this Division.

   Civil penalty: 2,000 penalty units.

(4) However, the credit reporting body may use or disclose the information under this subsection if:
   (a) the use or disclosure is for the purposes of the pending correction request, or pending dispute, in relation to the information; or
   (b) the use or disclosure of the information is required by or under an Australian law or a court/tribunal order.

(5) If the credit reporting body uses or discloses the information under subsection (4), the body must make a written note of the use or disclosure.

   Civil penalty: 500 penalty units.
Part IIIA  Credit reporting
Division 2  Credit reporting bodies

Section 20ZA

Direction to destroy information etc.

(6) The Commissioner may, by legislative instrument, direct the credit reporting body to destroy the information, or ensure that the information is de-identified, by a specified day.

(7) If the Commissioner gives a direction under subsection (6) to the credit reporting body, the body must comply with the direction.

Civil penalty: 1,000 penalty units.

(8) To avoid doubt, section 20M applies in relation to credit reporting information that is de-identified as a result of the credit reporting body complying with the direction.

20ZA  Dealing with information if an Australian law etc. requires it to be retained

(1) This section applies if a credit reporting body is not required:
(a) to do a thing referred to in subsection 20V(2) to credit information because of subsection 20V(4); or
(b) to do a thing referred to in subsection 20V(5) to CRB derived information because of subsection 20V(7); or
(c) to destroy credit reporting information under subsection 20Y(2) because of subsection 20Y(3).

Use or disclosure

(2) The credit reporting body must not use or disclose the information under Subdivision D of this Division.

Civil penalty: 2,000 penalty units.

(3) However, the credit reporting body may use or disclose the information under this subsection if the use or disclosure of the information is required by or under an Australian law or a court/tribunal order.
Section 20ZA

(4) If the credit reporting body uses or discloses the information under subsection (3), the body must make a written note of the use or disclosure.

Civil penalty: 500 penalty units.

Other requirements

(5) Subdivision E of this Division (other than section 20Q) does not apply in relation to the use or disclosure of the information.

Note: Section 20Q deals with the security of credit reporting information.

(6) Subdivision F of this Division does not apply in relation to the information.
Part IIIA Credit reporting
Division 3 Credit providers

Section 21

Division 3—Credit providers

Subdivision A—Introduction and application of this Division

21 Guide to this Division

This Division sets out rules that apply to credit providers in relation to their handling of the following:

(a) credit information;
(b) credit eligibility information;
(c) CRB derived information.

If a credit provider is an APP entity, the rules apply in relation to that information in addition to, or instead of, any relevant Australian Privacy Principles.

21A Application of this Division to credit providers

(1) This Division applies to a credit provider in relation to the following:
(a) credit information;
(b) credit eligibility information;
(c) CRB derived information.

(2) If the credit provider is an APP entity, this Division may apply to the provider in relation to information referred to in subsection (1) in addition to, or instead of, the Australian Privacy Principles.
Subdivision B—Consideration of information privacy

21B Open and transparent management of credit information etc.

(1) The object of this section is to ensure that credit providers manage credit information and credit eligibility information in an open and transparent way.

Compliance with this Division etc.

(2) A credit provider must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the provider’s functions or activities as a credit provider that:

(a) will ensure that the provider complies with this Division and the registered CR code if it binds the provider; and

(b) will enable the provider to deal with inquiries or complaints from individuals about the provider’s compliance with this Division or the registered CR code if it binds the provider.

Policy about the management of credit information etc.

(3) A credit provider must have a clearly expressed and up-to-date policy about the management of credit information and credit eligibility information by the provider.

(4) Without limiting subsection (3), the policy of the credit provider must contain the following information:

(a) the kinds of credit information that the provider collects and holds, and how the provider collects and holds that information;

(b) the kinds of credit eligibility information that the provider holds and how the provider holds that information;

(c) the kinds of CP derived information that the provider usually derives from credit reporting information disclosed to the provider by a credit reporting body under Division 2 of this Part;
(d) the purposes for which the provider collects, holds, uses and discloses credit information and credit eligibility information;
(e) how an individual may access credit eligibility information about the individual that is held by the provider;
(f) how an individual may seek the correction of credit information or credit eligibility information about the individual that is held by the provider;
(g) how an individual may complain about a failure of the provider to comply with this Division or the registered CR code if it binds the provider;
(h) how the provider will deal with such a complaint;
(i) whether the provider is likely to disclose credit information or credit eligibility information to entities that do not have an Australian link;
(j) if the provider is likely to disclose credit information or credit eligibility information to such entities—the countries in which those entities are likely to be located if it is practicable to specify those countries in the policy.

Availability of policy etc.

(5) A credit provider must take such steps as are reasonable in the circumstances to make the policy available:
(a) free of charge; and
(b) in such form as is appropriate.

Note: A credit provider will usually make the policy available on the provider’s website.

(6) If a person or body requests a copy, in a particular form, of the policy of a credit provider, the provider must take such steps as are reasonable in the circumstances to give the person or body a copy in that form.

Interaction with the Australian Privacy Principles

(7) If a credit provider is an APP entity, Australian Privacy Principles 1.3 and 1.4 do not apply to the provider in relation to credit information or credit eligibility information.
Subdivision C—Dealing with credit information

21C Additional notification requirements for the collection of personal information etc.

(1) At or before the time a credit provider collects personal information about an individual that the provider is likely to disclose to a credit reporting body, the provider must:
   (a) notify the individual of the following matters:
       (i) the name and contact details of the body;
       (ii) any other matter specified in the registered CR code; or
   (b) otherwise ensure that the individual is aware of those matters.

(2) If a credit provider is an APP entity, subsection (1) applies to the provider in relation to personal information in addition to Australian Privacy Principle 5.

(3) If a credit provider is an APP entity, then the matters for the purposes of Australian Privacy Principle 5.1 include the following matters to the extent that the personal information referred to in that principle is credit information or credit eligibility information:
   (a) that the policy (the credit reporting policy) of the provider that is referred to in subsection 21B(3) contains information about how an individual may access the credit eligibility information about the individual that is held by the provider;
   (b) that the credit reporting policy of the provider contains information about how an individual may seek the correction of credit information or credit eligibility information about the individual that is held by the provider;
   (c) that the credit reporting policy of the provider contains information about how an individual may complain about a failure of the provider to comply with this Division or the registered CR code if it binds the provider;
   (d) that the credit reporting policy of the provider contains information about how the provider will deal with such a complaint;
Section 21D

(e) whether the provider is likely to disclose credit information or credit eligibility information to entities that do not have an Australian link;

(f) if the provider is likely to disclose credit information or credit eligibility information to such entities—the countries in which those entities are likely to be located if it is practicable to specify those countries in the credit reporting policy.

21D Disclosure of credit information to a credit reporting body

Prohibition on disclosure

(1) A credit provider must not disclose credit information about an individual to a credit reporting body (whether or not the body’s credit reporting business is carried on in Australia).

Civil penalty: 2,000 penalty units.

Permitted disclosure

(2) Subsection (1) does not apply to the disclosure of credit information about the individual if:

(a) the credit provider:
   (i) is a member of a recognised external dispute resolution scheme or is prescribed by the regulations; and
   (ii) knows, or believes on reasonable grounds, that the individual is at least 18 years old; and

(b) the credit reporting body is:
   (i) an agency; or
   (ii) an organisation that has an Australian link; and

(c) the information meets the requirements of subsection (3).

Note: Section 21F limits the disclosure of credit information if there is a ban period for the information.

(3) Credit information about an individual meets the requirements of this subsection if:
(a) the information does not relate to an act, omission, matter or thing that occurred or existed before the individual turned 18; and

(b) if the information relates to consumer credit or commercial credit—the credit is or has been provided, or applied for, in Australia; and

(c) if the information is repayment history information about the individual:
   (i) the credit provider is a licensee or is prescribed by the regulations; and
   (ii) the consumer credit to which the information relates is consumer credit in relation to which the provider also discloses, or a credit provider has previously disclosed, consumer credit liability information about the individual to the credit reporting body; and
   (iii) the provider complies with any requirements relating to the disclosure of the information that are prescribed by the regulations; and

(d) if the information is default information about the individual:
   (i) the credit provider has given the individual a notice in writing stating that the provider intends to disclose the information to the credit reporting body; and
   (ii) at least 14 days have passed since the giving of the notice.

(4) Paragraph (3)(a) does not apply to identification information about the individual.

(5) Despite paragraph (3)(a), consumer credit liability information about the individual may relate to consumer credit that was entered into on a day before the individual turned 18, so long as the consumer credit was not terminated, or did not otherwise cease to be in force, on a day before the individual turned 18.

Written note of disclosure

(6) If a credit provider discloses credit information under this section, the provider must make a written note of that disclosure.
Part IIA  Credit reporting
Division 3  Credit providers

Section 21E

Civil penalty: 500 penalty units.

Interaction with the Australian Privacy Principles

(7) If a credit provider is an APP entity, Australian Privacy Principles 6 and 8 do not apply to the disclosure by the provider of credit information to a credit reporting body.

21E Payment information must be disclosed to a credit reporting body

If:
(a) a credit provider has disclosed default information about an individual to a credit reporting body under section 21D; and
(b) after the default information was disclosed, the amount of the overdue payment to which the information relates is paid;

the provider must, within a reasonable period after the amount is paid, disclose payment information about the amount to the body under that section.

Civil penalty: 500 penalty units.

21F Limitation on the disclosure of credit information during a ban period

(1) This section applies if:
(a) a credit reporting body holds credit reporting information about an individual; and
(b) a credit provider requests the body to disclose the information to the provider for the purpose of assessing an application for consumer credit made to the provider by the individual, or a person purporting to be the individual; and
(c) the body is not permitted to disclose the information because there is a ban period for the information; and
(d) during the ban period, the provider provides the consumer credit to which the application relates to the individual, or the person purporting to be the individual.
Section 21G

(2) If the credit provider holds credit information about the individual that relates to the consumer credit, the provider must not, despite sections 21D and 21E, disclose the information to a credit reporting body.

Civil penalty: 2,000 penalty units.

(3) Subsection (2) does not apply if the credit provider has taken such steps as are reasonable in the circumstances to verify the identity of the individual.

Subdivision D—Dealing with credit eligibility information etc.

21G Use or disclosure of credit eligibility information

Prohibition on use or disclosure

(1) If a credit provider holds credit eligibility information about an individual, the provider must not use or disclose the information.

Civil penalty: 2,000 penalty units.

Permitted uses

(2) Subsection (1) does not apply to the use of credit eligibility information about the individual if:

(a) the use is for a consumer credit related purpose of the credit provider in relation to the individual; or

(b) the use is a permitted CP use in relation to the individual; or

(c) both of the following apply:

(i) the credit provider believes on reasonable grounds that the individual has committed a serious credit infringement;

(ii) the provider uses the information in connection with the infringement; or

(d) the use is required or authorised by or under an Australian law or a court/tribunal order; or

(e) the use is a use prescribed by the regulations.
Part IIIA  Credit reporting
Division 3  Credit providers

Section 21G

Permitted disclosures

(3) Subsection (1) does not apply to the disclosure of credit eligibility information about the individual if:

(a) the disclosure is a permitted CP disclosure in relation to the individual; or

(b) the disclosure is to a related body corporate of the credit provider; or

(c) the disclosure is to:
   (i) a person for the purpose of processing an application for credit made to the credit provider; or
   (ii) a person who manages credit provided by the credit provider for use in managing that credit; or

(d) both of the following apply:
   (i) the credit provider believes on reasonable grounds that the individual has committed a serious credit infringement;
   (ii) the provider discloses the information to another credit provider that has an Australian link, or to an enforcement body; or

(e) both of the following apply:
   (i) the disclosure is for the purposes of a recognised external dispute resolution scheme;
   (ii) a credit provider or credit reporting body is a member of the scheme; or

(f) the disclosure is required or authorised by or under an Australian law or a court/tribunal order; or

(g) the disclosure is a disclosure prescribed by the regulations.

Note: See section 21NA for additional rules about the disclosure of credit eligibility information under paragraph (3)(b) or (c).

(4) However, if the credit eligibility information about the individual is, or was derived from, repayment history information about the individual, the credit provider must not disclose the information under subsection (3).

Civil penalty: 2,000 penalty units.
Section 21H

(5) Subsection (4) does not apply if:
   (a) the recipient of the credit eligibility information is another credit provider who is a licensee; or
   (b) the disclosure is a permitted CP disclosure within the meaning of section 21L; or
   (c) the credit provider discloses the credit eligibility information under paragraph (3)(b), (c), (e) or (f); or
   (d) the credit provider discloses the credit eligibility information under paragraph (3)(d) to an enforcement body.

Written note of use or disclosure

(6) If a credit provider uses or discloses credit eligibility information under this section, the provider must make a written note of that use or disclosure.

Civil penalty: 500 penalty units.

Interaction with the Australian Privacy Principles

(7) If a credit provider is an APP entity, Australian Privacy Principles 6, 7 and 8 do not apply to the provider in relation to credit eligibility information.

(8) If:
   (a) a credit provider is an APP entity; and
   (b) the credit eligibility information is a government related identifier of the individual;

Australian Privacy Principle 9.2 does not apply to the provider in relation to the information.

21H Permitted CP uses in relation to individuals

A use by a credit provider of credit eligibility information about an individual is a permitted CP use in relation to the individual if:
   (a) the relevant credit reporting information was disclosed to the provider under a provision specified in column 1 of the table for the purpose (if any) specified in that column; and
Section 21H

(b) the provider uses the credit eligibility information for the purpose specified in column 2 of the table.

<table>
<thead>
<tr>
<th>Item</th>
<th>Column 1</th>
<th>Column 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>item 1 of the table in subsection 20F(1) for the purpose of assessing an application for consumer credit made by the individual to the provider.</td>
<td>(a) a securitisation related purpose of the provider in relation to the individual; or (b) the internal management purposes of the provider that are directly related to the provision or management of consumer credit by the provider.</td>
</tr>
<tr>
<td>2</td>
<td>item 2 of the table in subsection 20F(1) for a particular commercial credit related purpose of the provider in relation to the individual.</td>
<td>that particular commercial credit related purpose.</td>
</tr>
<tr>
<td>3</td>
<td>item 2 of the table in subsection 20F(1) for the purpose of assessing an application for commercial credit made by a person to the provider.</td>
<td>the internal management purposes of the provider that are directly related to the provision or management of commercial credit by the provider.</td>
</tr>
<tr>
<td>4</td>
<td>item 3 of the table in subsection 20F(1) for a credit guarantee purpose of the provider in relation to the individual.</td>
<td>(a) the credit guarantee purpose; or (b) the internal management purposes of the provider that are directly related to the provision or management of any credit by the provider.</td>
</tr>
<tr>
<td>5</td>
<td>item 5 of the table in subsection 20F(1).</td>
<td>the purpose of assisting the individual to avoid defaulting on his or her obligations in relation to consumer credit provided by the provider to the individual.</td>
</tr>
</tbody>
</table>
Section 21J

**Permitted CP uses**

<table>
<thead>
<tr>
<th>Item</th>
<th>Column 1</th>
<th>Column 2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The relevant credit reporting information was disclosed to the credit provider under ...</td>
<td>The credit provider uses the credit eligibility information for ...</td>
</tr>
<tr>
<td>6</td>
<td>item 6 of the table in subsection 20F(1) for a particular securitisation related purpose of the provider in relation to the individual.</td>
<td>that particular securitisation related purpose.</td>
</tr>
</tbody>
</table>

**21J Permitted CP disclosures between credit providers**

*Consent*

(1) A disclosure by a credit provider of credit eligibility information about an individual is a *permitted CP disclosure* in relation to the individual if:

   (a) the disclosure is to another credit provider (the *recipient*) for a particular purpose; and
   (b) the recipient has an Australian link; and
   (c) the individual expressly consents to the disclosure of the information to the recipient for that purpose.

(2) The consent of the individual under paragraph (1)(c):

   (a) must be given in writing unless:

      (i) the disclosure of the information to the recipient is for the purpose of assessing an application for consumer credit or commercial credit made to the recipient; and
      (ii) the application has not been made in writing; and
   (b) must be given to the credit provider or recipient.

*Agents of credit providers*

(3) A disclosure by a credit provider of credit eligibility information about an individual is a *permitted CP disclosure* in relation to the individual if:
Section 21J

(a) the provider is acting as an agent of another credit provider that has an Australian link; and
(b) while the provider is so acting, the provider is a credit provider under subsection 6H(1); and
(c) the provider discloses the information to the other credit provider in the provider’s capacity as such an agent.

Securitisation arrangements etc.

(4) A disclosure by a credit provider of credit eligibility information about an individual is a permitted CP disclosure in relation to the individual if:
(a) the provider is a credit provider under subsection 6J(1) in relation to credit; and
(b) the credit has been provided by, or is credit for which an application has been made to, another credit provider (the original credit provider) that has an Australian link; and
(c) the original credit provider is not a credit provider under that subsection; and
(d) the information is disclosed to:
   (i) the original credit provider; or
   (ii) another credit provider that is a credit provider under that subsection in relation to the credit and that has an Australian link; and
(e) the disclosure of the information is reasonably necessary for:
   (i) purchasing, funding or managing, or processing an application for, the credit by means of a securitisation arrangement; or
   (ii) undertaking credit enhancement in relation to the credit.

Mortgage credit secured by the same real property

(5) A disclosure by a credit provider of credit eligibility information about an individual is a permitted CP disclosure in relation to the individual if:
(a) the disclosure is to another credit provider that has an Australian link; and
Section 21K

(b) both credit providers have provided mortgage credit to the individual in relation to which the same real property forms all or part of the security; and

c) the individual is at least 60 days overdue in making a payment in relation to the mortgage credit provided by either provider; and

d) the information is disclosed for the purpose of either provider deciding what action to take in relation to the overdue payment.

21K Permitted CP disclosures relating to guarantees etc.

Offer to act as a guarantor etc.

(1) A disclosure by a credit provider of credit eligibility information about an individual is a permitted CP disclosure in relation to the individual if:

(a) either:
   (i) the provider has provided credit to the individual; or
   (ii) the individual has applied to the provider for credit; and

(b) the disclosure is to a person for the purpose of that person considering whether:
   (i) to offer to act as a guarantor in relation to the credit; or
   (ii) to offer property as security for the credit; and

(c) the person has an Australian link; and

(d) the individual expressly consents to the disclosure of the information to the person for that purpose.

(2) The consent of the individual under paragraph (1)(d) must be given in writing unless:

(a) if subparagraph (1)(a)(i) applies—the application for the credit was not made in writing; or

(b) if subparagraph (1)(a)(ii) applies—the application for the credit has not been made in writing.

Privacy Act 1988

Compilation No. 78
Compilation date: 1/7/18
Registered: 30/7/18
Guarantors etc.

(3) A disclosure by a credit provider of credit eligibility information about an individual is a permitted CP disclosure in relation to the individual if:

(a) the disclosure is to a person who:
   (i) is a guarantor in relation to credit provided by the provider to the individual; or
   (ii) has provided property as security for such credit; and
(b) the person has an Australian link; and
(c) either:
   (i) the individual expressly consents to the disclosure of the information to the person; or
   (ii) if subparagraph (a)(i) applies—the information is disclosed to the person for a purpose related to the enforcement, or proposed enforcement, of the guarantee.

(4) The consent of the individual under subparagraph (3)(c)(i) must be given in writing unless the application for the credit was not made in writing.

21L Permitted CP disclosures to mortgage insurers

A disclosure by a credit provider of credit eligibility information about an individual is a permitted CP disclosure in relation to the individual if the disclosure is to a mortgage insurer that has an Australian link for:

(a) a mortgage insurance purpose of the insurer in relation to the individual; or
(b) any purpose arising under a contract for mortgage insurance that has been entered into between the provider and the insurer.
21M Permitted CP disclosures to debt collectors

(1) A disclosure by a credit provider of credit eligibility information about an individual is a permitted CP disclosure in relation to the individual if:

(a) the disclosure is to a person or body that carries on a business or undertaking that involves the collection of debts on behalf of others; and

(c) the information is disclosed to the person or body for the primary purpose of the person or body collecting payments that are overdue in relation to:

(i) consumer credit provided by the provider to the individual; or

(ii) commercial credit provided by the provider to a person; and

(d) the information is information of a kind referred to in subsection (2).

Note: See section 21NA for additional rules about the disclosure of credit eligibility information under this subsection.

(2) The information for the purposes of paragraph (1)(d) is:

(a) identification information about the individual; or

(b) court proceedings information about the individual; or

(c) personal insolvency information about the individual; or

(d) if subparagraph (1)(c)(i) applies—default information about the individual if:

(i) the information relates to a payment that the individual is overdue in making in relation to consumer credit that has been provided by the credit provider to the individual; and

(ii) the provider does not hold, or has not held, payment information about the individual that relates to that overdue payment.
21N Permitted CP disclosures to other recipients

*Mortgage credit assistance schemes*

(1) A disclosure by a credit provider of credit eligibility information about an individual is a *permitted CP disclosure* in relation to the individual if:

(a) the disclosure is to a State or Territory authority; and

(b) the functions or responsibilities of the authority include:

(i) giving assistance (directly or indirectly) that facilitates the provision of mortgage credit to individuals; or

(ii) the management or supervision of schemes or arrangements under which such assistance is given; and

(c) the information is disclosed for the purpose of enabling the authority:

(i) to determine the extent of the assistance (if any) to give in relation to the provision of mortgage credit to the individual; or

(ii) to manage or supervise such a scheme or arrangement.

*Assignment of debts owed to credit providers etc.*

(2) A disclosure by a credit provider of credit eligibility information about an individual is a *permitted CP disclosure* in relation to the individual if:

(a) the disclosure is to one or more of the following (the recipient):

(i) an entity;

(ii) a professional legal adviser of the entity;

(iii) a professional financial adviser of the entity; and

(b) the recipient has an Australian link; and

(c) subsection (3) applies to the information.

(3) This subsection applies to the credit eligibility information if the recipient proposes to use the information:

(a) in the process of the entity considering whether to:
Section 21NA

(i) accept an assignment of a debt owed to the credit provider; or
(ii) accept a debt owed to the provider as security for credit provided to the provider; or
(iii) purchase an interest in the provider or a related body corporate of the provider; or
(b) in connection with exercising rights arising from the acceptance of such an assignment or debt, or the purchase of such an interest.

21NA Disclosures to certain persons and bodies that do not have an Australian link

Related bodies corporate and credit managers etc.

(1) Before a credit provider discloses credit eligibility information under paragraph 21G(3)(b) or (c) to a related body corporate, or person, that does not have an Australian link, the provider must take such steps as are reasonable in the circumstances to ensure that the body or person does not breach the following provisions (the relevant provisions) in relation to the information:
(a) for a disclosure under paragraph 21G(3)(b)—section 22D;
(b) for a disclosure under paragraph 21G(3)(c)—section 22E;
(c) in both cases—the Australian Privacy Principles (other than Australian Privacy Principles 1, 6, 7, 8 and 9.2).

(2) If:
(a) a credit provider discloses credit eligibility information under paragraph 21G(3)(b) or (c) to a related body corporate, or person, that does not have an Australian link; and
(b) the relevant provisions do not apply, under this Act, to an act done, or a practice engaged in, by the body or person in relation to the information; and
(c) the body or person does an act, or engages in a practice, in relation to the information that would be a breach of the relevant provisions if those provisions applied to the act or practice;
Part IIIA Credit reporting
Division 3 Credit providers

Section 21P

the act done, or the practice engaged in, by the body or person is
taken, for the purposes of this Act, to have been done, or engaged
in, by the provider and to be a breach of those provisions by the
provider.

Debt collectors

(3) Before a credit provider discloses credit eligibility information
under subsection 21M(1) to a person or body that does not have an
Australian link, the provider must take such steps as are reasonable
in the circumstances to ensure that the person or body does not
breach the Australian Privacy Principles (other than Australian
Privacy Principle 1) in relation to the information.

(4) If:
(a) a credit provider discloses credit eligibility information under
subsection 21M(1) to a person or body that does not have an
Australian link; and
(b) the Australian Privacy Principles do not apply, under this
Act, to an act done, or a practice engaged in, by the person or
body in relation to the information; and
(c) the person or body does an act, or engages in a practice, in
relation to the information that would be a breach of the
Australian Privacy Principles (other than Australian Privacy
Principle 1) if those Australian Privacy Principles applied to
the act or practice;
the act done, or the practice engaged in, by the person or body is
taken, for the purposes of this Act, to have been done, or engaged
in, by the provider and to be a breach of those Australian Privacy
Principles by the provider.

21P Notification of a refusal of an application for consumer credit

(1) This section applies if:
(a) a credit provider refuses an application for consumer credit
made in Australia:
(i) by an individual; or
(ii) jointly by an individual and one or more other persons (the other applicants); and

(b) the refusal is based wholly or partly on credit eligibility information about one or more of the following:
   (i) the individual;
   (ii) a person who is proposing to act as a guarantor in relation to the consumer credit;
   (iii) if the application is an application of a kind referred to in subparagraph (a)(ii)—one of the other applicants; and

(c) a credit reporting body disclosed the relevant credit reporting information to the provider for the purposes of assessing the application.

(2) The credit provider must, within a reasonable period after refusing the application, give the individual a written notice that:
   (a) states that the application has been refused; and
   (b) states that the refusal is based wholly or partly on credit eligibility information about one or more of the persons referred to in paragraph (1)(b); and
   (c) if that information is about the individual—sets out:
      (i) the name and contact details of the credit reporting body that disclosed the relevant credit reporting information to the provider; and
      (ii) any other matter specified in the registered CR code.

Subdivision E—Integrity of credit information and credit eligibility information

21Q Quality of credit eligibility information

(1) A credit provider must take such steps (if any) as are reasonable in the circumstances to ensure that the credit eligibility information the provider collects is accurate, up-to-date and complete.

(2) A credit provider must take such steps (if any) as are reasonable in the circumstances to ensure that the credit eligibility information
Part IIA  Credit reporting
Division 3  Credit providers

Section 21R

the provider uses or discloses is, having regard to the purpose of
the use or disclosure, accurate, up-to-date, complete and relevant.

(3) If a credit provider is an APP entity, Australian Privacy
Principle 10 does not apply to the provider in relation to credit
eligibility information.

21R  False or misleading credit information or credit eligibility
information

Offences

(1) A credit provider commits an offence if:
(a) the provider discloses credit information under section 21D;
and
(b) the information is false or misleading in a material particular.

Penalty: 200 penalty units.

(2) A credit provider commits an offence if:
(a) the provider uses or discloses credit eligibility information
under this Division; and
(b) the information is false or misleading in a material particular.

Penalty: 200 penalty units.

Civil penalties

(3) A credit provider must not disclose credit information under
section 21D if the information is false or misleading in a material
particular.

Civil penalty: 2,000 penalty units.

(4) A credit provider must not use or disclose credit eligibility
information under this Division if the information is false or
misleading in a material particular.

Civil penalty: 2,000 penalty units.
21S Security of credit eligibility information

(1) If a credit provider holds credit eligibility information, the provider must take such steps as are reasonable in the circumstances to protect the information:
   (a) from misuse, interference and loss; and
   (b) from unauthorised access, modification or disclosure.

(2) If:
   (a) a credit provider holds credit eligibility information about an individual; and
   (b) the provider no longer needs the information for any purpose for which the information may be used or disclosed by the provider under this Division; and
   (c) the provider is not required by or under an Australian law, or a court/tribunal order, to retain the information;

   the provider must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

   Civil penalty: 1,000 penalty units.

(3) If a credit provider is an APP entity, Australian Privacy Principle 11 does not apply to the provider in relation to credit eligibility information.

Subdivision F—Access to, and correction of, information

21T Access to credit eligibility information

Access

(1) If a credit provider holds credit eligibility information about an individual, the provider must, on request by an access seeker in relation to the information, give the access seeker access to the information.
Part IIIA  Credit reporting

Division 3  Credit providers

Section 21T

Exceptions to access

(2) Despite subsection (1), the credit provider is not required to give the access seeker access to the credit eligibility information to the extent that:

(a) giving access would be unlawful; or

(b) denying access is required or authorised by or under an Australian law or a court/tribunal order; or

(c) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Dealing with requests for access

(3) The credit provider must respond to the request within a reasonable period after the request is made.

Means of access

(4) If the credit provider gives access to the credit eligibility information, the access must be given in the manner set out in the registered CR code.

Access charges

(5) If the credit provider is an agency, the provider must not charge the access seeker for the making of the request or for giving access to the information.

(6) If a credit provider is an organisation or small business operator, any charge by the provider for giving access to the information must not be excessive and must not apply to the making of the request.

Refusal to give access

(7) If the provider refuses to give access to the information because of subsection (2), the provider must give the access seeker a written notice that:
Section 21U

(a) sets out the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

(b) states that, if the access seeker is not satisfied with the response to the request, the access seeker may:

(i) access a recognised external dispute resolution scheme of which the provider is a member; or

(ii) make a complaint to the Commissioner under Part V.

Interaction with the Australian Privacy Principles

(8) If a credit provider is an APP entity, Australian Privacy Principle 12 does not apply to the provider in relation to credit eligibility information.

21U Correction of credit information or credit eligibility information

(1) If:

(a) a credit provider holds credit information or credit eligibility information about an individual; and

(b) the provider is satisfied that, having regard to a purpose for which the information is held by the provider, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading;

the provider must take such steps (if any) as are reasonable in the circumstances to correct the information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.

Notice of correction

(2) If:

(a) the credit provider corrects credit information or credit eligibility information under subsection (1); and

(b) the provider has previously disclosed the information under:

(i) this Division (other than subsection 21V(4)); or
Part IIIA  Credit reporting
Division 3  Credit providers

Section 21V

(ii) the Australian Privacy Principles (other than Australian Privacy Principle 4.2);
the provider must, within a reasonable period, give each recipient of the information written notice of the correction.

(3) Subsection (2) does not apply if:
(a) it is impracticable for the credit provider to give the notice under that subsection; or
(b) the credit provider is required by or under an Australian law, or a court/tribunal order, not to give the notice under that subsection.

Interaction with the Australian Privacy Principles

(4) If a credit provider is an APP entity, Australian Privacy Principle 13:
(a) applies to the provider in relation to credit information or credit eligibility information that is identification information; but
(b) does not apply to the provider in relation to any other kind of credit information or credit eligibility information.

Note: Identification information may be corrected under this section or Australian Privacy Principle 13.

21V Individual may request the correction of credit information etc.

Request

(1) An individual may request a credit provider to correct personal information about the individual if:
(a) the personal information is:
   (i) credit information about the individual; or
   (ii) CRB derived information about the individual; or
   (iii) CP derived information about the individual; and
(b) the provider holds at least one kind of the personal information referred to in paragraph (a).
Section 21V

Correction

(2) If the credit provider is satisfied that the personal information is inaccurate, out-of-date, incomplete, irrelevant or misleading, the provider must take such steps (if any) as are reasonable in the circumstances to correct the information within:
   (a) the period of 30 days that starts on the day on which the request is made; or
   (b) such longer period as the individual has agreed to in writing.

Consultation

(3) If the credit provider considers that the provider cannot be satisfied of the matter referred to in subsection (2) in relation to the personal information without consulting either or both of the following (the interested party):
   (a) a credit reporting body that holds or held the information and that has an Australian link;
   (b) another credit provider that holds or held the information and that has an Australian link;
the provider must consult that interested party, or those interested parties, about the individual’s request.

(4) The use or disclosure of personal information about the individual for the purposes of the consultation is taken, for the purposes of this Act, to be a use or disclosure that is authorised by this subsection.

No charge

(5) The credit provider must not charge the individual for the making of the request or for correcting the information.

Interaction with the Australian Privacy Principles

(6) If a credit provider is an APP entity, Australian Privacy Principle 13:
Part IIIA  Credit reporting
Division 3  Credit providers

Section 21W

(a) applies to the provider in relation to personal information referred to in paragraph (1)(a) that is identification information; but

(b) does not apply to the provider in relation to any other kind of personal information referred to in that paragraph.

Note: Identification information may be corrected under this section or Australian Privacy Principle 13.

21W Notice of correction etc. must be given

(1) This section applies if an individual requests a credit provider to correct personal information under subsection 21V(1).

Notice of correction etc.

(2) If the credit provider corrects personal information about the individual under subsection 21V(2), the provider must, within a reasonable period:

(a) give the individual written notice of the correction; and

(b) if the provider consulted an interested party under subsection 21V(3) about the individual’s request—give the party written notice of the correction; and

(c) if the correction relates to information that the provider has previously disclosed under:

(i) this Division (other than subsection 21V(4)); or

(ii) the Australian Privacy Principles (other than Australian Privacy Principle 4.2);

give each recipient of the information written notice of the correction.

(3) If the credit provider does not correct the personal information under subsection 21V(2), the provider must, within a reasonable period, give the individual written notice that:

(a) states that the correction has not been made; and

(b) sets out the provider’s reasons for not correcting the information (including evidence substantiating the correctness of the information); and
(c) states that, if the individual is not satisfied with the response to the request, the individual may:

(i) access a recognised external dispute resolution scheme of which the provider is a member; or

(ii) make a complaint to the Commissioner under Part V.

Exceptions

(4) Paragraph (2)(c) does not apply if it is impracticable for the credit provider to give the notice under that paragraph.

(5) Subsection (2) or (3) does not apply if the credit provider is required by or under an Australian law, or a court/tribunal order, not to give the notice under that subsection.
Part IIIA  Credit reporting  
Division 4  Affected information recipients

Section 22

Division 4—Affected information recipients

22  Guide to this Division

This Division sets out rules that apply to affected information recipients in relation to their handling of their regulated information.

If an affected information recipient is an APP entity, the rules apply in relation to the regulated information of the recipient in addition to, or instead of, any relevant Australian Privacy Principles.

Subdivision A—Consideration of information privacy

22A  Open and transparent management of regulated information

(1) The object of this section is to ensure that an affected information recipient manages the regulated information of the recipient in an open and transparent way.

Compliance with this Division etc.

(2) An affected information recipient must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the recipient’s functions or activities that:
(a) will ensure that the recipient complies with this Division and the registered CR code if it binds the recipient; and
(b) will enable the recipient to deal with inquiries or complaints from individuals about the recipient’s compliance with this Division or the registered CR code if it binds the recipient.
Policy about the management of regulated information

(3) An affected information recipient must have a clearly expressed and up-to-date policy about the recipient’s management of the regulated information of the recipient.

(4) Without limiting subsection (3), the policy of the affected information recipient must contain the following information:

(a) the kinds of regulated information that the recipient collects and holds, and how the recipient collects and holds that information;

(b) the purposes for which the recipient collects, holds, uses and discloses regulated information;

(c) how an individual may access regulated information about the individual that is held by the recipient and seek the correction of such information;

(d) how an individual may complain about a failure of the recipient to comply with this Division or the registered CR code if it binds the recipient;

(e) how the recipient will deal with such a complaint.

Availability of policy etc.

(5) An affected information recipient must take such steps as are reasonable in the circumstances to make the policy available:

(a) free of charge; and

(b) in such form as is appropriate.

Note: An affected information recipient will usually make the policy available on the recipient’s website.

(6) If a person or body requests a copy, in a particular form, of the policy of an affected information recipient, the recipient must take such steps as are reasonable in the circumstances to give the person or body a copy in that form.
Part IIIA Credit reporting
Division 4 Affected information recipients

Section 22B

Interaction with the Australian Privacy Principles

(7) If an affected information recipient is an APP entity, Australian Privacy Principles 1.3 and 1.4 do not apply to the recipient in relation to the regulated information of the recipient.

Subdivision B—Dealing with regulated information

22B Additional notification requirements for affected information recipients

If an affected information recipient is an APP entity, then the matters for the purposes of Australian Privacy Principle 5.1 include the following matters to the extent that the personal information referred to in that principle is regulated information of the recipient:

(a) that the policy (the credit reporting policy) of the recipient that is referred to in subsection 22A(3) contains information about how an individual may access the regulated information about the individual that is held by the recipient, and seek the correction of such information;

(b) that the credit reporting policy of the recipient contains information about how an individual may complain about a failure of the recipient to comply with this Division or the registered CR code if it binds the recipient; and

(c) that the credit reporting policy of the recipient contains information about how the recipient will deal with such a complaint.

22C Use or disclosure of information by mortgage insurers or trade insurers

Prohibition on use or disclosure

(1) If:

(a) a mortgage insurer or trade insurer holds or held personal information about an individual; and
Section 22C

(b) the information was disclosed to the insurer by a credit reporting body or credit provider under Division 2 or 3 of this Part;

the insurer must not use or disclose the information, or any personal information about the individual derived from that information.

Civil penalty: 2,000 penalty units.

Permitted uses

(2) Subsection (1) does not apply to the use of the information if:

(a) for a mortgage insurer—the use is for:

(i) a mortgage insurance purpose of the insurer in relation to the individual; or

(ii) any purpose arising under a contract for mortgage insurance that has been entered into between the credit provider and the insurer; or

(b) for a trade insurer—the use is for a trade insurance purpose of the insurer in relation to the individual; or

(c) the use is required or authorised by or under an Australian law or a court/tribunal order.

Permitted disclosure

(3) Subsection (1) does not apply to the disclosure of the information if the disclosure is required or authorised by or under an Australian law or a court/tribunal order.

Interaction with the Australian Privacy Principles

(4) If the mortgage insurer or trade insurer is an APP entity, Australian Privacy Principles 6, 7 and 8 do not apply to the insurer in relation to the information.

(5) If:

(a) the mortgage insurer or trade insurer is an APP entity; and

Privacy Act 1988

Compilation No. 78

Compilation date: 1/7/18

Registered: 30/7/18
Part IIA  Credit reporting
Division 4  Affected information recipients

Section 22D

(b) the information is a government related identifier of the individual;

Australian Privacy Principle 9.2 does not apply to the insurer in relation to the information.

22D  Use or disclosure of information by a related body corporate

Prohibition on use or disclosure

(1) If:

(a) a body corporate holds or held credit eligibility information about an individual; and

(b) the information was disclosed to the body by a credit provider under paragraph 21G(3)(b);

the body must not use or disclose the information, or any personal information about the individual derived from that information.

Civil penalty: 1,000 penalty units.

Permitted use or disclosure

(2) Subsection (1) does not apply to the use or disclosure of the information by the body corporate if the body would be permitted to use or disclose the information under section 21G if the body were the credit provider.

(3) In determining whether the body corporate would be permitted to use or disclose the information under section 21G, assume that the body is whichever of the following is applicable:

(a) the credit provider that has provided the relevant credit to the individual;

(b) the credit provider to which the relevant application for credit was made by the individual.
Interaction with the Australian Privacy Principles

(4) If the body corporate is an APP entity, Australian Privacy Principles 6, 7 and 8 do not apply to the body in relation to the information.

(5) If:
   (a) the body corporate is an APP entity; and
   (b) the information is a government related identifier of the individual;
Australian Privacy Principle 9.2 does not apply to the body in relation to the information.

22E Use or disclosure of information by credit managers etc.

Prohibition on use or disclosure

(1) If:
   (a) a person holds or held credit eligibility information about an individual; and
   (b) the information was disclosed to the person by a credit provider under paragraph 21G(3)(c);
the person must not use or disclose the information, or any personal information about the individual derived from that information.

Civil penalty: 1,000 penalty units.

Permitted uses

(2) Subsection (1) does not apply to the use of the information if:
   (a) the person uses the information for the purpose for which it was disclosed to the person under paragraph 21G(3)(c); or
   (b) the use is required or authorised by or under an Australian law or a court/tribunal order.
Part IIIA Credit reporting

Division 4 Affected information recipients

Section 22F

Permitted disclosure

(3) Subsection (1) does not apply to the disclosure of the information if:
   (a) the disclosure is to the credit provider; or
   (b) the disclosure is required or authorised by or under an
       Australian law or a court/tribunal order.

Interaction with the Australian Privacy Principles

(4) If the person is an APP entity, Australian Privacy Principles 6, 7
    and 8 do not apply to the person in relation to the information.

(5) If:
   (a) the person is an APP entity; and
   (b) the information is a government related identifier of the
       individual;

          Australian Privacy Principle 9.2 does not apply to the person in
          relation to the information.

22F Use or disclosure of information by advisers etc.

Prohibition on use or disclosure

(1) If:
   (a) any of the following (the recipient) holds or held credit
       eligibility information about an individual:
       (i) an entity;
       (ii) a professional legal adviser of the entity;
       (iii) a professional financial adviser of the entity; and
   (b) the information was disclosed to the recipient by a credit
       provider under subsection 21N(2);

          the recipient must not use or disclose the information, or any
          personal information about the individual derived from that
          information.

          Civil penalty: 1,000 penalty units.
Permitted uses

(2) Subsection (1) does not apply to the use of the information if:
   (a) for a recipient that is the entity—the information is used for a matter referred to in subsection 21N(3); or
   (b) for a recipient that is the professional legal adviser, or professional financial adviser, of the entity—the information is used:
      (i) in the adviser’s capacity as an adviser of the entity; and
      (ii) in connection with advising the entity about a matter referred to in subsection 21N(3); or
   (c) the use is required or authorised by or under an Australian law or a court/tribunal order.

Permitted disclosure

(3) Subsection (1) does not apply to the disclosure of the information if the disclosure is required or authorised by or under an Australian law or a court/tribunal order.

Interaction with the Australian Privacy Principles

(4) If the recipient is an APP entity, Australian Privacy Principles 6, 7 and 8 do not apply to the recipient in relation to the information.

(5) If:
   (a) the recipient is an APP entity; and
   (b) the information is a government related identifier of the individual;
Australian Privacy Principle 9.2 does not apply to the recipient in relation to the information.
Division 5—Complaints

Guide to this Division

This Division deals with complaints about credit reporting bodies or credit providers.

Individuals may complain to credit reporting bodies or credit providers about acts or practices that may be a breach of certain provisions of this Part or the registered CR code.

If a complaint is made, the respondent for the complaint must investigate the complaint and make a decision about the complaint.

23A Individual may complain about a breach of a provision of this Part etc.

Complaint

(1) An individual may complain to a credit reporting body about an act or practice engaged in by the body that may be a breach of either of the following provisions in relation to the individual:
   (a) a provision of this Part (other than section 20R or 20T);
   (b) a provision of the registered CR code (other than a provision that relates to that section).

Note: A complaint about a breach of section 20R or 20T, or a provision of the registered CR code that relates to that section, may be made to the Commissioner under Part V.

(2) An individual may complain to a credit provider about an act or practice engaged in by the provider that may be a breach of either of the following provisions in relation to the individual:
   (a) a provision of this Part (other than section 21T or 21V);
   (b) a provision of the registered CR code (other than a provision that relates to that section) if it binds the credit provider.
Section 23B

Nature of complaint

(3) If an individual makes a complaint, the individual must specify the nature of the complaint.

(4) The complaint may relate to personal information that has been destroyed or de-identified.

No charge

(5) The credit reporting body or credit provider must not charge the individual for the making of the complaint or for dealing with the complaint.

23B Dealing with complaints

(1) If an individual makes a complaint under section 23A, the respondent for the complaint:

(a) must, within 7 days after the complaint is made, give the individual a written notice that:

(i) acknowledges the making of the complaint; and

(ii) sets out how the respondent will deal with the complaint; and

(b) must investigate the complaint.

Consultation about the complaint

(2) If the respondent for the complaint considers that it is necessary to consult a credit reporting body or credit provider about the complaint, the respondent must consult the body or provider.

(3) The use or disclosure of personal information about the individual for the purposes of the consultation is taken, for the purposes of this Act, to be a use or disclosure that is authorised by this subsection.
Part IIIA  Credit reporting  
Division 5  Complaints

Section 23C

Decision about the complaint

(4) After investigating the complaint, the respondent must, within the period referred to in subsection (5), make a decision about the complaint and give the individual a written notice that:
   (a) sets out the decision; and
   (b) states that, if the individual is not satisfied with the decision, the individual may:
       (i) access a recognised external dispute resolution scheme of which the respondent is a member; or
       (ii) make a complaint to the Commissioner under Part V.

(5) The period for the purposes of subsection (4) is:
   (a) the period of 30 days that starts on the day on which the complaint is made; or
   (b) such longer period as the individual has agreed to in writing.

23C  Notification requirements relating to correction complaints

(1) This section applies if an individual makes a complaint under section 23A about an act or practice that may breach section 20S or 21U (which deal with the correction of personal information by credit reporting bodies and credit providers).

Notification of complaint etc.

(2) If:
   (a) the respondent for the complaint is a credit reporting body; and
   (b) the complaint relates to credit information or credit eligibility information that a credit provider holds;

the respondent must, in writing:
   (c) notify the provider of the making of the complaint as soon as practicable after it is made; and
   (d) notify the provider of the making of a decision about the complaint under subsection 23B(4) as soon as practicable after it is made.
(3) If:
   (a) the respondent for the complaint is a credit provider; and
   (b) the complaint relates to:
       (i) credit reporting information that a credit reporting body holds; or
       (ii) credit information or credit eligibility information that another credit provider holds;
   the respondent must, in writing:
   (c) notify the body or other provider (as the case may be) of the making of the complaint as soon as practicable after it is made; and
   (d) notify the body or other provider (as the case may be) of the making of a decision about the complaint under subsection 23B(4) as soon as practicable after it is made.

Notification of recipients of disclosed information

(4) If:
   (a) a credit reporting body discloses credit reporting information to which the complaint relates under Division 2 of this Part; and
   (b) at the time of the disclosure, a decision about the complaint under subsection 23B(4) has not been made;
   the body must, at that time, notify in writing the recipient of the information of the complaint.

(5) If:
   (a) a credit provider discloses personal information to which the complaint relates under Division 3 of this Part or under the Australian Privacy Principles; and
   (b) at the time of the disclosure, a decision about the complaint under subsection 23B(4) has not been made;
   the provider must, at that time, notify in writing the recipient of the information of the complaint.
Part IIIA Credit reporting
Division 5 Complaints

Section 23C

Exceptions

(6) Subsection (2), (3), (4) or (5) does not apply if:
(a) it is impracticable for the credit reporting body or credit provider to give the notification under that subsection; or
(b) the credit reporting body or credit provider is required by or under an Australian law, or a court/tribunal order, not to give the notification under that subsection.
Division 6—Unauthorised obtaining of credit reporting information etc.

24 Obtaining credit reporting information from a credit reporting body

Offences

(1) An entity commits an offence if:
   (a) the entity obtains credit reporting information; and
   (b) the information is obtained from a credit reporting body; and
   (c) the entity is not:
      (i) an entity to which the body is permitted to disclose the
          information under Division 2 of this Part; or
      (ii) an access seeker for the information.

Penalty: 200 penalty units.

(2) An entity commits an offence if:
   (a) the entity obtains credit reporting information; and
   (b) the information is obtained from a credit reporting body; and
   (c) the information is obtained by false pretence.

Penalty: 200 penalty units.

Civil penalties

(3) An entity must not obtain credit reporting information from a credit reporting body if the entity is not:
   (a) an entity to which the body is permitted to disclose the
       information under Division 2 of this Part; or
   (b) an access seeker for the information.

Civil penalty: 2,000 penalty units.

(4) An entity must not obtain, by false pretence, credit reporting information from a credit reporting body.
Section 24A

Civil penalty: 2,000 penalty units.

24A Obtaining credit eligibility information from a credit provider

Offences

(1) An entity commits an offence if:
   (a) the entity obtains credit eligibility information; and
   (b) the information is obtained from a credit provider; and
   (c) the entity is not:
      (i) an entity to which the provider is permitted to disclose
          the information under Division 3 of this Part; or
      (ii) an access seeker for the information.

   Penalty: 200 penalty units.

(2) An entity commits an offence if:
   (a) the entity obtains credit eligibility information; and
   (b) the information is obtained from a credit provider; and
   (c) the information is obtained by false pretence.

   Penalty: 200 penalty units.

Civil penalties

(3) An entity must not obtain credit eligibility information from a credit provider if the entity is not:
   (a) an entity to which the provider is permitted to disclose the information under Division 3 of this Part; or
   (b) an access seeker for the information.

   Civil penalty: 2,000 penalty units.

(4) An entity must not obtain, by false pretence, credit eligibility information from a credit provider.

   Civil penalty: 2,000 penalty units.
Division 7—Court orders

25 Compensation orders

(1) The Federal Court or the Federal Circuit Court may order an entity to compensate a person for loss or damage (including injury to the person’s feelings or humiliation) suffered by the person if:
   (a) either:
       (i) a civil penalty order has been made against the entity for a contravention of a civil penalty provision (other than section 13G); or
       (ii) the entity is found guilty of an offence against this Part; and
   (b) that loss or damage resulted from the contravention or commission of the offence.

The order must specify the amount of compensation.

(2) The court may make the order only if:
   (a) the person applies for an order under this section; and
   (b) the application is made within 6 years of the day the cause of action that relates to the contravention or commission of the offence accrued.

(3) If the court makes the order, the amount of compensation specified in the order that is to be paid to the person may be recovered as a debt due to the person.

25A Other orders to compensate loss or damage

(1) This section applies if:
   (a) either:
       (i) a civil penalty order has been made against an entity for a contravention of a civil penalty provision (other than section 13G); or
       (ii) an entity is found guilty of an offence against this Part; and
Section 25A

(b) a person has suffered, or is likely to suffer, loss or damage (including injury to the person’s feelings or humiliation) as a result of the contravention or commission of the offence.

(2) The Federal Court or the Federal Circuit Court may make such order as the Court considers appropriate against the entity to:

(a) compensate the person, in whole or in part, for that loss or damage; or

(b) prevent or reduce that loss or damage suffered, or likely to be suffered, by the person.

(3) Without limiting subsection (2), examples of orders the court may make include:

(a) an order directing the entity to perform any reasonable act, or carry out any reasonable course of conduct, to redress the loss or damage suffered by the person; and

(b) an order directing the entity to pay the person a specified amount to reimburse the person for expenses reasonably incurred by the person in connection with the contravention or commission of the offence; and

(c) an order directing the defendant to pay to the person the amount of loss or damage the plaintiff suffered.

(4) The court may make the order only if:

(a) the person applies for an order under this section; and

(b) the application is made within 6 years of the day the cause of action that relates to the contravention or commission of the offence accrued.

(5) If the court makes an order that the entity pay an amount to the person, the person may recover the amount as a debt due to the person.
Part IIB—Privacy codes

Division 1—Introduction

26 Guide to this Part

This Part deals with privacy codes.

Division 2 deals with codes of practice about information privacy, called APP codes. APP code developers or the Commissioner may develop APP codes, which:

(a) must set out how one or more of the Australian Privacy Principles are to be applied or complied with; and

(b) may impose additional requirements to those imposed by the Australian Privacy Principles; and

(c) may deal with other specified matters.

If the Commissioner includes an APP code on the Codes Register, an APP entity bound by the code must not breach it. A breach of a registered APP code is an interference with the privacy of an individual.

Division 3 deals with a code of practice about credit reporting, called a CR code. CR code developers or the Commissioner may develop a CR code, which:

(a) must set out how one or more of the provisions of Part IIIA are to be applied or complied with; and

(b) must deal with matters required or permitted by Part IIIA to be provided for by the registered CR code; and
Part IIIB  Privacy codes
Division 1  Introduction

Section 26

(c) may deal with other specified matters.

If the Commissioner includes a CR code on the Codes Register, an entity bound by the code must not breach it. A breach of the registered CR code is an interference with the privacy of an individual.

Division 4 deals with the Codes Register, guidelines relating to codes and the review of the operation of registered codes.
Division 2—Registered APP codes

Subdivision A—Compliance with registered APP codes etc.

26A APP entities to comply with binding registered APP codes

An APP entity must not do an act, or engage in a practice, that breaches a registered APP code that binds the entity.

26B What is a registered APP code

(1) A registered APP code is an APP code:
   (a) that is included on the Codes Register; and
   (b) that is in force.

(2) A registered APP code is a legislative instrument.

(3) Subsection 12(2) (retrospective application of legislative instruments) of the Legislation Act 2003 does not apply to a registered APP code.

Note: An APP code cannot come into force before it is included on the Codes Register: see paragraph 26C(2)(c).

26C What is an APP code

(1) An APP code is a written code of practice about information privacy.

(2) An APP code must:
   (a) set out how one or more of the Australian Privacy Principles are to be applied or complied with; and
   (b) specify the APP entities that are bound by the code, or a way of determining the APP entities that are bound by the code; and
   (c) set out the period during which the code is in force (which must not start before the day the code is registered under section 26H).
Part IIIB  Privacy codes
Division 2  Registered APP codes

Section 26D

(3) An APP code may do one or more of the following:
   (a) impose additional requirements to those imposed by one or more of the Australian Privacy Principles, so long as the additional requirements are not contrary to, or inconsistent with, those principles;
   (b) cover an act or practice that is exempt within the meaning of subsection 7B(1), (2) or (3);
   (c) deal with the internal handling of complaints;
   (d) provide for the reporting to the Commissioner about complaints;
   (e) deal with any other relevant matters.

(4) An APP code may be expressed to apply to any one or more of the following:
   (a) all personal information or a specified type of personal information;
   (b) a specified activity, or a specified class of activities, of an APP entity;
   (c) a specified industry sector or profession, or a specified class of industry sectors or professions;
   (d) APP entities that use technology of a specified kind.

(5) An APP code is not a legislative instrument.

26D  Extension of Act to exempt acts or practices covered by registered APP codes

If a registered APP code covers an act or practice that is exempt within the meaning of subsection 7B(1), (2) or (3), this Act applies in relation to the code as if that act or practice were not exempt.
Subdivision B—Development and registration of APP codes

26E Development of APP codes by APP code developers

Own initiative

(1) An APP code developer may develop an APP code.

At the Commissioner’s request

(2) The Commissioner may, in writing, request an APP code developer to develop an APP code, and apply to the Commissioner for the code to be registered, if the Commissioner is satisfied it is in the public interest for the code to be developed.

(3) The request must:
   (a) specify the period within which the request must be complied with; and
   (b) set out the effect of section 26A.

(4) The period:
   (a) must run for at least 120 days from the date the request is made; and
   (b) may be extended by the Commissioner.

(5) The request may:
   (a) specify one or more matters that the APP code must deal with; and
   (b) specify the APP entities, or a class of APP entities, that should be bound by the code.

(6) Despite paragraph (5)(a), the Commissioner must not require an APP code to cover an act or practice that is exempt within the meaning of subsection 7B(1), (2) or (3). However, the APP code that is developed by the APP code developer may cover such an act or practice.

(7) The Commissioner must make a copy of the request publicly available as soon as practicable after the request is made.
Part III B  Privacy codes

Division 2  Registered APP codes

Section 26F

26F  Application for registration of APP codes

(1) If an APP code developer develops an APP code, the developer may apply to the Commissioner for registration of the code.

(2) Before making the application, the APP code developer must:

(a) make a draft of the APP code publicly available; and

(b) invite the public to make submissions to the developer about the draft within a specified period (which must run for at least 28 days); and

(c) give consideration to any submissions made within the specified period.

(3) The application must:

(a) be made in the form and manner specified by the Commissioner; and

(b) be accompanied by such information as is specified by the Commissioner.

(4) The APP code developer may vary the APP code at any time before the Commissioner registers the code, but only with the consent of the Commissioner.

26G  Development of APP codes by the Commissioner

(1) This section applies if the Commissioner made a request under subsection 26E(2) and either:

(a) the request has not been complied with; or

(b) the request has been complied with but the Commissioner has decided not to register, under section 26H, the APP code that was developed as requested.

(2) The Commissioner may develop an APP code if the Commissioner is satisfied that it is in public interest to develop the code. However, despite subsection 26C(3)(b), the APP code must not cover an act or practice that is exempt within the meaning of subsection 7B(1), (2) or (3).
(3) Before registering the APP code under section 26H, the Commissioner must:
   (a) make a draft of the code publicly available; and
   (b) invite the public to make submissions to the Commissioner about the draft within a specified period (which must run for at least 28 days); and
   (c) give consideration to any submissions made within the specified period.

26H Commissioner may register APP codes

(1) If:
   (a) an application for registration of an APP code is made under section 26F; or
   (b) the Commissioner develops an APP code under section 26G;
the Commissioner may register the code by including it on the Codes Register.

(2) In deciding whether to register the APP code, the Commissioner may:
   (a) consult any person the Commissioner considers appropriate; and
   (b) consider the matters specified in any relevant guidelines made under section 26V.

(3) If the Commissioner decides not to register an APP code developed by an APP code developer, the Commissioner must give written notice of the decision to the developer, including reasons for the decision.

Subdivision C—Variation and removal of registered APP codes

26J Variation of registered APP codes

(1) The Commissioner may, in writing, approve a variation of a registered APP code:
   (a) on his or her own initiative; or
Part III B Privacy codes
Division 2 Registered APP codes

Section 26 J

(b) on application by an APP entity that is bound by the code; or
(c) on application by a body or association representing one or more APP entities that are bound by the code.

(2) An application under paragraph (1)(b) or (c) must:
(a) be made in the form and manner specified by the Commissioner; and
(b) be accompanied by such information as is specified by the Commissioner.

(3) If the Commissioner varies a registered APP code on his or her own initiative, then, despite subsection 26 C(3)(b), the variation must not deal with an act or practice that is exempt within the meaning of subsection 7B(1), (2) or (3).

(4) Before deciding whether to approve a variation, the Commissioner must:
(a) make a draft of the variation publicly available; and
(b) consult any person the Commissioner considers appropriate about the variation; and
(c) consider the extent to which members of the public have been given an opportunity to comment on the variation.

(5) In deciding whether to approve a variation, the Commissioner may consider the matters specified in any relevant guidelines made under section 26 V.

(6) If the Commissioner approves a variation of a registered APP code (the original code), the Commissioner must:
(a) remove the original code from the Codes Register; and
(b) register the APP code, as varied, by including it on the Register.

(7) If the Commissioner approves a variation, the variation comes into effect on the day specified in the approval, which must not be before the day on which the APP code, as varied, is included on the Codes Register.

(8) An approval is not a legislative instrument.
26K Removal of registered APP codes

(1) The Commissioner may remove a registered APP code from the Codes Register:
   (a) on his or her own initiative; or
   (b) on application by an APP entity that is bound by the code; or
   (c) on application by a body or association representing one or more APP entities that are bound by the code.

(2) An application under paragraph (1)(b) or (c) must:
   (a) be made in the form and manner specified by the Commissioner; and
   (b) be accompanied by such information as is specified by the Commissioner.

(3) Before deciding whether to remove the registered APP code, the Commissioner must:
   (a) consult any person the Commissioner considers appropriate about the proposed removal; and
   (b) consider the extent to which members of the public have been given an opportunity to comment on the proposed removal.

(4) In deciding whether to remove the registered APP code, the Commissioner may consider the matters specified in any relevant guidelines made under section 26V.
Division 3—Registered CR code

Subdivision A—Compliance with the registered CR code

26L Entities to comply with the registered CR code if bound by the code

If an entity is bound by the registered CR code, the entity must not do an act, or engage in a practice, that breaches the code.

Note: There must always be one, and only one, registered CR code at all times after this Part commences: see subsection 26S(4).

26M What is the registered CR code

(1) The registered CR code is the CR code that is included on the Codes Register.

(2) The registered CR code is a legislative instrument.

(3) Subsection 12(2) (retrospective application of legislative instruments) of the Legislation Act 2003 does not apply to the registered CR code.

26N What is a CR code

(1) A CR code is a written code of practice about credit reporting.

(2) A CR code must:

(a) set out how one or more of the provisions of Part IIIA are to be applied or complied with; and

(b) make provision for, or in relation to, matters required or permitted by Part IIIA to be provided for by the registered CR code; and

(c) bind all credit reporting bodies; and

(d) specify the credit providers that are bound by the code, or a way of determining which credit providers are bound; and
Section 26P

(e) specify any other entities subject to Part IIIA that are bound by the code, or a way of determining which of those entities are bound.

(3) A CR code may do one or more of the following:
   (a) impose additional requirements to those imposed by Part IIIA, so long as the additional requirements are not contrary to, or inconsistent with, that Part;
   (b) deal with the internal handling of complaints;
   (c) provide for the reporting to the Commissioner about complaints;
   (d) deal with any other relevant matters.

(4) A CR code may be expressed to apply differently in relation to:
   (a) classes of entities that are subject to Part IIIA; and
   (b) specified classes of credit information, credit reporting information or credit eligibility information; and
   (c) specified classes of activities of entities that are subject to Part IIIA.

(5) A CR code is not a legislative instrument.

Subdivision B—Development and registration of CR code

26P Development of CR code by CR code developers

(1) The Commissioner may, in writing, request a CR code developer to develop a CR code and apply to the Commissioner for the code to be registered.

(2) The request must:
   (a) specify the period within which the request must be complied with; and
   (b) set out the effect of section 26L.

(3) The period:
   (a) must run for at least 120 days from the date the request is made; and
Section 26Q

(b) may be extended by the Commissioner.

(4) The request may:
   (a) specify one or more matters that the CR code must deal with; and
   (b) specify the credit providers, or a class of credit providers, that should be bound by the code; and
   (c) specify the other entities, or a class of other entities, subject to Part IIIA that should be bound by the code.

(5) The Commissioner must make a copy of the request publicly available as soon as practicable after the request is made.

26Q Application for registration of CR code

(1) If a CR code developer develops a CR code, the developer may apply to the Commissioner for registration of the code.

(2) Before making the application, the CR code developer must:
   (a) make a draft of the CR code publicly available; and
   (b) invite the public to make submissions to the developer about the draft within a specified period (which must run for at least 28 days); and
   (c) give consideration to any submissions made within the specified period.

(3) The application must:
   (a) be made in the form and manner specified by the Commissioner; and
   (b) be accompanied by such information as is specified by the Commissioner.

(4) The CR code developer may vary the CR code at any time before the Commissioner registers the code, but only with the consent of the Commissioner.
26R Development of CR code by the Commissioner

(1) The Commissioner may develop a CR code if the Commissioner made a request under section 26P and either:
   (a) the request has not been complied with; or
   (b) the request has been complied with but the Commissioner has decided not to register, under section 26S, the CR code that was developed as requested.

(2) Before registering the CR code under section 26S, the Commissioner must:
   (a) make a draft of the code publicly available; and
   (b) invite the public to make submissions to the Commissioner about the draft within a specified period (which must run for at least 28 days); and
   (c) give consideration to any submissions made within the specified period.

26S Commissioner may register CR code

(1) If:
   (a) an application for registration of a CR code is made under section 26Q; or
   (b) the Commissioner develops a CR code under section 26R; the Commissioner may register the code by including it on the Codes Register.

(2) In deciding whether to register the CR code, the Commissioner may:
   (a) consult any person the Commissioner considers appropriate; and
   (b) consider the matters specified in any guidelines made under section 26V.

(3) If the Commissioner decides not to register a CR code developed by a CR code developer, the Commissioner must give written notice of the decision to the developer, including reasons for the decision.
Part IIIB  Privacy codes
Division 3  Registered CR code

Section 26T

(4) The Commissioner must ensure that there is one, and only one, registered CR code at all times after this Part commences.

Subdivision C—Variation of the registered CR code

26T Variation of the registered CR code

(1) The Commissioner may, in writing, approve a variation of the registered CR code:
   (a) on his or her own initiative; or
   (b) on application by an entity that is bound by the code; or
   (c) on application by a body or association representing one or more of the entities that are bound by the code.

(2) An application under paragraph (1)(b) or (c) must:
   (a) be made in the form and manner specified by the Commissioner; and
   (b) be accompanied by such information as is specified by the Commissioner.

(3) Before deciding whether to approve a variation, the Commissioner must:
   (a) make a draft of the variation publicly available; and
   (b) consult any person the Commissioner considers appropriate about the variation; and
   (c) consider the extent to which members of the public have been given an opportunity to comment on the variation.

(4) In deciding whether to approve a variation, the Commissioner may consider the matters specified in any relevant guidelines made under section 26V.

(5) If the Commissioner approves a variation of the registered CR code (the original code), the Commissioner must:
   (a) remove the original code from the Codes Register; and
   (b) register the CR code, as varied, by including it on the Register.
Section 26T

(6) If the Commissioner approves a variation, the variation comes into effect on the day specified in the approval, which must not be before the day on which the CR code, as varied, is included on the Codes Register.

(7) An approval is not a legislative instrument.

Note: The CR code, as varied, is a legislative instrument once it is included on the Codes Register: see section 26M.
Part IIIB Privacy codes
Division 4 General matters

Section 26U

Division 4—General matters

26U Codes Register

(1) The Commissioner must keep a register (the Codes Register) which includes:
   (a) the APP codes the Commissioner has decided to register under section 26H; and
   (b) the APP codes the Commissioner must register under section 26J; and
   (c) the CR code the Commissioner has decided to register under section 26S; and
   (d) the CR code the Commissioner must register under section 26T.

(2) Despite subsection (1), the Commissioner is not required to include on the Codes Register:
   (a) an APP code removed from the Register under section 26J or 26K; or
   (b) the CR code removed from the Register under section 26T.

(3) The Commissioner must make the Codes Register available on the Commissioner’s website.

(4) The Commissioner may charge fees for providing copies of, or extracts from, the Codes Register.

26V Guidelines relating to codes

(1) The Commissioner may make written guidelines:
   (a) to assist APP code developers to develop APP codes; or
   (b) to assist APP entities bound by registered APP codes to apply or comply with the codes; or
   (c) to assist CR code developers to develop a CR code; or
   (d) to assist entities bound by the registered CR code to apply or comply with the code.
(2) The Commissioner may make written guidelines about matters the Commissioner may consider in deciding whether:
   (a) to register an APP code or a CR code; or
   (b) to approve a variation of a registered APP code or the registered CR code; or
   (c) to remove a registered APP code from the Codes Register.

(3) The Commissioner may publish any such guidelines on the Commissioner’s website.

(4) Guidelines are not a legislative instrument.

26W  Review of operation of registered codes

(1) The Commissioner may review the operation of a registered APP code.

   Note: The review may inform a decision by the Commissioner to approve a variation of a registered APP code or to remove a registered APP code from the Codes Register.

(2) The Commissioner may review the operation of the registered CR code.

   Note: The review may inform a decision by the Commissioner to approve a variation of the registered CR code.
Part IIIC—Notification of eligible data breaches

Division 1—Introduction

26WA  Simplified outline of this Part

- This Part sets up a scheme for notification of eligible data breaches.
- An eligible data breach happens if:
  (a) there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and
  (b) the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.
- An entity must give a notification if:
  (a) it has reasonable grounds to believe that an eligible data breach has happened; or
  (b) it is directed to do so by the Commissioner.

26WB  Entity

For the purposes of this Part, *entity* includes a person who is a file number recipient.

26WC  Deemed holding of information

*Overseas recipients*

(1) If:
  (a) an APP entity has disclosed personal information about one or more individuals to an overseas recipient; and
Section 26WD

(b) Australian Privacy Principle 8.1 applied to the disclosure of the personal information; and
(c) the overseas recipient holds the personal information;
this Part has effect as if:
(d) the personal information were held by the APP entity; and
(e) the APP entity were required under section 15 not to do an act, or engage in a practice, that breaches Australian Privacy Principle 11.1 in relation to the personal information.

Bodies or persons with no Australian link

(2) If:
   (a) either:
      (i) a credit provider has disclosed, under paragraph 21G(3)(b) or (c), credit eligibility information about one or more individuals to a related body corporate, or person, that does not have an Australian link; or
      (ii) a credit provider has disclosed, under subsection 21M(1), credit eligibility information about one or more individuals to a body or person that does not have an Australian link; and
   (b) the related body corporate, body or person holds the credit eligibility information;
this Part has effect as if:
(c) the credit eligibility information were held by the credit provider; and
(d) the credit provider were required to comply with subsection 21S(1) in relation to the credit eligibility information.

Note: See section 21NA.

26WD Exception—notification under the My Health Records Act 2012

If:
Part III C Notification of eligible data breaches
Division 1 Introduction

Section 26WD

(a) an unauthorised access to information; or
(b) an unauthorised disclosure of information; or
(c) a loss of information;
has been, or is required to be, notified under section 75 of the My Health Records Act 2012, this Part does not apply in relation to the access, disclosure or loss.
Notification of eligible data breaches  Part IIIC
Eligible data breach  Division 2

Section 26WE

Division 2—Eligible data breach

26WE  Eligible data breach

Scope

(1) This section applies if:

(a) both:
   (i) an APP entity holds personal information relating to one
       or more individuals; and
   (ii) the APP entity is required under section 15 not to do an
        act, or engage in a practice, that breaches Australian
        Privacy Principle 11.1 in relation to the personal
        information; or

(b) both:
   (i) a credit reporting body holds credit reporting
        information relating to one or more individuals; and
   (ii) the credit reporting body is required to comply with
        section 20Q in relation to the credit reporting
        information; or

(c) both:
   (i) a credit provider holds credit eligibility information
        relating to one or more individuals; and
   (ii) the credit provider is required to comply with
        subsection 21S(1) in relation to the credit eligibility
        information; or

(d) both:
   (i) a file number recipient holds tax file number
        information relating to one or more individuals; and
   (ii) the file number recipient is required under section 18
        not to do an act, or engage in a practice, that breaches a
        section 17 rule that relates to the tax file number
        information.
Part IIIC  Notification of eligible data breaches
Division 2  Eligible data breach

Section 26WF

Eligible data breach

(2) For the purposes of this Act, if:
   (a) both of the following conditions are satisfied:
       (i) there is unauthorised access to, or unauthorised disclosure of, the information;
       (ii) a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates; or
   (b) the information is lost in circumstances where:
       (i) unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and
       (ii) assuming that unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates;

   (c) the access or disclosure covered by paragraph (a), or the loss covered by paragraph (b), is an eligible data breach of the APP entity, credit reporting body, credit provider or file number recipient, as the case may be; and
   (d) an individual covered by subparagraph (a)(ii) or (b)(ii) is at risk from the eligible data breach.

(3) Subsection (2) has effect subject to section 26WF.

26WF Exception—remedial action

Access to, or disclosure of, information

(1) If:
   (a) an access to, or disclosure of, information is covered by paragraph 26WE(2)(a); and
Section 26WF

(b) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, takes action in relation to the access or disclosure; and

(c) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, does so before the access or disclosure results in serious harm to any of the individuals to whom the information relates; and

(d) as a result of the action, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to any of those individuals;

the access or disclosure is not, and is taken never to have been:

(e) an eligible data breach of the APP entity, credit reporting body, credit provider or file number recipient, as the case may be; or

(f) an eligible data breach of any other entity.

(2) If:

(a) an access to, or disclosure of, information is covered by paragraph 26WE(2)(a); and

(b) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, takes action in relation to the access or disclosure; and

(c) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, does so before the access or disclosure results in serious harm to a particular individual to whom the information relates; and

(d) as a result of the action, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to the individual;

this Part does not require:

(e) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be; or

(f) any other entity;

to take steps to notify the individual of the contents of a statement that relates to the access or disclosure.
Loss of information

(3) If:
   (a) a loss of information is covered by paragraph 26WE(2)(b); and
   (b) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, takes action in relation to the loss; and
   (c) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, does so before there is unauthorised access to, or unauthorised disclosure of, the information; and
   (d) as a result of the action, there is no unauthorised access to, or unauthorised disclosure of, the information;

the loss is not, and is taken never to have been:

(e) an eligible data breach of the APP entity, credit reporting body, credit provider or file number recipient, as the case may be; or

(f) an eligible data breach of any other entity.

(4) If:
   (a) a loss of information is covered by paragraph 26WE(2)(b); and
   (b) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, takes action in relation to the loss; and
   (c) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, does so:
      (i) after there is unauthorised access to, or unauthorised disclosure of, the information; and
      (ii) before the access or disclosure results in serious harm to any of the individuals to whom the information relates; and

   (d) as a result of the action, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to any of those individuals;
the loss is not, and is taken never to have been:

(e) an eligible data breach of the APP entity, credit reporting body, credit provider or file number recipient, as the case may be; or

(f) an eligible data breach of any other entity.

(5) If:

(a) a loss of information is covered by paragraph 26WE(2)(b); and

(b) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, takes action in relation to the loss; and

(c) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, does so:

(i) after there is unauthorised access to, or unauthorised disclosure of, the information; and

(ii) before the access or disclosure results in serious harm to a particular individual to whom the information relates; and

(d) as a result of the action, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to the individual;

this Part does not require:

(e) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be; or

(f) any other entity;

to take steps to notify the individual of the contents of a statement that relates to the loss.

26WG Whether access or disclosure would be likely, or would not be likely, to result in serious harm—relevant matters

For the purposes of this Division, in determining whether a reasonable person would conclude that an access to, or a disclosure of, information:

(a) would be likely; or
Part IIIC  Notification of eligible data breaches
Division 2  Eligible data breach

Section 26WG

(b) would not be likely;

to result in serious harm to any of the individuals to whom the
information relates, have regard to the following:

(c) the kind or kinds of information;

(d) the sensitivity of the information;

(e) whether the information is protected by one or more security
measures;

(f) if the information is protected by one or more security
measures—the likelihood that any of those security measures
could be overcome;

(g) the persons, or the kinds of persons, who have obtained, or
who could obtain, the information;

(h) if a security technology or methodology:

(i) was used in relation to the information; and

(ii) was designed to make the information unintelligible or
meaningless to persons who are not authorised to obtain
the information;

the likelihood that the persons, or the kinds of persons, who:

(iii) have obtained, or who could obtain, the information;

and

(iv) have, or are likely to have, the intention of causing harm
to any of the individuals to whom the information
relates;

have obtained, or could obtain, information or knowledge
required to circumvent the security technology or
methodology;

(i) the nature of the harm;

(j) any other relevant matters.

Note:  If the security technology or methodology mentioned in paragraph (h)
is encryption, an encryption key is an example of information required
to circumvent the security technology or methodology.
Notification of eligible data breaches  Part IIIC
Notification of eligible data breaches  Division 3

Section 26WH

Division 3—Notification of eligible data breaches

Subdivision A—Suspected eligible data breaches

26WH  Assessment of suspected eligible data breach

Scope

(1) This section applies if:
   (a) an entity is aware that there are reasonable grounds to suspect that there may have been an eligible data breach of the entity; and
   (b) the entity is not aware that there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach of the entity.

Assessment

(2) The entity must:
   (a) carry out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach of the entity; and
   (b) take all reasonable steps to ensure that the assessment is completed within 30 days after the entity becomes aware as mentioned in paragraph (1)(a).

Note: Section 26WK applies if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity.

26WJ  Exception—eligible data breaches of other entities

If:
   (a) an entity complies with section 26WH in relation to an eligible data breach of the entity; and
Section 26WK

(b) the access, disclosure or loss that constituted the eligible data breach of the entity is an eligible data breach of one or more other entities;

that section does not apply in relation to those eligible data breaches of those other entities.

Subdivision B—General notification obligations

26WK Statement about eligible data breach

Scope

(1) This section applies if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity.

Statement

(2) The entity must:

(a) both:

(i) prepare a statement that complies with subsection (3);

and

(ii) give a copy of the statement to the Commissioner; and

(b) do so as soon as practicable after the entity becomes so aware.

(3) The statement referred to in subparagraph (2)(a)(i) must set out:

(a) the identity and contact details of the entity; and

(b) a description of the eligible data breach that the entity has reasonable grounds to believe has happened; and

(c) the kind or kinds of information concerned; and

(d) recommendations about the steps that individuals should take in response to the eligible data breach that the entity has reasonable grounds to believe has happened.

(4) If the entity has reasonable grounds to believe that the access, disclosure or loss that constituted the eligible data breach of the entity is an eligible data breach of one or more other entities, the
statement referred to in subparagraph (2)(a)(i) may also set out the identity and contact details of those other entities.

26WL Entity must notify eligible data breach

Scope

(1) This section applies if:

(a) an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity; and

(b) the entity has prepared a statement that:
   (i) complies with subsection 26WK(3); and
   (ii) relates to the eligible data breach that the entity has reasonable grounds to believe has happened.

Notification

(2) The entity must:

(a) if it is practicable for the entity to notify the contents of the statement to each of the individuals to whom the relevant information relates—take such steps as are reasonable in the circumstances to notify the contents of the statement to each of the individuals to whom the relevant information relates; or

(b) if it is practicable for the entity to notify the contents of the statement to each of the individuals who are at risk from the eligible data breach—take such steps as are reasonable in the circumstances to notify the contents of the statement to each of the individuals who are at risk from the eligible data breach; or

(c) if neither paragraph (a) nor (b) applies:
   (i) publish a copy of the statement on the entity’s website (if any); and
   (ii) take reasonable steps to publicise the contents of the statement.

Note: See also subsections 26WF(2) and (5), which deal with remedial action.
Section 26WM

(3) The entity must comply with subsection (2) as soon as practicable after the completion of the preparation of the statement.

Method of providing a statement to an individual

(4) If the entity normally communicates with a particular individual using a particular method, the notification to the individual under paragraph (2)(a) or (b) may use that method. This subsection does not limit paragraph (2)(a) or (b).

26WM Exception—eligible data breaches of other entities

If:

(a) an entity complies with sections 26WK and 26WL in relation to an eligible data breach of the entity; and

(b) the access, disclosure or loss that constituted the eligible data breach of the entity is an eligible data breach of one or more other entities;

those sections do not apply in relation to those eligible data breaches of those other entities.

26WN Exception—enforcement related activities

If:

(a) an entity is an enforcement body; and

(b) the chief executive officer of the enforcement body believes on reasonable grounds that there has been an eligible data breach of the entity; and

(c) the chief executive officer of the enforcement body believes on reasonable grounds that compliance with section 26WL in relation to the eligible data breach would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, the enforcement body;

paragraph 26WK(3)(d) and section 26WL do not apply in relation to:

(d) the eligible data breach of the entity; and
(e) if the access, disclosure or loss that constituted the eligible data breach of the entity is an eligible data breach of one or more other entities—such an eligible data breach of those other entities.

26WP Exception—inconsistency with secrecy provisions

Secrecy provisions

(1) For the purposes of this section, secrecy provision means a provision that:

(a) is a provision of a law of the Commonwealth (other than this Act); and

(b) prohibits or regulates the use or disclosure of information.

(2) If compliance by an entity with subparagraph 26WK(2)(a)(ii) in relation to a statement would, to any extent, be inconsistent with a secrecy provision (other than a prescribed secrecy provision), subsection 26WK(2) does not apply to the entity, in relation to the statement, to the extent of the inconsistency.

(3) If compliance by an entity with section 26WL in relation to a statement would, to any extent, be inconsistent with a secrecy provision (other than a prescribed secrecy provision), section 26WL does not apply to the entity, in relation to the statement, to the extent of the inconsistency.

Prescribed secrecy provisions

(4) For the purposes of this section, prescribed secrecy provision means a secrecy provision that is specified in the regulations.

(5) For the purposes of a prescribed secrecy provision:

(a) subparagraph 26WK(2)(a)(ii); and

(b) section 26WL;

are taken not to be provisions that require or authorise the use or disclosure of information.
Section 26WQ

(6) If compliance by an entity with subparagraph 26WK(2)(a)(ii) in relation to a statement would, to any extent, be inconsistent with a prescribed secrecy provision, subsection 26WK(2) does not apply to the entity in relation to the statement.

(7) If compliance by an entity with section 26WL in relation to a statement would, to any extent, be inconsistent with a prescribed secrecy provision, section 26WL does not apply to the entity in relation to the statement.

26WQ Exception—declaration by Commissioner

(1) If the Commissioner:
   (a) is aware that there are reasonable grounds to believe that there has been an eligible data breach of an entity; or
   (b) is informed by an entity that the entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity;

the Commissioner may, by written notice given to the entity:
   (c) declare that sections 26WK and 26WL do not apply in relation to:
       (i) the eligible data breach of the entity; and
       (ii) if the access, disclosure or loss that constituted the eligible data breach of the entity is an eligible data breach of one or more other entities—such an eligible data breach of those other entities; or
   (d) declare that subsection 26WL(3) has effect in relation to:
       (i) the eligible data breach of the entity; and
       (ii) if the access, disclosure or loss that constituted the eligible data breach of the entity is an eligible data breach of one or more other entities—such an eligible data breach of those other entities;

as if that subsection required compliance with subsection 26WL(2) before the end of a period specified in the declaration.
(2) The Commissioner’s power in paragraph (1)(d) may only be used to extend the time for compliance with subsection 26WL(2) to the end of a period that the Commissioner is satisfied is reasonable in the circumstances.

(3) The Commissioner must not make a declaration under subsection (1) 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) any relevant advice given to the Commissioner by:
      (i) an enforcement body; or
      (ii) the Australian Signals Directorate;
   (c) such other matters (if any) as the Commissioner considers relevant.

(4) Paragraph (3)(b) does not limit the advice to which the Commissioner may have regard.

(5) The Commissioner may give a notice of a declaration to an entity under subsection (1):
   (a) on the Commissioner’s own initiative; or
   (b) on application made to the Commissioner by the entity.

Applications

(6) An application by an entity under paragraph (5)(b) may be expressed to be:
   (a) an application for a paragraph (1)(c) declaration; or
   (b) an application for a paragraph (1)(d) declaration; or
   (c) an application for:
      (i) a paragraph (1)(c) declaration; or
      (ii) in the event that the Commissioner is not disposed to make such a declaration—a paragraph (1)(d) declaration.

(7) If an entity applies to the Commissioner under paragraph (5)(b):
Part IIIA  Notification of eligible data breaches
Division 3  Notification of eligible data breaches

Section 26WQ

(a) the Commissioner may refuse the application; and
(b) if the Commissioner does so—the Commissioner must give written notice of the refusal to the entity.

(8) If:

(a) an application for a paragraph (1)(d) declaration nominates a period to be specified in the declaration; and
(b) the Commissioner makes the declaration, but specifies a different period in the declaration;

the Commissioner is taken not to have refused the application.

(9) If an entity applies to the Commissioner under paragraph (5)(b) for a declaration that, to any extent, relates to an eligible data breach of the entity, sections 26WK and 26WL do not apply in relation to:

(a) the eligible data breach; or
(b) if the access, disclosure or loss that constituted the eligible data breach of the entity is an eligible data breach of one or more other entities—such an eligible data breach of those other entities;

until the Commissioner makes a decision in response to the application for the declaration.

(10) An entity is not entitled to make an application under paragraph (5)(b) in relation to an eligible data breach of the entity if:

(a) the access, disclosure or loss that constituted the eligible data breach of the entity is an eligible data breach of one or more other entities; and
(b) one of those other entities has already made an application under paragraph (5)(b) in relation to the eligible data breach of the other entity.

Extension of specified period

(11) If notice of a paragraph (1)(d) declaration has been given to an entity, the Commissioner may, by written notice given to the entity, extend the period specified in the declaration.
Subdivision C—Commissioner may direct entity to notify eligible data breach

26WR Commissioner may direct entity to notify eligible data breach

(1) If the Commissioner is aware that there are reasonable grounds to believe that there has been an eligible data breach of an entity, the Commissioner may, by written notice given to the entity, direct the entity to:

(a) prepare a statement that complies with subsection (4); and
(b) give a copy of the statement to the Commissioner.

(2) The direction must also require the entity to:

(a) if it is practicable for the entity to notify the contents of the statement to each of the individuals to whom the relevant information relates—take such steps as are reasonable in the circumstances to notify the contents of the statement to each of the individuals to whom the relevant information relates; or

(b) if it is practicable for the entity to notify the contents of the statement to each of the individuals who are at risk from the eligible data breach—take such steps as are reasonable in the circumstances to notify the contents of the statement to each of the individuals who are at risk from the eligible data breach; or

(c) if neither paragraph (a) nor (b) applies:

(i) publish a copy of the statement on the entity’s website (if any); and

(ii) take reasonable steps to publicise the contents of the statement.

Note: See also subsections 26WF(2) and (5), which deal with remedial action.

(3) Before giving a direction to an entity under subsection (1), the Commissioner must invite the entity to make a submission to the Commissioner in relation to the direction within the period specified in the invitation.
Part III C  Notification of eligible data breaches
Division 3  Notification of eligible data breaches

Section 26WR

(4) The statement referred to in paragraph (1)(a) must set out:
   (a) the identity and contact details of the entity; and
   (b) a description of the eligible data breach that the Commissioner has reasonable grounds to believe has happened; and
   (c) the kind or kinds of information concerned; and
   (d) recommendations about the steps that individuals should take in response to the eligible data breach that the Commissioner has reasonable grounds to believe has happened.

(5) A direction under subsection (1) may also require the statement referred to in paragraph (1)(a) to set out specified information that relates to the eligible data breach that the Commissioner has reasonable grounds to believe has happened.

(6) In deciding whether to give a direction to an entity under subsection (1), the Commissioner must have regard to the following:
   (a) any relevant advice given to the Commissioner by:
      (i) an enforcement body; or
      (ii) the Australian Signals Directorate;
   (b) any relevant submission that was made by the entity:
      (i) in response to an invitation under subsection (3); and
      (ii) within the period specified in the invitation;
   (c) such other matters (if any) as the Commissioner considers relevant.

(7) Paragraph (6)(a) does not limit the advice to which the Commissioner may have regard.

(8) If the Commissioner is aware that there are reasonable grounds to believe that the access, disclosure or loss that constituted the eligible data breach of the entity is an eligible data breach of one or more other entities, a direction under subsection (1) may also require the statement referred to in paragraph (1)(a) to set out the identity and contact details of those other entities.
Method of providing a statement to an individual

(9) If an entity normally communicates with a particular individual using a particular method, the notification to the individual mentioned in paragraph (2)(a) or (b) may use that method. This subsection does not limit paragraph (2)(a) or (b).

Compliance with direction

(10) An entity must comply with a direction under subsection (1) as soon as practicable after the direction is given.

26WS Exception—enforcement related activities

An entity is not required to comply with a direction under subsection 26WR(1) if:
(a) the entity is an enforcement body; and
(b) the chief executive officer of the enforcement body believes on reasonable grounds that compliance with the direction would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, the enforcement body.

26WT Exception—inconsistency with secrecy provisions

Secrecy provisions

(1) For the purposes of this section, secrecy provision means a provision that:
(a) is a provision of a law of the Commonwealth (other than this Act); and
(b) prohibits or regulates the use or disclosure of information.

(2) If compliance by an entity with paragraph 26WR(1)(b) or subsection 26WR(2) in relation to a statement would, to any extent, be inconsistent with a secrecy provision (other than a prescribed secrecy provision), paragraph 26WR(1)(b) or subsection 26WR(2), as the case may be, does not apply to the entity, in relation to the statement, to the extent of the inconsistency.
Part III C Notification of eligible data breaches
Division 3 Notification of eligible data breaches

Section 26WT

Prescribed secrecy provisions

(3) For the purposes of this section, prescribed secrecy provision means a secrecy provision that is specified in the regulations.

(4) For the purposes of a prescribed secrecy provision:
   (a) paragraph 26WR(1)(b); and
   (b) subsection 26WR(2);
   are taken not to be provisions that require or authorise the use or disclosure of information.

(5) If compliance by an entity with paragraph 26WR(1)(b) or subsection 26WR(2) in relation to a statement would, to any extent, be inconsistent with a prescribed secrecy provision, paragraph 26WR(1)(b) or subsection 26WR(2), as the case may be, does not apply to the entity in relation to the statement.
Part IV—Functions of the Information Commissioner

Division 2—Functions of Commissioner

27 Functions of the Commissioner

(1) The Commissioner has the following functions:
   (a) the functions that are conferred on the Commissioner by or under:
      (i) this Act; or
      (ii) any other law of the Commonwealth;
   (b) the guidance related functions;
   (c) the monitoring related functions;
   (d) the advice related functions;
   (e) to do anything incidental or conducive to the performance of any of the above functions.

(2) The Commissioner has power to do all things necessary or convenient to be done for, or in connection with, the performance of the Commissioner’s functions.

(3) Without limiting subsection (2), the Commissioner may establish a panel of persons with expertise in relation to a particular matter to assist the Commissioner in performing any of the Commissioner’s functions.

(4) Section 38 of the Healthcare Identifiers Act 2010, rather than section 12B of this Act, applies in relation to an investigation of an act or practice referred to in subsection 29(1) of that Act in the same way as it applies to Parts 3 and 4 of that Act.

Note: Section 38 of the Healthcare Identifiers Act 2010 deals with the additional effect of Parts 3 and 4 of that Act.
28 Guidance related functions of the Commissioner

(1) The following are the guidance related functions of the Commissioner:

(a) making guidelines for the avoidance of acts or practices that may or might be interferences with the privacy of individuals, or which may otherwise have any adverse effects on the privacy of individuals;

(b) making, by legislative instrument, guidelines for the purposes of paragraph (d) of Australian Privacy Principle 6.3;

(c) promoting an understanding and acceptance of:
   (i) the Australian Privacy Principles and the objects of those principles; and
   (ii) a registered APP code; and
   (iii) the provisions of Part IIIA and the objects of those provisions; and
   (iv) the registered CR code;

(d) undertaking educational programs for the purposes of promoting the protection of individual privacy.

(2) The Commissioner may publish the guidelines referred to in paragraphs (1)(a) and (b) in such manner as the Commissioner considers appropriate.

(3) The educational programs referred to in paragraph (1)(d) may be undertaken by:

(a) the Commissioner; or

(b) a person or authority acting on behalf of the Commissioner.

(4) Guidelines made under paragraph (1)(a) are not a legislative instrument.

28A Monitoring related functions of the Commissioner

Credit reporting and tax file number information

(1) The following are the monitoring related functions of the Commissioner:
(a) monitoring the security and accuracy of information held by an entity that is information to which Part IIIA applies;
(b) examining the records of entities to ensure that the entities:
   (i) are not using information to which Part IIIA applies for unauthorised purposes; and
   (ii) are taking adequate measures to prevent the unlawful disclosure of such information;
(c) examining the records of the Commissioner of Taxation to ensure that the Commissioner:
   (i) is not using tax file number information for purposes beyond his or her powers; and
   (ii) is taking adequate measures to prevent the unlawful disclosure of the tax file number information that he or she holds;
(d) evaluating compliance with the rules issued under section 17;
(e) monitoring the security and accuracy of tax file number information kept by file number recipients.

Other matters

(2) The following are also the monitoring related functions of the Commissioner:
(a) examining a proposed enactment that would require or authorise acts or practices of an entity that might otherwise be interferences with the privacy of individuals, or which may otherwise have any adverse effects on the privacy of individuals;
(b) examining a proposal for data matching or linkage that may involve an interference with the privacy of individuals, or which may otherwise have any adverse effects on the privacy of individuals;
(c) ensuring that any adverse effects of the proposed enactment or the proposal on the privacy of individuals are minimised;
(d) undertaking research into, and monitoring developments in, data processing and technology (including data matching and
Part IV  Functions of the Information Commissioner

Division 2  Functions of Commissioner

Section 28B

linkage) to ensure that any adverse effects of such developments on the privacy of individuals are minimised;
(e) reporting to the Minister the results of that research and monitoring;
(f) monitoring and reporting on the adequacy of equipment and user safeguards.

(3) The functions referred to in paragraphs (2)(a) and (b) may be performed by the Commissioner:
(a) on request by a Minister; or
(b) on the Commissioner’s own initiative.

(4) If the reporting referred to in paragraph (2)(e) or (f) is done in writing, the instrument is not a legislative instrument.

28B  Advice related functions of the Commissioner

(1) The following are the advice related functions of the Commissioner:
(a) providing advice to a Minister or entity about any matter relevant to the operation of this Act;
(b) informing the Minister of action that needs to be taken by an agency in order to comply with the Australian Privacy Principles;
(c) providing reports and recommendations to the Minister in relation to any matter concerning the need for, or the desirability of, legislative or administrative action in the interests of the privacy of individuals;
(d) providing advice to file number recipients about:
   (i) their obligations under the Taxation Administration Act 1953 in relation to the confidentiality of tax file number information; or
   (ii) any matter relevant to the operation of this Act.

(2) The functions referred to in paragraphs (1)(a), (c) and (d) may be performed by the Commissioner on request or on the Commissioner’s own initiative.
(3) The Commissioner may perform the function referred to in paragraph (1)(b) whenever the Commissioners think it is necessary to do so.

(4) If the Minister is informed under paragraph (1)(b) in writing, or the report referred to in paragraph (1)(c) is provided in writing, the instrument is not a legislative instrument.

29 Commissioner must have due regard to the objects of the Act

The Commissioner must have due regard to the objects of this Act in performing the Commissioner’s functions, and exercising the Commissioner’s powers, conferred by this Act.

Note: The objects of this Act are set out in section 2A.
Division 3—Reports by Commissioner

30 Reports following investigation of act or practice

(1) Where the Commissioner has investigated an act or practice without a complaint having been made under section 36, the Commissioner may report to the Minister about the act or practice, and shall do so:

(a) if so directed by the Minister; or

(b) if the Commissioner:

(i) thinks that the act or practice is an interference with the privacy of an individual; and

(ii) does not consider that it is reasonably possible that the matter that gave rise to the investigation can be conciliated successfully or has attempted to conciliate the matter without success.

(2) Where the Commissioner reports under subsection (1) about an act done in accordance with a practice, the Commissioner shall also report to the Minister about the practice.

(3) Where, after an investigation of an act or practice of an agency, file number recipient, credit reporting body or credit provider that is an interference with the privacy of an individual under subsection 13(1), (2) or (4), the Commissioner is required by virtue of paragraph (1)(b) of this section to report to the Minister about the act or practice, the Commissioner:

(a) shall set out in the report his or her findings and the reasons for those findings;

(b) may include in the report any recommendations by the Commissioner for preventing a repetition of the act or a continuation of the practice;

(c) may include in the report any recommendation by the Commissioner for either or both of the following:
(i) the payment of compensation in respect of a person who has suffered loss or damage as a result of the act or practice;
(ii) the taking of other action to remedy or reduce loss or damage suffered by a person as a result of the act or practice;
(d) shall serve a copy of the report on the agency, file number recipient, credit reporting body or credit provider concerned and the Minister (if any) responsible for the agency, recipient, credit reporting body or credit provider; and
(e) may serve a copy of the report on any person affected by the act or practice.

(4) Where, at the end of 60 days after a copy of a report about an act or practice of an agency, file number recipient, credit reporting body or credit provider was served under subsection (3), the Commissioner:
(a) still thinks that the act or practice is an interference with the privacy of an individual; and
(b) is not satisfied that reasonable steps have been taken to prevent a repetition of the act or a continuation of the practice;
the Commissioner shall give to the Minister a further report that:
(c) incorporates the first-mentioned report and any document that the Commissioner has received, in response to the first-mentioned report, from the agency, file number recipient, credit reporting body or credit provider;
(d) states whether, to the knowledge of the Commissioner, any action has been taken as a result of the findings, and recommendations (if any), set out in the first-mentioned report and, if so, the nature of that action; and
(e) states why the Commissioner is not satisfied that reasonable steps have been taken to prevent a repetition of the act or a continuation of the practice;
and shall serve a copy of the report on the Minister (if any) responsible for the agency, recipient, credit reporting body or credit provider.
Part IV  Functions of the Information Commissioner  
Division 3  Reports by Commissioner

Section 31

(5) The Minister shall cause a copy of a report given to the Minister under subsection (4) to be laid before each House of the Parliament within 15 sitting days of that House after the report is received by the Minister.

31 Report following examination of proposed enactment

(1) Where the Commissioner has examined a proposed enactment under paragraph 28A(2)(a), subsections (2) and (3) of this section have effect.

(2) If the Commissioner thinks that the proposed enactment would require or authorise acts or practices of an entity that would be interferences with the privacy of individuals, the Commissioner shall:
   (a) report to the Minister about the proposed enactment; and
   (b) include in the report any recommendations he or she wishes to make for amendment of the proposed enactment to ensure that it would not require or authorise such acts or practices.

(3) Otherwise, the Commissioner may report to the Minister about the proposed enactment, and shall do so if so directed by the Minister.

(4) Where the Commissioner is of the belief that it is in the public interest that the proposed enactment should be the subject of a further report, the Commissioner may give to the Minister a further report setting out the Commissioner’s reasons for so doing.

(5) The Minister shall cause a copy of a report given under subsection (4) to be laid before each House of the Parliament as soon as practicable, and no later than 15 sitting days of that House, after the report is received by the Minister.

32 Commissioner may report to the Minister if the Commissioner has monitored certain activities etc.

(1) If the Commissioner has:
Functions of the Information Commissioner  
Part IV  
Reports by Commissioner  
Division 3

Section 33

(a) monitored an activity in the performance of a function under paragraph 28(1)(d), 28A(1)(a), (b), (d) or (e) or (2)(b), (c) or (d) or 28B(1)(b) or (c); or

(b) conducted an assessment under section 33C;

the Commissioner may report to the Minister about the activity or assessment, and must do so if so directed by the Minister.

(2) Where the Commissioner is of the belief that it is in the public interest that the activity or assessment should be the subject of a further report, the Commissioner may give to the Minister a further report setting out the Commissioner’s reasons for so doing.

(3) The Minister shall cause a copy of a report given under subsection (2) to be laid before each House of the Parliament as soon as practicable, and no later than 15 sitting days of that House, after the report is received by the Minister.

33 Exclusion of certain matters from reports

(1) In setting out findings, opinions and reasons in a report to be given under section 30, 31 or 32, the Commissioner may exclude a matter if the Commissioner considers it desirable to do so having regard to the obligations of the Commissioner under subsections (2) and (3).

(2) In deciding under subsection (1) whether or not to exclude matter from a report, the Commissioner shall have regard to the need to prevent:

(a) prejudice to the security, defence or international relations of Australia;

(b) prejudice to relations between the Commonwealth Government and the Government of a State or between the Government of a State and the Government of another State;

(c) the disclosure of deliberations or decisions of the Cabinet, or of a Committee of the Cabinet, of the Commonwealth or of a State;

(d) the disclosure of deliberations or advice of the Federal Executive Council or the Executive Council of a State;
Part IV  Functions of the Information Commissioner
Division 3  Reports by Commissioner

Section 33

(da) the disclosure of the deliberations or decisions of the Australian Capital Territory Executive or of a committee of that Executive;
(e) the disclosure, or the ascertaining by a person, of the existence or identity of a confidential source of information in relation to the enforcement of the criminal law;
(f) the endangering of the life or safety of any person;
(g) prejudice to the proper enforcement of the law or the protection of public safety;
(h) the disclosure of information the disclosure of which is prohibited, absolutely or subject to qualifications, by or under another enactment;
(j) the unreasonable disclosure of the personal affairs of any person; and
(k) the unreasonable disclosure of confidential commercial information.

(3) The Commissioner shall try to achieve an appropriate balance between meeting the need referred to in subsection (2) and the desirability of ensuring that interested persons are sufficiently informed of the results of the Commissioner’s investigation, examination or monitoring.

(4) Where the Commissioner excludes a matter from a report, he or she shall give to the Minister a report setting out the excluded matter and his or her reasons for excluding the matter.

Norfolk Island

(5) In this section:

State includes Norfolk Island.
Division 3A—Assessments by, or at the direction of, the Commissioner

33C Commissioner may conduct an assessment relating to the Australian Privacy Principles etc.

(1) The Commissioner may conduct an assessment of the following matters:
   (a) whether personal information held by an APP entity is being maintained and handled in accordance with the following:
      (i) the Australian Privacy Principles;
      (ii) a registered APP code that binds the entity;
   (b) whether information held by an entity is being maintained and handled in accordance with the following to the extent that they apply to the information:
      (i) the provisions of Part IIIA;
      (ii) the registered CR code if it binds the entity;
   (c) whether tax file number information held by a file number recipient is being maintained and handled in accordance with any relevant rules issued under section 17;
   (d) whether the data matching program (within the meaning of the Data-matching Program (Assistance and Tax) Act 1990) of an agency complies with Part 2 of that Act and the rules issued under section 12 of that Act;
   (e) whether information to which section 135AA of the National Health Act 1953 applies is being maintained and handled in accordance with the rules issued under that section.

(2) The Commissioner may conduct the assessment in such manner as the Commissioner considers fit.

33D Commissioner may direct an agency to give a privacy impact assessment

(1) If:
Part IV Functions of the Information Commissioner

Division 3A Assessments by, or at the direction of, the Commissioner

Section 33D

(a) an agency proposes to engage in an activity or function involving the handling of personal information about individuals; and

(b) the Commissioner considers that the activity or function might have a significant impact on the privacy of individuals;

the Commissioner may, in writing, direct the agency to give the Commissioner, within a specified period, a privacy impact assessment about the activity or function.

(2) A direction under subsection (1) is not a legislative instrument.

Privacy impact assessment

(3) A privacy impact assessment is a written assessment of an activity or function that:

(a) identifies the impact that the activity or function might have on the privacy of individuals; and

(b) sets out recommendations for managing, minimising or eliminating that impact.

(4) Subsection (3) does not limit the matters that the privacy impact assessment may deal with.

(5) A privacy impact assessment is not a legislative instrument.

Failure to comply with a direction

(6) If an agency does not comply with a direction under subsection (1), the Commissioner must advise both of the following of the failure:

(a) the Minister;

(b) if another Minister is responsible for the agency—that other Minister.

Review

(7) Before the fifth anniversary of the commencement of this section, the Minister must cause a review to be undertaken of whether this section should apply in relation to organisations.
Division 3B—Enforceable undertakings

33E Commissioner may accept undertakings

(1) The Commissioner may accept any of the following undertakings:
   (a) a written undertaking given by an entity that the entity will, in order to comply with this Act, take specified action;
   (b) a written undertaking given by an entity that the entity will, in order to comply with this Act, refrain from taking specified action;
   (c) a written undertaking given by an entity that the entity will take specified action directed towards ensuring that the entity does not do an act, or engage in a practice, in the future that interferes with the privacy of an individual.

(2) The undertaking must be expressed to be an undertaking under this section.

(3) The entity may withdraw or vary the undertaking at any time, but only with the consent of the Commissioner.

(4) The Commissioner may, by written notice given to the entity, cancel the undertaking.

(5) The Commissioner may publish the undertaking on the Commissioner’s website.

33F Enforcement of undertakings

(1) If:
   (a) an entity gives an undertaking under section 33E; and
   (b) the undertaking has not been withdrawn or cancelled; and
   (c) the Commissioner considers that the entity has breached the undertaking;

the Commissioner may apply to the Federal Court or Federal Circuit Court for an order under subsection (2).
(2) If the court is satisfied that the entity has breached the undertaking, the court may make any or all of the following orders:

(a) an order directing the entity to comply with the undertaking;

(b) any order that the court considers appropriate directing the person to compensate any other person who has suffered loss or damage as a result of the breach;

(c) any other order that the court considers appropriate.
Division 4—Miscellaneous

34 Provisions relating to documents exempt under the Freedom of Information Act 1982

(1) The Commissioner shall not, in connection with the performance of the Commissioner’s functions, give to a person information as to the existence or non-existence of a document where information as to the existence or non-existence of that document would, if included in a document of an agency, cause the last-mentioned document to be:

(a) an exempt document by virtue of section 33 or subsection 37(1) or 45A(1) of the Freedom of Information Act 1982; or

(b) an exempt document to the extent referred to in subsection 45A(2) or (3) of that Act.

(2) The Commissioner shall not, in connection with the performance of the Commissioner’s functions, give to a person information:

(a) about the contents of a document of an agency, or the contents of an official document of a Minister, being a document that is an exempt document; or

(b) about exempt matter contained in a document of an agency or in an official document of a Minister.

(3) An expression used in this section and in the Freedom of Information Act 1982 has the same meaning in this section as in that Act.

35 Direction where refusal or failure to amend exempt document

(1) Where:

(a) an application made under subsection 55(1) of the Freedom of Information Act 1982 for review of a decision under that Act refusing access to a document has been finally determined or otherwise disposed of;
Section 35

(b) the period within which an appeal may be made to the Federal Court has expired or, if such an appeal has been instituted, the appeal has been determined;

(c) the effect of the review and any appeal is that access is not to be given to the document;

(d) the applicant has requested the agency concerned to amend the document;

(e) the applicant has complained to the Commissioner under this Act about the refusal or failure of the agency to amend the document;

(f) the Commissioner has, as a result of the complaint, recommended under subsection 30(3) of this Act that the agency amend the document, or amend a part of the document, to which the applicant has been refused access; and

(g) as at the end of 60 days after a copy of the report containing the recommendation was served on the agency, the Commissioner:
   (i) still thinks that the agency should amend the document in a particular manner; and
   (ii) is not satisfied that the agency has amended the document in that manner;

the Commissioner may direct the agency to add to the document an appropriate notation setting out particulars of the amendments of the document that the Commissioner thinks should be made.

(2) An agency shall comply with a direction given in accordance with subsection (1).

(3) In subsection (1), amend, in relation to a document, means amend by making a correction, deletion or addition.

(4) An expression used in this section and in the Freedom of Information Act 1982 has the same meaning in this section as in that Act.
35A Commissioner may recognise external dispute resolution schemes

(1) The Commissioner may, by written notice, recognise an external dispute resolution scheme:
   (a) for an entity or a class of entities; or
   (b) for a specified purpose.

(2) In considering whether to recognise an external dispute resolution scheme, the Commissioner must take the following matters into account:
   (a) the accessibility of the scheme;
   (b) the independence of the scheme;
   (c) the fairness of the scheme;
   (d) the accountability of the scheme;
   (e) the efficiency of the scheme;
   (f) the effectiveness of the scheme;
   (g) any other matter the Commissioner considers relevant.

(3) The Commissioner may:
   (a) specify a period for which the recognition of an external dispute resolution scheme is in force; and
   (b) make the recognition of an external dispute resolution scheme subject to specified conditions, including conditions relating to the conduct of an independent review of the operation of the scheme; and
   (c) vary or revoke:
      (i) the recognition of an external dispute resolution scheme; or
      (ii) the period for which the recognition is in force; or
      (iii) a condition to which the recognition is subject.

(4) A notice under subsection (1) is not a legislative instrument.
Part V—Investigations etc.

Division 1A—Introduction

36A Guide to this Part

In general, this Part deals with complaints and investigations about acts or practices that may be an interference with the privacy of an individual.

An individual may complain to the Commissioner about an act or practice that may be an interference with the privacy of the individual. If a complaint is made, the Commissioner is required to investigate the act or practice except in certain circumstances.

The Commissioner may also, on his or her own initiative, investigate an act or practice that may be an interference with the privacy of an individual or a breach of Australian Privacy Principle 1.

The Commissioner has a range powers relating to the conduct of investigations including powers:

(a) to conciliate complaints; and
(b) to make preliminary inquiries of any person; and
(c) to require a person to give information or documents, or to attend a compulsory conference; and
(d) to transfer matters to an alternative complaint body in certain circumstances.
Section 36A

After an investigation, the Commissioner may make a determination in relation to the investigation. An entity to which a determination relates must comply with certain declarations included in the determination. Court proceedings may be commenced to enforce a determination.
Part V  Investigations etc.
Division 1  Investigation of complaints and investigations on the Commissioner’s initiative

Section 36

Division 1—Investigation of complaints and investigations on the Commissioner’s initiative

36 Complaints

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

(2) In the case of an act or practice that may be an interference with the privacy of 2 or more individuals, any one of those individuals may make a complaint under subsection (1) on behalf of all of the individuals.

(2A) In the case of a representative complaint, this section has effect subject to section 38.

(3) A complaint shall be in writing.

(4) It is the duty of:
   (a) members of the staff of the Commissioner; and
   (b) members of the staff of the Ombudsman who have had powers of the Commissioner delegated to them under section 99;
   to provide appropriate assistance to a person who wishes to make a complaint and requires assistance to formulate the complaint.

(5) The complaint shall specify the respondent to the complaint.

(6) In the case of a complaint about an act or practice of an agency:
   (a) if the agency is an individual or a body corporate, the agency shall be the respondent; and
   (b) if the agency is an unincorporated body, the principal executive of the agency shall be the respondent.

(7) In the case of a complaint about an act or practice of an organisation, the organisation is the respondent.
Note: Sections 98A to 98C contain further rules about how this Part operates in relation to respondent organisations that are not legal persons.

(8) The respondent to a complaint about an act or practice described in subsection 13(2), (4) or (5), other than an act or practice of an agency or organisation, is the person or entity who engaged in the act or practice.

37 Principal executive of agency

The principal executive of an agency of a kind specified in column 1 of an item in the following table is the person specified in column 2 of the item:

<table>
<thead>
<tr>
<th>Item</th>
<th>Column 1 Agency</th>
<th>Column 2 Principal executive</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Department</td>
<td>The Secretary of the Department</td>
</tr>
<tr>
<td>2</td>
<td>An unincorporated body, or a tribunal, referred to in paragraph (c) of the definition of agency in subsection 6(1)</td>
<td>The chief executive officer of the body or tribunal</td>
</tr>
<tr>
<td>3</td>
<td>A body referred to in paragraph (d) of the definition of agency in subsection 6(1)</td>
<td>The chief executive officer of the body</td>
</tr>
<tr>
<td>4</td>
<td>A federal court</td>
<td>The principal registrar of the court or the person occupying an equivalent office</td>
</tr>
<tr>
<td>5</td>
<td>The Australian Federal Police</td>
<td>The Commissioner of Police</td>
</tr>
<tr>
<td>5A</td>
<td>A public sector agency (within the meaning of the Public Sector Management Act 2000 of Norfolk Island)</td>
<td>The Chief Executive Officer (within the meaning of the Public Sector Management Act 2000 of Norfolk Island)</td>
</tr>
</tbody>
</table>
38 Conditions for making a representative complaint

(1) A representative complaint may be lodged under section 36 only if:
   (a) the class members have complaints against the same person or entity; and
   (b) all the complaints are in respect of, or arise out of, the same, similar or related circumstances; and
   (c) all the complaints give rise to a substantial common issue of law or fact.

(2) A representative complaint made under section 36 must:
   (a) describe or otherwise identify the class members; and
   (b) specify the nature of the complaints made on behalf of the class members; and
   (c) specify the nature of the relief sought; and
   (d) specify the questions of law or fact that are common to the complaints of the class members.
In describing or otherwise identifying the class members, it is not necessary to name them or specify how many there are.

(3) A representative complaint may be lodged without the consent of class members.

38A Commissioner may determine that a complaint is not to continue as a representative complaint

(1) The Commissioner may, on application by the respondent or on his or her own initiative, determine that a complaint should no longer continue as a representative complaint.

(2) The Commissioner may only make such a determination if the Commissioner is satisfied that it is in the interests of justice to do so for any of the following reasons:
   (a) the costs that would be incurred if the complaint were to continue as a representative complaint are likely to exceed the costs that would be incurred if each class member lodged a separate complaint;
   (b) the representative complaint will not provide an efficient and effective means of dealing with the complaints of the class members;
   (c) the complaint was not brought in good faith as a representative complaint;
   (d) it is otherwise inappropriate that the complaints be pursued by means of a representative complaint.

(3) If the Commissioner makes such a determination:
   (a) the complaint may be continued as a complaint by the complainant on his or her own behalf against the respondent; and
   (b) on the application of a person who was a class member for the purposes of the former representative complaint, the Commissioner may join that person as a complainant to the complaint as continued under paragraph (a).
**Part V**  Investigations etc.
**Division 1**  Investigation of complaints and investigations on the Commissioner’s initiative

**Section 38B**

38B  **Additional rules applying to the determination of representative complaints**

(1) The Commissioner may, on application by a class member, replace the complainant with another class member, where it appears to the Commissioner that the complainant is not able adequately to represent the interests of the class members.

(2) A class member may, by notice in writing to the Commissioner, withdraw from a representative complaint:
   (a) if the complaint was lodged without the consent of the member—at any time; or
   (b) otherwise—at any time before the Commissioner begins to hold an inquiry into the complaint.

Note: If a class member withdraws from a representative complaint that relates to a matter, the former member may make a complaint under section 36 that relates to the matter.

(3) The Commissioner may at any stage direct that notice of any matter be given to a class member or class members.

38C  **Amendment of representative complaints**

If the Commissioner is satisfied that a complaint could be dealt with as a representative complaint if the class of persons on whose behalf the complaint is lodged is increased, reduced or otherwise altered, the Commissioner may amend the complaint so that the complaint can be dealt with as a representative complaint.

39  **Class member for representative complaint not entitled to lodge individual complaint**

A person who is a class member for a representative complaint is not entitled to lodge a complaint in respect of the same subject matter.
40 Investigations

(1) Subject to subsection (1A), the Commissioner shall investigate an act or practice if:
   (a) the act or practice may be an interference with the privacy of an individual; and
   (b) a complaint about the act or practice has been made under section 36.

(1A) The Commissioner must not investigate a complaint if the complainant did not complain to the respondent before making the complaint to the Commissioner under section 36. However, the Commissioner may decide to investigate the complaint if he or she considers that it was not appropriate for the complainant to complain to the respondent.

(1B) Subsection (1A) does not apply if the complaint is about an act or practice that may breach:
   (a) section 20R, 20T, 21T or 21V (which are about access to, and correction of, credit reporting information etc.); or
   (b) a provision of the registered CR code that relates to that section.

(2) The Commissioner may, on the Commissioner’s own initiative, investigate an act or practice if:
   (a) the act or practice may be an interference with the privacy of an individual or a breach of Australian Privacy Principle 1; and
   (b) the Commissioner thinks it is desirable that the act or practice be investigated.

(3) This section has effect subject to section 41.

40A Conciliation of complaints

(1) If:
   (a) a complaint about an act or practice is made under section 36; and
Part V  Investigations etc.
Division 1  Investigation of complaints and investigations on the Commissioner’s initiative

Section 41

(b) the Commissioner considers it is reasonably possible that the complaint may be conciliated successfully;
the Commissioner must make a reasonable attempt to conciliate the complaint.

(2) Subsection (1) does not apply if the Commissioner has decided under section 41 or 50 not to investigate, or not to investigate further, the act or practice.

(3) If the Commissioner is satisfied that there is no reasonable likelihood that the complaint will be resolved by conciliation, the Commissioner must, in writing, notify the complainant and respondent of that matter.

(4) If a notification is given under subsection (3), the Commissioner may decide not to investigate, or not to investigate further, the act or practice.

(5) Evidence of anything said or done in the course of the conciliation is not admissible in any hearing before the Commissioner, or in any legal proceedings, relating to complaint or the act or practice unless:
   (a) the complainant and respondent otherwise agree; or
   (b) the thing was said or done in furtherance of the commission of a fraud or an offence, or the commission of an act that renders a person liable to a civil penalty.

41  Commissioner may or must decide not to investigate etc. in certain circumstances

(1) The Commissioner may decide not to investigate, or not to investigate further, an act or practice about which a complaint has been made under section 36 if the Commissioner is satisfied that:
   (a) the act or practice is not an interference with the privacy of an individual; or
   (c) the complaint was made more than 12 months after the complainant became aware of the act or practice; or
Investigations etc.  Part V
Investigation of complaints and investigations on the Commissioner’s initiative
Division 1

Section 41

(d) the complaint is frivolous, vexatious, misconceived, lacking in substance or not made in good faith; or
(da) an investigation, or further investigation, of the act or practice is not warranted having regard to all the circumstances; or
(db) the complainant has not responded, within the period specified by the Commissioner, to a request for information in relation to the complaint; or
(dc) the act or practice is being dealt with by a recognised external dispute resolution scheme; or
(dd) the act or practice would be more effectively or appropriately dealt with by a recognised external dispute resolution scheme; or
(e) the act or practice is the subject of an application under another Commonwealth law, or a State or Territory law, and the subject-matter of the complaint has been, or is being, dealt with adequately under that law; or
(f) another Commonwealth law, or a State or Territory law, provides a more appropriate remedy for the act or practice that is the subject of the complaint.

(1A) The Commissioner must not investigate, or investigate further, an act or practice about which a complaint has been made under section 36 if the Commissioner is satisfied that the complainant has withdrawn the complaint.

(2) The Commissioner may decide not to investigate, or not to investigate further, an act or practice about which a complaint has been made under section 36 if the Commissioner is satisfied that the complainant has complained to the respondent about the act or practice and either:
(a) the respondent has dealt, or is dealing, adequately with the complaint; or
(b) the respondent has not yet had an adequate opportunity to deal with the complaint.
Part V  Investigations etc.
Division 1  Investigation of complaints and investigations on the Commissioner’s initiative

Section 42

(3) The Commissioner may defer the investigation or further investigation of an act or practice about which a complaint has been made under section 36 if:

(a) an application has been made by the respondent for a determination under section 72 in relation to the act or practice; and

(b) the Commissioner is satisfied that the interests of persons affected by the act or practice would not be unreasonably prejudiced if the investigation or further investigation were deferred until the application had been disposed of.

42 Preliminary inquiries

(1) Where a complaint has been made to the Commissioner, the Commissioner may, for the purpose of determining:

(a) whether the Commissioner has power to investigate the matter to which the complaint relates; or

(b) whether the Commissioner may, in his or her discretion, decide not to investigate the matter;

make inquiries of the respondent or any other person.

(2) The Commissioner may make inquiries of any person for the purpose of determining whether to investigate an act or practice under subsection 40(2).

43 Conduct of investigations

(1) Before commencing an investigation of a matter to which a complaint relates, the Commissioner shall inform the respondent that the matter is to be investigated.

(1A) Before starting to investigate an act done, or practice engaged in, by a contracted service provider for the purpose of providing

Privacy Act 1988

Compilation No. 78  Compilation date: 1/7/18  Registered: 30/7/18

Authorised Version C2018C00292 registered 30/07/2018
Investigations etc.  Part V
Investigation of complaints and investigations on the Commissioner’s initiative
Division 1

Section 43

(directly or indirectly) a service to an agency under a Commonwealth contract, the Commissioner must also inform the agency that the act or practice is to be investigated.

Note: See subsection 6(9) about provision of services to an agency.

(2) An investigation under this Division shall be conducted in such manner as the Commissioner thinks fit.

(3) The Commissioner may, for the purposes of an investigation, obtain information from such persons, and make such inquiries, as he or she thinks fit.

(4) The Commissioner may make a determination under section 52 in relation to an investigation under this Division without holding a hearing, if:
   (a) it appears to the Commissioner that the matter to which the investigation relates can be adequately determined in the absence of:
      (i) in the case of an investigation under subsection 40(1)—the complainant and respondent; or
      (ii) otherwise—the person or entity that engaged in the act or practice that is being investigated; and
   (b) the Commissioner is satisfied that there are no unusual circumstances that would warrant the Commissioner holding a hearing; and
   (c) an application for a hearing has not been made under section 43A.

(7) Where, in connection with an investigation of a matter under this Division, the Commissioner proposes to hold a hearing, or proposes to make a requirement of a person under section 44, the Commissioner shall, if he or she has not previously informed the responsible Minister (if any) that the matter is being investigated, inform that Minister accordingly.

(8) The Commissioner may, either before or after the completion of an investigation under this Division, discuss any matter that is
Part V Investigations etc.
Division 1 Investigation of complaints and investigations on the Commissioner’s initiative

Section 43A

relevant to the investigation with a Minister concerned with the matter.

(8A) Subsection (8) does not allow the Commissioner to discuss a matter relevant to an investigation of a breach of the Australian Privacy Principles or a registered APP code with a Minister, unless the investigation is of an act done, or practice engaged in:

(a) by a contracted service provider for a Commonwealth contract; and

(b) for the purpose of providing a service to an agency to meet (directly or indirectly) an obligation under the contract.

(9) Where the Commissioner forms the opinion, either before or after completing an investigation under this Division, that there is evidence that an officer of an agency has been guilty of a breach of duty or of misconduct and that the evidence is, in all the circumstances, of sufficient force to justify the Commissioner doing so, the Commissioner shall bring the evidence to the notice of:

(a) an appropriate officer of an agency; or

(b) if the Commissioner thinks that there is no officer of an agency to whose notice the evidence may appropriately be drawn—an appropriate Minister.

43A Interested party may request a hearing

(1) An interested party in relation to an investigation under this Division may, in writing, request that the Commissioner hold a hearing before the Commissioner makes a determination under section 52 in relation to the investigation.

(2) If an interested party makes request under subsection (1), the Commissioner must:

(a) notify any other interested party of the request; and

(b) give all interested parties a reasonable opportunity to make a submission about the request; and

(c) decide whether or not to hold a hearing.
(3) In this section:

interested party in relation to an investigation means:

(a) in the case of an investigation under subsection 40(1)—the complainant or respondent; or

(b) otherwise—the person or entity that engaged in the act or practice that is being investigated.

44 Power to obtain information and documents

(1) If the Commissioner has reason to believe that a person has information or a document relevant to an investigation under this Division, the Commissioner may give to the person a written notice requiring the person:

(a) to give the information to the Commissioner in writing signed by the person or, in the case of a body corporate, by an officer of the body corporate; or

(b) to produce the document to the Commissioner.

(2) A notice given by the Commissioner under subsection (1) shall state:

(a) the place at which the information or document is to be given or produced to the Commissioner; and

(b) the time at which, or the period within which, the information or document is to be given or produced.

(2A) If documents are produced to the Commissioner in accordance with a requirement under subsection (1), the Commissioner:

(a) may take possession of, and may make copies of, or take extracts from, the documents; and

(b) may retain possession of the documents for any period that is necessary for the purposes of the investigation to which the documents relate; and

(c) during that period must permit a person who would be entitled to inspect any one or more of the documents if they were not in the Commissioner’s possession to inspect at all
Part V  Investigations etc.
Division 1  Investigation of complaints and investigations on the Commissioner’s initiative

Section 45

reasonable times any of the documents that the person would be so entitled to inspect.

(3) If the Commissioner has reason to believe that a person has information relevant to an investigation under this Division, the Commissioner may give to the person a written notice requiring the person to attend before the Commissioner at a time and place specified in the notice to answer questions relevant to the investigation.

(4) This section is subject to section 70 but it has effect regardless of any other enactment.

(5) A person is not liable to a penalty under the provisions of any other enactment because he or she gives information, produces a document or answers a question when required to do so under this Division.

45  Power to examine witnesses

(1) The Commissioner may administer an oath or affirmation to a person required under section 44 to attend before the Commissioner and may examine such a 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.

46  Directions to persons to attend compulsory conference

(1) For the purposes of performing the Commissioner’s functions in relation to a complaint, the Commissioner may, by written notice, direct:
   (a) the complainant;
   (b) the respondent; and
   (c) any other person who, in the opinion of the Commissioner, is likely to be able to provide information relevant to the matter to which the complaint relates or whose presence at the
conference is, in the opinion of the Commissioner, likely to assist in connection with the performance of the Commissioner’s functions in relation to the complaint; to attend, at a time and place specified in the notice, a conference presided over by the Commissioner.

(2) A person who has been directed to attend a conference and who:
(a) fails to attend as required by the direction; or
(b) fails to attend from day to day unless excused, or released from further attendance, by the Commissioner; commits an offence punishable on conviction:
(c) in the case of an individual—by imprisonment for a period not exceeding 6 months or a fine not exceeding 10 penalty units, or both; or
(d) in the case of a body corporate—by a fine not exceeding 50 penalty units.

(2A) Subsection (2) does not apply if the person has a reasonable excuse.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2A) (see subsection 13.3(3) of the Criminal Code).

(3) A person who has been directed under subsection (1) to attend a conference is entitled to be paid by the Commonwealth a reasonable sum for the person’s attendance at the conference.

(4) The Commissioner may, in a notice given to a person under subsection (1), require the person to produce such documents at the conference as are specified in the notice.

47 Conduct of compulsory conference

(1) The Commissioner may require a person attending a conference under this Division to produce a document.

(2) A conference under this Division shall be held in private and shall be conducted in such manner as the Commissioner thinks fit.
Part V Investigations etc.
Division 1 Investigation of complaints and investigations on the Commissioner’s initiative

Section 48

(3) A body of persons, whether corporate or unincorporate, that is directed under section 46 to attend a conference shall be deemed to attend if a member, officer or employee of that body attends on behalf of that body.

(4) Except with the consent of the Commissioner:

(a) an individual is not entitled to be represented at the conference by another person; and

(b) a body of persons, whether corporate or unincorporate, is not entitled to be represented at the conference by a person other than a member, officer or employee of that body.

48 Complainant and certain other persons to be informed of various matters

(1) Where the Commissioner decides not to investigate, or not to investigate further, a matter to which a complaint relates, the Commissioner shall, as soon as practicable and in such manner as the Commissioner thinks fit, inform the complainant and the respondent of the decision and of the reasons for the decision.

(2) If the Commissioner decides not to investigate (at all or further) an act done, or practice engaged in, by a contracted service provider for the purpose of providing (directly or indirectly) a service to an agency under a Commonwealth contract, the Commissioner must also inform the agency of the decision.

Note: See subsection 6(9) about provision of services to an agency.

49 Investigation under section 40 to cease if certain offences may have been committed

(1) Where, in the course of an investigation under section 40, the Commissioner forms the opinion that a tax file number offence, a healthcare identifier offence, an AML/CTF verification offence or a credit reporting offence may have been committed, the Commissioner shall:
Section 49

(a) inform the Commissioner of Police or the Director of Public Prosecutions of that opinion;

(b) in the case of an investigation under subsection 40(1), give a copy of the complaint to the Commissioner of Police or the Director of Public Prosecutions, as the case may be; and

(c) subject to subsection (3), discontinue the investigation except to the extent that it concerns matters unconnected with the offence that the Commissioner believes may have been committed.

(2) If, after having been informed of the Commissioner’s opinion under paragraph (1)(a), the Commissioner of Police or the Director of Public Prosecutions, as the case may be, decides that the matter will not be, or will no longer be, the subject of proceedings for an offence, he or she shall give a written notice to that effect to the Commissioner.

(3) Upon receiving such a notice the Commissioner may continue the investigation discontinued under paragraph (1)(c).

(4) In subsection (1):

**AML/CTF verification offence** (short for anti-money laundering and counter-terrorism financing offence) means an offence against section 35H, 35J or 35K of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.

**credit reporting offence** means:

(a) an offence against subsection 20P(1), 21R(1) or (2), 24(1) or (2) or 24A(1) or (2); or

(b) an offence against section 6 of the *Crimes Act 1914*, or section 11.1, 11.4 or 11.5 of the *Criminal Code*, being an offence that relates to an offence referred to in paragraph (a) of this definition.

**tax file number offence** means:

(a) an offence against section 8WA or 8WB of the *Taxation Administration Act 1953*; or
Part V  Investigations etc.
Division 1  Investigation of complaints and investigations on the Commissioner’s initiative

Section 49A

(b) an offence against section 6 of the Crimes Act 1914, or section 11.1, 11.4 or 11.5 of the Criminal Code, being an offence that relates to an offence referred to in paragraph (a) of this definition.

49A  Investigation under section 40 to cease if civil penalty provision under Personal Property Securities Act 2009 may have been contravened

(1) If, in the course of an investigation under section 40, the Commissioner forms the opinion that subsection 172(3) of the Personal Property Securities Act 2009 (civil penalty for searching otherwise than for authorised purposes) may have been contravened, the Commissioner must:

(a) inform the Registrar of Personal Property Securities under the Personal Property Securities Act 2009 of that opinion; and

(b) in the case of an investigation under subsection 40(1), give a copy of the complaint to the Registrar of Personal Property Securities; and

(c) discontinue the investigation except to the extent that it concerns matters unconnected with the contravention that the Commissioner believes may have taken place.

(2) The Registrar of Personal Property Securities must notify the Commissioner in writing if, after having been informed of the Commissioner’s opinion under paragraph (1)(a), the Registrar decides:

(a) not to apply for an order under section 222 of the Personal Property Securities Act 2009; or

(b) to discontinue a proceeding that is an application for an order under section 222 of that Act.

(3) Upon receiving a notice under subsection (2), the Commissioner may continue an investigation discontinued under paragraph (1)(c).
50 Reference of matters to other authorities

(1) In this section:

*alternative complaint body* means:

(a) the Australian Human Rights Commission; or
(b) the Ombudsman; or
(c) the Postal Industry Ombudsman; or
(d) the Overseas Students Ombudsman; or
(e) the Australian Public Service Commissioner; or
(g) a recognised external dispute resolution scheme.

*Australian Human Rights Commission* includes a person performing functions of that Commission.

*Ombudsman* means the Commonwealth Ombudsman.

(2) Where, before the Commissioner commences, or after the Commissioner has commenced, to investigate a matter to which a complaint relates, the Commissioner forms the opinion that:

(a) a complaint relating to that matter has been, or could have been, made by the complainant:

(i) to the Australian Human Rights Commission under Division 3 of Part II of the *Australian Human Rights Commission Act 1986*; or
(ii) to the Ombudsman under the *Ombudsman Act 1976*; or
(iia) to the Ombudsman under a particular Norfolk Island enactment; or
(iii) to the Postal Industry Ombudsman under the *Ombudsman Act 1976*; or
(iv) to the Overseas Students Ombudsman under the *Ombudsman Act 1976*; or
(v) to a recognised external dispute resolution scheme; or
(b) an application with respect to that matter has been, or could have been, made by the complainant to the Australian Public Service Commissioner under the *Public Service Act 1999*;
and that that matter could be more conveniently or effectively dealt with by the alternative complaint body, the Commissioner may decide not to investigate the matter, or not to investigate the matter further, as the case may be, and, if the Commissioner so decides, he or she shall:

(c) transfer the complaint to the alternative complaint body; and

(d) give notice in writing to the complainant stating that the complaint has been so transferred; and

(e) give to the alternative complaint body any information or documents that relate to the complaint and are in the possession, or under the control, of the Commissioner.

(3) A complaint transferred under subsection (2) shall be taken to be:

(a) a complaint made:

(i) to the Australian Human Rights Commission under Division 3 of Part II of the *Australian Human Rights Commission Act 1986*; or

(ii) to the Ombudsman under the *Ombudsman Act 1976*; or

(iia) to the Ombudsman under the Norfolk Island enactment concerned; or

(iii) to the Postal Industry Ombudsman under the *Ombudsman Act 1976*; or

(iv) to the Overseas Students Ombudsman under the *Ombudsman Act 1976*; or

(v) to the recognised external dispute resolution scheme; or

(b) an application made to the Australian Public Service Commissioner under the *Public Service Act 1999*; as the case requires.
50A Substitution of respondent to complaint

(1) This section lets the Commissioner substitute an agency for an organisation as respondent to a complaint if:
   (a) the organisation is a contracted service provider for a Commonwealth contract to provide services to the agency; and
   (b) before the Commissioner makes a determination under section 52 in relation to the complaint, the organisation:
      (i) dies or ceases to exist; or
      (ii) becomes bankrupt or insolvent, commences to be wound up, applies to take the benefit of a law for the relief of bankrupt or insolvent debtors, compounds with creditors or makes an assignment of any property for the benefit of creditors.

(2) The Commissioner may amend the complaint to specify as a respondent to the complaint the agency or its principal executive, instead of the organisation.

   Note 1: The complaint still relates to the act or practice of the organisation.

   Note 2: The Commissioner may determine under section 53B that the determination applies in relation to an agency if the organisation has not complied with the determination.

(3) Before amending the complaint, the Commissioner must:
   (a) give the agency a notice stating that the Commissioner proposes to amend the complaint and stating the reasons for the proposal; and
   (b) give the agency an opportunity to appear before the Commissioner and to make oral and/or written submissions relating to the proposed amendment.

(4) If the Commissioner amends the complaint after starting to investigate it, the Commissioner is taken to have satisfied subsection 43(1A) in relation to the agency.
Part V  Investigations etc.
Division 1  Investigation of complaints and investigations on the Commissioner’s initiative

Section 51

51 Effect of investigation by Auditor-General

Where the Commissioner becomes aware that a matter being investigated by the Commissioner is, or is related to, a matter that is under investigation by the Auditor-General, the Commissioner shall not, unless the Commissioner and Auditor-General agree to the contrary, continue to investigate the matter until the investigation by the Auditor-General has been completed.
Division 2—Determinations following investigation of complaints

52 Determination of the Commissioner

(1) After investigating a complaint, the Commissioner may:
   (a) make a determination dismissing the complaint; or
   (b) find the complaint substantiated and make a determination that includes one or more of the following:
      (i) a declaration:
         (A) where the principal executive of an agency is the respondent—that the agency has engaged in conduct constituting an interference with the privacy of an individual and must not repeat or continue such conduct; or
         (B) in any other case—that the respondent has engaged in conduct constituting an interference with the privacy of an individual and must not repeat or continue such conduct;
      (ia) a declaration that the respondent must take specified steps within a specified period to ensure that such conduct is not repeated or continued;
      (ii) a declaration that the respondent must perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant;
      (iii) a declaration that the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint;
      (iv) a declaration that it would be inappropriate for any further action to be taken in the matter.

(1A) After investigating an act or practice of a person or entity under subsection 40(2), the Commissioner may make a determination that includes one or more of the following:
Section 52

(a) a declaration that:
   (i) the act or practice is an interference with the privacy of
       one or more individuals; and
   (ii) the person or entity must not repeat or continue the act
        or practice;
(b) a declaration that the person or entity must take specified
    steps within a specified period to ensure that the act or
    practice is not repeated or continued;
(c) a declaration that the person or entity must perform any
    reasonable act or course of conduct to redress any loss or
    damage suffered by one or more of those individuals;
(d) a declaration that one or more of those individuals are
    entitled to a specified amount by way of compensation for
    any loss or damage suffered by reason of the act or practice;
(e) a declaration that it would be inappropriate for any further
    action to be taken in the matter.

(1AA) The steps specified by the Commissioner under
subparagraph (1)(b)(ia) or paragraph (1A)(b) must be reasonable
and appropriate.

(1AB) The loss or damage referred to in paragraph (1)(b) or
subsection (1A) includes:
   (a) injury to the feelings of the complainant or individual; and
   (b) humiliation suffered by the complainant or individual.

(1B) A determination of the Commissioner under subsection (1) or (1A)
is not binding or conclusive between any of the parties to the
determination.

(2) The Commissioner shall, in a determination, state any findings of
fact upon which the determination is based.

(3) In a determination under paragraph (1)(a) or (b) (other than a
determination made on a representative complaint), the
Commissioner may include a declaration that the complainant is
entitled to a specified amount to reimburse the complainant for
expenses reasonably incurred by the complainant in connection
with the making of the complaint and the investigation of the complaint.

(3A) A determination under paragraph (1)(b) or subsection (1A) may include any order that the Commissioner considers necessary or appropriate.

(4) A determination by the Commissioner under subparagraph (1)(b)(iii) on a representative complaint:

(a) may provide for payment of specified amounts or of amounts worked out in a manner specified by the Commissioner; and

(b) if the Commissioner provides for payment in accordance with paragraph (a), must make provision for the payment of the money to the complainants concerned.

(5) If the Commissioner makes a determination under subparagraph (1)(b)(iii) on a representative complaint, the Commissioner may give such directions (if any) as he or she thinks just in relation to:

(a) the manner in which a class member is to establish his or her entitlement to the payment of an amount under the determination; and

(b) the manner for determining any dispute regarding the entitlement of a class member to the payment.

(6) In this section:

complainant, in relation to a representative complaint, means the class members.

53 Determination must identify the class members who are to be affected by the determination

A determination under section 52 on a representative complaint must describe or otherwise identify those of the class members who are to be affected by the determination.
Part V  Investigations etc.
Division 2  Determinations following investigation of complaints

Section 53A

53A Notice to be given to outsourcing agency

(1) If the Commissioner makes a determination that applies in relation to a contracted service provider for a Commonwealth contract, the Commissioner:
   (a) must give a copy of the determination to each agency:
      (i) to which services are or were to be provided under the contract; and
      (ii) to which the Commissioner considers it appropriate to give a copy; and
   (b) may give such an agency a written recommendation of any measures that the Commissioner considers appropriate.

(2) The Commissioner may give an agency a recommendation only after consulting the agency.

(3) An agency that receives a recommendation from the Commissioner must tell the Commissioner in writing of any action the agency proposes to take in relation to the recommendation. The agency must do so within 60 days of receiving the recommendation.

53B Substituting an agency for a contracted service provider

(1) This section applies if:
   (a) a determination under section 52 applies in relation to a contracted service provider for a Commonwealth contract; and
   (b) the determination includes:
      (i) a declaration under subparagraph 52(1)(b)(iii) that the complainant is entitled to a specified amount by way of compensation; or
      (ia) a declaration under paragraph 52(1A)(d) that one or more individuals are entitled to a specified amount by way of the compensation; or
      (ii) a declaration under subsection 52(3) that the complainant is entitled to a specified amount by way of reimbursement; and
Investigations etc. Part V
Determinations following investigation of complaints Division 2

Section 53B

(c) at a particular time after the determination was made, the provider:
   (i) dies or ceases to exist; or
   (ii) becomes bankrupt or insolvent, commences to be wound up, applies to take the benefit of a law for the relief of bankrupt or insolvent debtors, compounds with creditors or makes an assignment of any property for the benefit of creditors; and
   (d) at that time, the complainant or individuals had not been paid the whole or part of an amount referred to in paragraph (b).

(2) The Commissioner may determine in writing that the determination under section 52 instead applies in relation to a specified agency to which services were or were to be provided under the contract. The determination has effect according to its terms for the purposes of section 60.

Note: This means that the amount owed by the contracted service provider will be a debt due by the agency to the complainant or individuals.

(3) Before making a determination, the Commissioner must give the agency:
   (a) a notice stating that the Commissioner proposes to make the determination and stating the reasons for the proposal; and
   (b) an opportunity to appear before the Commissioner and to make oral and/or written submissions relating to the proposed determination.
Section 54

Division 3—Enforcement

54 Application of Division

(1) This Division applies to a determination made under section 52 after the commencement of this Division, except where the determination applies in relation to an agency or the principal executive of an agency.

(2) In this section:

agency does not include an eligible hearing service provider.

55 Obligations of organisations and small business operators

If the determination applies in relation to an organisation or small business operator, the organisation or operator:

(a) must not repeat or continue conduct that is covered by a declaration included in the determination under sub-subparagraph 52(1)(b)(i)(B) or paragraph 52(1A)(a); and

(b) must take the steps that are specified in a declaration included in the determination under subparagraph 52(1)(b)(ia) or paragraph 52(1A)(b) within the specified period; and

(c) must perform the act or course of conduct that is covered by a declaration included in the determination under subparagraph 52(1)(b)(ii) or paragraph 52(1A)(c).

55A Proceedings in the Federal Court or Federal Circuit Court to enforce a determination

(1) The following persons may commence proceedings in the Federal Court or the Federal Circuit Court for an order to enforce a determination:

(a) if the determination was made under subsection 52(1)—the complainant;

(b) the Commissioner.
(2) If the court is satisfied that the person or entity in relation to which the determination applies has engaged in conduct that constitutes an interference with the privacy of an individual, the court may make such orders (including a declaration of right) as it thinks fit.

(3) The court may, if it thinks fit, grant an interim injunction pending the determination of the proceedings.

(4) The court is not to require a person, as a condition of granting an interim injunction, to give an undertaking as to damages.

(5) The court is to deal by way of a hearing de novo with the question whether the person or entity in relation to which the determination applies has engaged in conduct that constitutes an interference with the privacy of an individual.

(6) Despite subsection (5), the court may receive any of the following as evidence in proceedings about a determination made by the Commissioner under section 52:
   (a) a copy of the Commissioner’s written reasons for the determination;
   (b) a copy of any document that was before the Commissioner;
   (c) a copy of a record (including any tape recording) of any hearing before the Commissioner (including any oral submissions made).

(7A) In conducting a hearing and making an order under this section, the court is to have due regard to the objects of this Act.

(8) In this section:

   *complainant*, in relation to a representative complaint, means any of the class members.
Section 55B

55B Evidentiary certificate

(1) The Commissioner may issue a written certificate setting out the findings of fact upon which the Commissioner based his or her determination that:

(a) a specified APP entity had breached an Australian Privacy Principle; or

(b) a specified APP entity had breached a registered APP code that binds the entity.

(3) In any proceedings under section 55A, a certificate under subsection (1) of this section is prima facie evidence of the facts found by the Commissioner and set out in the certificate. However, the certificate is not prima facie evidence of a finding that:

(a) a specified APP entity had breached an Australian Privacy Principle; or

(b) a specified APP entity had breached a registered APP code that binds the entity.

(4) A document purporting to be a certificate under subsection (1) must, unless the contrary is established, be taken to be a certificate and to have been properly given.
Division 4—Review and enforcement of determinations involving Commonwealth agencies

57 Application of Division

(1) This Division applies to a determination that is made under section 52 and that applies in relation to an agency or the principal executive of an agency.

(2) In this section:

agency does not include an eligible hearing service provider.

58 Obligations of agencies

If this Division applies to a determination and the determination applies in relation to an agency, the agency:

(a) must not repeat or continue conduct that is covered by a declaration included in the determination under subparagraph 52(1)(b)(i) or paragraph 52(1A)(a); and

(b) must take the steps that are specified in a declaration included in the determination under subparagraph 52(1)(b)(ia) or paragraph 52(1A)(b) within the specified period; and

(c) must perform the act or course of conduct that is covered by a declaration included in the determination under subparagraph 52(1)(b)(ii) or paragraph 52(1A)(c).

59 Obligations of principal executive of agency

If this Division applies to a determination and the determination applies in relation to the principal executive of an agency, the principal executive must take all such steps as are reasonably within his or her power to ensure:

(a) that the terms of the determination are brought to the notice of all members, officers and employees of the agency whose
Part V  Investigations etc.
Division 4  Review and enforcement of determinations involving Commonwealth agencies

Section 60

duties are such that they may engage in conduct of the kind to which the determination relates; and

(b) that no member, officer or employee of the agency repeats or continues conduct that is covered by a declaration included in the determination under subparagraph 52(1)(b)(i) or paragraph 52(1A)(a); and

(ba) that the steps specified in a declaration included in the determination under subparagraph 52(1)(b)(ia) or paragraph 52(1A)(b) are taken within the specified period; and

(c) the performance of any act or course of conduct that is covered by a declaration included in the determination under subparagraph 52(1)(b)(ii) or paragraph 52(1A)(c).

60  Compensation and expenses

(1) If a determination to which this Division applies includes a declaration of the kind referred to in subparagraph 52(1)(b)(iii), paragraph 52(1A)(d) or subsection 52(3), the complainant or individual is entitled to be paid the amount specified in the declaration.

(2) If the determination applies in relation to an agency that has the capacity to sue and be sued, the amount is recoverable as a debt due by the agency to the complainant or individual. In any other case, the amount is recoverable as a debt due by the Commonwealth to the complainant or individual.

(2B) If a determination relates to a Norfolk Island agency, the reference in subsection (2) to the Commonwealth is to be read as a reference to Norfolk Island.

(3) In this section:

complainant, in relation to a representative complaint, means a class member.
62 Enforcement of determination against an agency

(1) If an agency fails to comply with section 58, an application may be made to the Federal Court or the Federal Circuit Court for an order directing the agency to comply.

(2) If the principal executive of an agency fails to comply with section 59, an application may be made to the Federal Court or the Federal Circuit Court for an order directing the principal executive to comply.

(3) The application may be made by:
   (a) if the determination was made under subsection 52(1)—the complainant; or
   (b) the Commissioner.

(4) On an application under this section, the court may make such other orders as it thinks fit with a view to securing compliance by the agency or principal executive.

(5) An application may not be made under this section in relation to a determination under section 52 until:
   (a) the time has expired for making an application under section 96 for review of the determination; or
   (b) if such an application is made, the decision of the Administrative Appeals Tribunal on the application has come into operation.

(6) In this section:

complainant, in relation to a representative complaint, means a class member.
Division 5—Miscellaneous

63 Legal assistance

(1) If:
   (a) the Commissioner has dismissed a file number complaint; and
   (b) the respondent to the complaint is not an agency or the principal executive of an agency;
the respondent may apply to the Attorney-General for assistance under this section.

(2) A person who:
   (a) has commenced or proposes to commence proceedings in the Federal Court or the Federal Circuit Court under section 55; or
   (b) has engaged in conduct or is alleged to have engaged in conduct in respect of which proceedings have been commenced in the Federal Court or the Federal Circuit Court under section 55;
may apply to the Attorney-General for the provision of assistance under this section in respect of the proceedings.

(2A) Subsection (2) does not permit an application relating to proceedings under section 55A to enforce a determination relating to a code complaint or an APP complaint.

(3) If the Attorney-General is satisfied that in all the circumstances it is reasonable to grant an application made under this section, he or she may authorise the provision by the Commonwealth to the applicant of:
   (a) in the case of an application under subsection (1)—such financial assistance in connection with the investigation of the complaint as the Attorney-General determines; or
   (b) in the case of an application under subsection (2)—such legal or financial assistance in respect of the proceeding as the Attorney-General determines.
Section 64

(4) An authorisation under subsection (3) may be made subject to such conditions (if any) as the Attorney-General determines.

(5) In considering an application made under this section, the Attorney-General must have regard to any hardship to the applicant that refusal of the application would involve.

64 Commissioner etc. not to be sued

Neither the Commissioner nor a person acting under his or her direction or authority is liable to an action, suit or proceeding in relation to an act done or omitted to be done in good faith in the exercise or purported exercise of any power or authority conferred by this Act.

65 Failure to attend etc. before Commissioner

(1) A person shall not:
   (a) refuse or fail to attend before the Commissioner; or
   (b) refuse or fail to be sworn or make an affirmation;
when so required under this Act.

Penalty: Imprisonment for 12 months or 20 penalty units, or both.

(2) Subsection (1) does not apply if the person has a reasonable excuse.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2) (see subsection 13.3(3) of the Criminal Code).

(3) A person shall not furnish information or make a statement to the Commissioner knowing that it is false or misleading in a material particular.

Penalty for a contravention of this subsection: Imprisonment for 12 months or 20 penalty units, or both.
66 Failure to give information etc.

(1) A person shall not refuse or fail:
   (a) to give information; or
   (b) to answer a question or produce a document or record;
when so required under this Act.

   Penalty:
   (a) in the case of an individual—imprisonment for 12 months or
       20 penalty units, or both; or
   (b) in the case of a body corporate—100 penalty units.

(1A) For the purposes of subsection (1B), a journalist has a reasonable
excuse if giving the information, answering the question or
producing the document or record would tend to reveal the identity
of a person who gave information or a document or record to the
journalist in confidence.

(1B) Subsection (1) does not apply if the person has a reasonable
excuse.

Note: A defendant bears an evidential burden in relation to the matter in
subsection (1B) (see subsection 13.3(3) of the Criminal Code).

(2) For the purposes of subsections (3) to (11) (inclusive):

document includes a record.

information includes an answer to a question.

(3) Subject to subsections (4), (7) and (10), it is a reasonable excuse
for the purposes of subsection (1B) for an individual:
   (a) to refuse or fail to give information when so required under
       this Act; or
   (b) to refuse or fail to produce a document when so required
       under this Act;
that giving the information, or producing the document, as the case
may be, might tend to incriminate the individual or make the
individual liable to forfeiture or a penalty.
(4) Subsection (3) does not apply in relation to a failure or refusal by an individual to give information, or to produce a document, on the ground that giving the information or producing the document might tend to prove his or her guilt of an offence against, or make him or her liable to forfeiture or a penalty under, a law of the Commonwealth or of a Territory, if the Director of Public Prosecutions has given the individual a written undertaking under subsection (5).

(5) An undertaking by the Director of Public Prosecutions shall:
   (a) be an undertaking that:
      (i) information given, or a document produced, by the individual; or
      (ii) any information or document obtained as a direct or indirect consequence of the giving of the information, or the production of the document;
      will not be used in evidence in any proceedings for an offence against a law of the Commonwealth or of a Territory, or in any disciplinary proceedings, against the individual, other than proceedings in respect of the falsity of evidence given by the individual;
   (b) state that, in the opinion of the Director of Public Prosecutions, there are special reasons why, in the public interest, the information or document should be available to the Commissioner; and
   (c) state the general nature of those reasons.

(6) The Commissioner may recommend to the Director of Public Prosecutions that an individual who has been, or is to be, required under this Act to give information or produce a document be given an undertaking under subsection (5).

(7) Subsection (3) does not apply in relation to a failure or refusal by an individual to give information, or to produce a document, on the ground that giving the information or producing the document might tend to prove his or her guilt of an offence against, or make him or her liable to forfeiture or a penalty under, a law of a State, if the Attorney-General of the State, or a person authorised by that
Attorney-General (being the person holding the office of Director of Public Prosecutions, or a similar office, of the State) has given the individual a written undertaking under subsection (8).

(8) An undertaking by the Attorney-General of the State, or authorised person, shall:
(a) be an undertaking that:
   (i) information given, or a document produced, by the individual; or
   (ii) any information or document obtained as a direct or indirect consequence of the giving of the information, or the production of the document;
will not be used in evidence in any proceedings for an offence against a law of the State, or in any disciplinary proceedings, against the individual, other than proceedings in respect of the falsity of evidence given by the individual;
(b) state that, in the opinion of the person giving the undertaking, there are special reasons why, in the public interest, the information or document should be available to the Commissioner; and
(c) state the general nature of those reasons.

(9) The Commissioner may recommend to the Attorney-General of a State that an individual who has been, or is to be, required under this Act to give information or produce a document be given an undertaking under subsection (8).

(10) For the purposes of subsection (1B):
(a) it is not a reasonable excuse for a body corporate to refuse or fail to produce a document that production of the document might tend to incriminate the body corporate or make it liable to forfeiture or a penalty; and
(b) it is not a reasonable excuse for an individual to refuse or fail to produce a document that is, or forms part of, a record of an existing or past business (not being, if the individual is or has been an employee, a document that sets out details of earnings received by the individual in respect of his or her employment and does not set out any other information) that
production of the document might tend to incriminate the individual or make the individual liable to forfeiture or a penalty.

(11) Subsections (4), (7) and (10) do not apply where proceedings, in respect of which giving information or producing a document might tend to incriminate an individual or make an individual liable to forfeiture or a penalty, have been commenced against the individual and have not been finally dealt with by a court or otherwise disposed of.

67 Protection from civil actions

Civil proceedings do not lie against a person in respect of loss, damage or injury of any kind suffered by another person because of any of the following acts done in good faith:

(a) the making of a complaint under this Act;
(b) the making of a statement to, or the giving of a document or information to, the Commissioner, whether or not pursuant to a requirement under section 44.

68 Power to enter premises

(1) Subject to subsection (3), for the purposes of the performance by the Commissioner of his or her functions under this Act, a person authorised by the Commissioner in writing for the purposes of this section may, at any reasonable time of the day, enter premises occupied by an agency, an organisation, a file number recipient, a credit reporting body or a credit provider and inspect any documents that are kept at those premises and that are relevant to the performance of those functions, other than documents in respect of which the Attorney-General has furnished a certificate under subsection 70(1) or (2).

(1A) The Commissioner may authorise a person only while the person is a member of the staff assisting the Commissioner.

(2) The occupier or person in charge of the premises shall provide the authorised person with all reasonable facilities and assistance for
the effective exercise of the authorised person’s powers under subsection (1).

(3) A person shall not enter under subsection (1) premises other than premises that are occupied by an agency unless:
   (a) the occupier of the premises has consented to the person entering the premises; or
   (b) the person is authorised, pursuant to a warrant issued under subsection (4), to enter the premises.

(3A) Before obtaining the consent, the authorised person must inform the occupier or person in charge that he or she may refuse to consent.

(3B) An entry by an authorised person with the consent of the occupier or person in charge is not lawful if the consent was not voluntary.

(3C) The authorised person may not enter premises (other than premises occupied by an agency) if:
   (a) the occupant or person in charge asks the authorised person to produce his or her identity card; and
   (b) the authorised person does not produce it.

(3D) If an authorised person is on premises with the consent of the occupier or person in charge, the authorised person must leave the premises if the occupier or person in charge asks the authorised person to do so.

(4) If, on an application made by a person authorised by the Commissioner under subsection (1), a Magistrate is satisfied, by information on oath, that it is reasonably necessary, for the purposes of the performance by the Commissioner of his or her functions under this Act, that the person be empowered to enter the premises, the Magistrate may issue a warrant authorising the person, with such assistance as the person thinks necessary, to enter the premises, if necessary by force, for the purpose of exercising those powers.
(5) A warrant issued under subsection (4) shall state:
   (a) whether entry is authorised to be made at any time of the day
       or during specified hours of the day; and
   (b) a day, not being later than one month after the day on which
       the warrant was issued, at the end of which the warrant
       ceases to have effect.

(6) Nothing in subsection (1) restricts the operation of any other
    provision of this Part.

68A  Identity cards

(1) The Commissioner must issue to a person authorised for the
    purposes of section 68 an identity card in the form approved by the
    Commissioner. The identity card must contain a recent photograph
    of the authorised person.

(2) As soon as practicable after the person ceases to be authorised, he
    or she must return the identity card to the Commissioner.

(3) A person must not contravene subsection (2).
    Penalty: 1 penalty unit.

70  Certain documents and information not required to be disclosed

(1) Where the Attorney-General furnishes to the Commissioner a
    certificate certifying that the giving to the Commissioner of
    information concerning a specified matter (including the giving of
    information in answer to a question), or the production to the
    Commissioner of a specified document or other record, would be
    contrary to the public interest because it would:
    (a) prejudice the security, defence or international relations of
        Australia;
    (b) involve the disclosure of communications between a Minister
        of the Commonwealth and a Minister of a State, being a
        disclosure that would prejudice relations between the
        Commonwealth Government and the Government of a State;
Part V Investigations etc.
Division 5 Miscellaneous

Section 70

(c) involve the disclosure of deliberations or decisions of the Cabinet or of a Committee of the Cabinet;
(d) involve the disclosure of deliberations or advice of the Executive Council;
(e) prejudice the conduct of an investigation or inquiry into crime or criminal activity that is currently being pursued, or prejudice the fair trial of any person;
(f) disclose, or enable a person to ascertain, the existence or identity of a confidential source of information in relation to the enforcement of the criminal law;
(g) prejudice the effectiveness of the operational methods or investigative practices or techniques of agencies responsible for the enforcement of the criminal law; or
(h) endanger the life or physical safety of any person;
the Commissioner is not entitled to require a person to give any information concerning the matter or to produce the document or other record.

(2) Without limiting the operation of subsection (1), where the Attorney-General furnishes to the Commissioner a certificate certifying that the giving to the Commissioner of information as to the existence or non-existence of information concerning a specified matter (including the giving of information in answer to a question) or as to the existence or non-existence of any document or other record required to be produced to the Commissioner would be contrary to the public interest:

(a) by reason that it would prejudice the security, defence or international relations of Australia; or
(b) by reason that it would prejudice the proper performance of the functions of the ACC; or
(c) by reason that it would prejudice the proper performance of the functions of the Integrity Commissioner;
the Commissioner is not entitled, pursuant to this Act, to require a person to give any information as to the existence or non-existence of information concerning that matter or as to the existence of that document or other record.
70B Application of this Part to former organisations

If an individual, body corporate, partnership, unincorporated association or trust ceases to be an organisation but continues to exist, this Part operates in relation to:

(a) an act or practice of the organisation (while it was an organisation); and

(b) the individual, body corporate, partnership, unincorporated association or trust;

as if he, she or it were still (and had been at all relevant times) an organisation.

Example 1: If an individual carrying on a business was not a small business operator, but later became one and remained alive:

(a) a complaint may be made under this Part about an act or practice of the individual in carrying on the business before he or she became a small business operator; and

(b) the complaint may be investigated (and further proceedings taken) under this Part as though the individual were still an organisation.

Example 2: A small business operator chooses under section 6EA to be treated as an organisation, but later revokes the choice. A complaint about an act or practice the operator engaged in while the choice was registered under that section may be made and investigated under this Part as if the operator were an organisation.
Part VI—Public interest determinations and temporary public interest determinations

Division 1—Public interest determinations

71 Interpretation

For the purposes of this Part, a person is interested in an application made under section 73 if, and only if, the Commissioner is of the opinion that the person has a real and substantial interest in the application.

72 Power to make, and effect of, determinations

Determinations about an APP entity’s acts and practices

(2) Subject to this Division, if the Commissioner is satisfied that:
(a) an act or practice of an APP entity breaches, or may breach:
   (i) an Australian Privacy Principle; or
   (ii) a registered APP code that binds the entity; but
(b) the public interest in the entity doing the act, or engaging in the practice, substantially outweighs the public interest in adhering to that code or principle;

the Commissioner may, by legislative instrument, make a determination to that effect.

Effect of determination under subsection (2)

(3) The APP entity is taken not to contravene section 15 or 26A if the entity does the act, or engages in the practice, while the determination is in force under subsection (2).

Giving a determination under subsection (2) general effect

(4) The Commissioner may, by legislative instrument, make a determination that no APP entity is taken to contravene section 15...
or 26A if, while that determination is in force, an APP entity does an act, or engages in a practice, that is the subject of a determination under subsection (2) in relation to that entity or any other APP entity.

**Effect of determination under subsection (4)**

(5) A determination under subsection (4) has effect according to its terms.

### 73 Application by APP entity

(1) An APP entity may apply in accordance with the regulations for a determination under section 72 about an act or practice of the entity.

(1A) If:

(a) an application is made under subsection (1); and

(b) the Commissioner is satisfied that the application is frivolous, vexatious, misconceived, lacking in substance or not made in good faith;

the Commissioner may, in writing, dismiss the application.

(2) The CEO of the National Health and Medical Research Council may make an application under subsection (1) on behalf of other agencies concerned with medical research or the provision of health services.

(3) Where an application is made by virtue of subsection (2), a reference in the succeeding provisions of this Part to the agency is a reference to the CEO of the National Health and Medical Research Council.

(4) Where the Commissioner makes a determination under section 72 on an application made by virtue of subsection (2), that section has effect, in relation to each of the agencies on whose behalf the application was made as if the determination had been made on an application by that agency.
Part VI  Public interest determinations and temporary public interest determinations
Division 1  Public interest determinations

Section 74

74 Publication of application etc.

(1) Subject to subsection (2), the Commissioner shall publish, in such manner as he or she thinks fit, notice of:
   (a) the receipt by the Commissioner of an application; and
   (b) if the Commissioner dismisses an application under subsection 73(1A)—the dismissal of the application.

(2) The Commissioner shall not, except with the consent of the agency, permit the disclosure to another body or person of information contained in a document provided by an agency as part of, or in support of, an application if the agency has informed the Commissioner in writing that the agency claims that the document is an exempt document within the meaning of Part IV of the Freedom of Information Act 1982.

75 Draft determination

(1) The Commissioner shall prepare a draft of his or her proposed determination in relation to the application unless the Commissioner dismisses the application under subsection 73(1A).

(2) If the applicant is an agency, the Commissioner must send to the agency, and to each other person (if any) who is interested in the application, a written invitation to notify the Commissioner, within the period specified in the invitation, whether or not the agency or other person wishes the Commissioner to hold a conference about the draft determination.

(2A) If the applicant is an organisation, the Commissioner must:
   (a) send a written invitation to the organisation to notify the Commissioner, within the period specified in the invitation, whether or not the organisation wishes the Commissioner to hold a conference about the draft determination; and
   (b) issue, in any way the Commissioner thinks appropriate, an invitation in corresponding terms to the other persons (if any) that the Commissioner thinks appropriate.
(3) An invitation under subsection (2) or subsection (2A) shall specify a period that begins on the day on which the invitation is sent and is not shorter than the prescribed period.

76 Conference

(1) If an agency, organisation or person notifies the Commissioner, within the period specified in an invitation sent to the agency, organisation or person, that the agency, organisation or person wishes a conference to be held about the draft determination, the Commissioner shall hold such a conference.

(2) The Commissioner shall fix a day, time and place for the holding of the conference.

(3) The day fixed shall not be more than 30 days after the latest day on which a period specified in any of the invitations sent in relation to the draft determination expires.

(4) The Commissioner shall give notice of the day, time and place of the conference to the agency or organisation and to each person to whom an invitation was sent.

77 Conduct of conference

(1) At the conference, the agency or organisation is entitled to be represented by a person who is, or persons each of whom is, an officer or employee of the agency or organisation.

(2) At the conference, a person to whom an invitation was sent, or any other person who is interested in the application and whose presence at the conference is considered by the Commissioner to be appropriate, is entitled to attend and participate personally or, in the case of a body corporate, to be represented by a person who is, or persons each of whom is, a director, officer or employee of the body corporate.

(3) The Commissioner may exclude from the conference a person who:
Part VI  Public interest determinations and temporary public interest determinations
Division 1  Public interest determinations

Section 78

(a) is entitled neither to participate in the conference nor to represent a person who is entitled to be represented at the conference;
(b) uses insulting language at the conference;
(c) creates, or takes part in creating or continuing, a disturbance at the conference; or
(d) repeatedly disturbs the conference.

78 Determination of application

The Commissioner shall, after complying with this Part in relation to the application, make:
(a) such determination under section 72 as he or she considers appropriate; or
(b) a written determination dismissing the application.

79 Making of determination

(1) The Commissioner shall, in making a determination, take account of all matters raised at the conference.

(2) The Commissioner shall, in making a determination, take account of all submissions about the application that have been made, whether at a conference or not, by the agency, organisation or any other person.
Section 80A

Division 2—Temporary public interest determinations

80A Temporary public interest determinations

(1) This section applies if the Commissioner is satisfied that:
   (a) the act or practice of an APP entity that is the subject of an application under section 73 for a determination under section 72 breaches, or may breach:
      (i) an Australian Privacy Principle; or
      (ii) a registered APP code that binds the entity; and
   (b) the public interest in the entity doing the act, or engaging in the practice, outweighs to a substantial degree the public interest in adhering to that principle or code; and
   (c) the application raises issues that require an urgent decision.

(2) The Commissioner may, by legislative instrument, make a determination that he or she is satisfied of the matters set out in subsection (1). The Commissioner may do so:
   (a) on request by the APP entity; or
   (b) on the Commissioner’s own initiative.

(3) The Commissioner must specify in the determination a period of up to 12 months during which the determination is in force (subject to subsection 80D(2)).

80B Effect of temporary public interest determination

APP entity covered by a determination

(1) If an act or practice of an APP entity is the subject of a temporary public interest determination, the entity is taken not to breach section 15 or 26A if the entity does the act, or engages in the practice, while the determination is in force.
Section 80D

Giving a temporary public interest determination general effect

(3) The Commissioner may, by legislative instrument, make a
determination that no APP entity is taken to contravene section 15
or 26A if, while that determination is in force, an APP entity does
an act, or engages in a practice, that is the subject of a temporary
public interest determination in relation to that entity or another
APP entity.

Effect of determination under subsection (3)

(4) A determination under subsection (3) has effect according to its
terms.

80D Commissioner may continue to consider application

(1) The fact that the Commissioner has made a determination under
this Division about an act or practice does not prevent the
Commissioner from dealing under Division 1 with an application
made under section 73 in relation to that act or practice.

(2) A determination under this Division about an act or practice ceases
to be in effect when:
(a) a determination made under subsection 72(2) about the act or
practice comes into effect; or
(b) a determination is made under paragraph 78(b) to dismiss the
application.
Division 3—Register of determinations

80E Register of determinations

(1) The Commissioner must keep a register of determinations made under Division 1 or 2.

(2) The Commissioner may decide the form of the register and how it is to be kept.

(3) The Commissioner must make the register available to the public in the way that the Commissioner determines.

(4) The Commissioner may charge fees for:
   (a) making the register available to the public; or
   (b) providing copies of, or extracts from, the register.
Part VIA—Dealing with personal information in emergencies and disasters

Division 1—Object and interpretation

80F Object

The object of this Part is to make special provision for the collection, use and disclosure of personal information in emergencies and disasters.

80G Interpretation

(1) In this Part:

- **duty of confidence** means any duty or obligation arising under the common law or at equity pursuant to which a person is obliged not to disclose information, but does not include legal professional privilege.

- **emergency declaration** means a declaration under section 80J or 80K.

- **permanent resident** means a person, other than an Australian citizen:
  (a) whose normal place of residence is situated in Australia; and
  (b) whose presence in Australia is not subject to any limitation as to time imposed by law; and
  (c) who is not an illegal entrant within the meaning of the Migration Act 1958.

- **secrecy provision** means a provision of a law of the Commonwealth (including a provision of this Act), or of a Norfolk Island enactment, that prohibits or regulates the use or disclosure of personal information, whether the provision relates to the use or disclosure of personal information generally or in specified circumstances.
Dealing with personal information in emergencies and disasters  Part VIA
Object and interpretation  Division 1

Section 80H

(2) For the purposes of this Part, a reference in the definition of personal information in subsection 6(1) to an individual is taken to include a reference to an individual who is not living.

80H  Meaning of permitted purpose

(1) For the purposes of this Part, a permitted purpose is a purpose that directly relates to the Commonwealth’s response to an emergency or disaster in respect of which an emergency declaration is in force.

(2) Without limiting subsection (1), any of the following is a permitted purpose in relation to an emergency or disaster:

(a) identifying individuals who:
   (i) are or may be injured, missing or dead as a result of the emergency or disaster; or
   (ii) are or may be otherwise involved in the emergency or disaster;

(b) assisting individuals involved in the emergency or disaster to obtain services such as repatriation services, medical or other treatment, health services and financial or other humanitarian assistance;

(c) assisting with law enforcement in relation to the emergency or disaster;

(d) coordination or management of the emergency or disaster;

(e) ensuring that responsible persons for individuals who are, or may be, involved in the emergency or disaster are appropriately informed of matters that are relevant to:
   (i) the involvement of those individuals in the emergency or disaster; or
   (ii) the response to the emergency or disaster in relation to those individuals.
Part VIA  Dealing with personal information in emergencies and disasters

Division 2  Declaration of emergency

Section 80J

Division 2—Declaration of emergency

80J Declaration of emergency—events of national significance

The Prime Minister or the Minister may make a declaration under this section if the Prime Minister or the Minister (as the case may be) is satisfied that:

(a) an emergency or disaster has occurred; and
(b) the emergency or disaster is of such a kind that it is appropriate in the circumstances for this Part to apply in relation to the emergency or disaster; and
(c) the emergency or disaster is of national significance (whether because of the nature and extent of the emergency or disaster, the direct or indirect effect of the emergency or disaster, or for any other reason); and
(d) the emergency or disaster has affected one or more Australian citizens or permanent residents (whether within Australia or overseas).

Note: A declaration under this section is merely a trigger for the operation of this Part and is not directly related to any other legislative or non-legislative scheme about emergencies.

80K Declaration of emergency—events outside Australia

(1) The Prime Minister or the Minister may make a declaration under this section if the Prime Minister or the Minister (as the case may be) is satisfied that:

(a) an emergency or disaster has occurred outside Australia; and
(b) the emergency or disaster is of such a kind that it is appropriate in the circumstances for this Part to apply in relation to the emergency or disaster; and
(c) the emergency or disaster has affected one or more Australian citizens or permanent residents (whether within Australia or overseas).
Dealing with personal information in emergencies and disasters  Part VIA  Declaration of emergency  Division 2

Section 80L

(2) The Minister must consult the Minister administering the Diplomatic Privileges and Immunities Act 1967 before the Minister makes a declaration under this section.

Note: A declaration under this section is merely a trigger for the operation of this Part and is not directly related to any other legislative or non-legislative scheme about emergencies.

80L Form of declarations

(1) An emergency declaration must be in writing and signed by:
   (a) if the Prime Minister makes the declaration—the Prime Minister; or
   (b) if the Minister makes the declaration—the Minister.

(2) An emergency declaration must be published, as soon as practicable after the declaration has effect:
   (a) on the website maintained by the Department; and
   (b) by notice published in the Gazette.

(3) An emergency declaration is not a legislative instrument.

80M When declarations take effect

An emergency declaration has effect from the time at which the declaration is signed.

80N When declarations cease to have effect

An emergency declaration ceases to have effect at the earliest of:
   (a) if a time at which the declaration will cease to have effect is specified in the declaration—at that time; or
   (b) the time at which the declaration is revoked; or
   (c) the end of 12 months starting when the declaration is made.
Section 80P

Division 3—Provisions dealing with the use and disclosure of personal information

80P Authorisation of collection, use and disclosure of personal information

(1) At any time when an emergency declaration is in force in relation to an emergency or disaster, an entity may collect, use or disclose personal information relating to an individual if:
   (a) the entity reasonably believes that the individual may be involved in the emergency or disaster; and
   (b) the collection, use or disclosure is for a permitted purpose in relation to the emergency or disaster; and
   (c) in the case of a disclosure of the personal information by an agency—the disclosure is to:
      (i) an agency; or
      (ii) a State or Territory authority; or
      (iii) an organisation; or
      (iv) an entity not covered by subparagraph (i), (ii) or (iii) that is, or is likely to be, involved in managing, or assisting in the management of, the emergency or disaster; or
      (v) a responsible person for the individual; and
   (d) in the case of a disclosure of the personal information by an organisation or another person—the disclosure is to:
      (i) an agency; or
      (ii) an entity that is directly involved in providing repatriation services, medical or other treatment, health services or financial or other humanitarian assistance services to individuals involved in the emergency or disaster; or
      (iii) a person or entity prescribed by the regulations for the purposes of this paragraph; or
Dealing with personal information in emergencies and disasters

Part VIA
Provisions dealing with the use and disclosure of personal information
Division 3

Section 80P

(iv) a person or entity specified by the Minister, by legislative instrument, for the purposes of this paragraph; and

(e) in the case of any disclosure of the personal information—the disclosure is not to a media organisation.

(2) An entity is not liable to any proceedings for contravening a secrecy provision in respect of a use or disclosure of personal information authorised by subsection (1), unless the secrecy provision is a designated secrecy provision (see subsection (7)).

(3) An entity is not liable to any proceedings for contravening a duty of confidence in respect of a disclosure of personal information authorised by subsection (1).

(4) An entity does not breach an Australian Privacy Principle, or a registered APP code that binds the entity, in respect of a collection, use or disclosure of personal information authorised by subsection (1).

(6) A collection, use or disclose of personal information by an officer or employee of an agency in the course of duty as an officer or employee is authorised by subsection (1) only if the officer or employee is authorised by the agency to collect, use or disclose the personal information.

(7) In this section:

**designated secrecy provision** means any of the following:

(a) sections 18, 18A, 18B and 92 of the *Australian Security Intelligence Organisation Act 1979*;

(b) section 34 of the *Inspector-General of Intelligence and Security Act 1986*;

(c) sections 39, 39A, 40, 40A to 40M and 41 of the *Intelligence Services Act 2001*;

(d) a provision of a law of the Commonwealth prescribed by the regulations for the purposes of this paragraph;
Section 80P

(e) a provision of a law of the Commonwealth of a kind prescribed by the regulations for the purposes of this paragraph.

_entity_ includes the following:

(a) a person;
(b) an agency;
(c) an organisation.
Dealing with personal information in emergencies and disasters  Part VIA
Other matters  Division 4

Section 80Q

Division 4—Other matters

80Q Disclosure of information—offence

(1) A person (the first person) commits an offence if:
   (a) personal information that relates to an individual is disclosed to the first person because of the operation of this Part; and
   (b) the first person subsequently discloses the personal information; and
   (c) the first person is not a responsible person for the individual.

Penalty: 60 penalty units or imprisonment for 1 year, or both.

(2) Subsection (1) does not apply to the following disclosures:
   (a) if the first person is an APP entity—a disclosure permitted under an Australian Privacy Principle or a registered APP code that binds the person;
   (b) a disclosure permitted under section 80P;
   (c) a disclosure made with the consent of the individual to whom the personal information relates;
   (d) a disclosure to the individual to whom the personal information relates;
   (e) a disclosure prescribed by the regulations.

Note: A defendant bears an evidential burden in relation to a matter in subsection (2) (see subsection 13.3(3) of the Criminal Code).

(3) If a disclosure of personal information is covered by subsection (2), the disclosure is authorised by this section.

(4) For the purposes of paragraph (2)(f), court includes any tribunal, authority or person having power to require the production of documents or the answering of questions.
**Part VIA**  Dealing with personal information in emergencies and disasters

**Division 4**  Other matters

Section 80R

**80R Operation of Part**

(1) The operation of this Part is not limited by a secrecy provision of any other law of the Commonwealth (whether made before or after the commencement of this Act) except to the extent that the secrecy provision expressly excludes the operation of this section.

Note: Section 3 provides for the concurrent operation of State and Territory laws.

(1A) The operation of this Part is not limited by a secrecy provision of a Norfolk Island enactment (whether made before or after the commencement of this subsection) except to the extent that the secrecy provision expressly excludes the operation of this subsection.

(2) Nothing in this Part is to be taken to require an entity to collect, use or disclose personal information.

**80S Severability—additional effect of Part**

(1) Without limiting its effect apart from each of the following subsections of this section, this Part has effect in relation to a collection, use or disclosure as provided by that subsection.

(2) This Part has the effect it would have if its operation in relation to a collection, use or disclosure were expressly confined to a collection, use or disclosure by a corporation.

(3) This Part also has the effect it would have if its operation in relation to a collection, use or disclosure were expressly confined to a collection, use or disclosure taking place in the course of, or in relation to, trade or commerce:

(a) between Australia and places outside Australia; or

(b) among the States; or

(c) within a Territory, between a State and a Territory or between 2 Territories.

(4) This Part also has the effect it would have if its operation in relation to a collection, use or disclosure were expressly confined...
to a collection, use or disclosure using a postal, telegraphic, telephonic or other like service within the meaning of paragraph 51(v) of the Constitution.

(5) This Part also has the effect it would have if its operation in relation to a collection, use or disclosure were expressly confined to a collection, use or disclosure taking place in a Territory.

(6) This Part also has the effect it would have if its operation in relation to a collection, use or disclosure were expressly confined to a collection, use or disclosure taking place in a place acquired by the Commonwealth for public purposes.

(7) This Part also has the effect it would have if its operation in relation to a collection, use or disclosure were expressly confined to a collection, use or disclosure by an agency.

(8) This Part also has the effect it would have if its operation in relation to a collection, use or disclosure were expressly confined to a collection, use or disclosure for purposes relating to the defence of the Commonwealth.

(9) This Part also has the effect that it would have if its operation in relation to a collection, use or disclosure were expressly confined to a collection, use or disclosure taking place outside Australia.

(10) This Part also has the effect that it would have if its operation in relation to a collection, use or disclosure were expressly confined to a collection, use or disclosure:
   (a) in relation to which the Commonwealth is under an obligation under an international agreement; or
   (b) that is of international concern.

(11) This Part also has the effect that it would have if its operation in relation to a collection, use or disclosure were expressly confined to a collection, use or disclosure in relation to an emergency of national significance.
Part VIA Dealing with personal information in emergencies and disasters
Division 4 Other matters

Section 80T

80T Compensation for acquisition of property—constitutional safety net

(1) If the operation of this Part would result in an acquisition of property from a person otherwise than on just terms, the Commonwealth is liable to pay a reasonable amount of compensation to the person.

(2) If the Commonwealth and the person do not agree on the amount of the compensation, the person may institute proceedings in a court of competent jurisdiction for the recovery from the Commonwealth of such reasonable amount of compensation as the court determines.

(3) In this section:

acquisition of property has the same meaning as in paragraph 51(xxxi) of the Constitution.

just terms has the same meaning as in paragraph 51(xxxi) of the Constitution.
Civil penalty orders  Part VIB
Civil penalty provisions  Division 1

Section 80U

Part VIB—Civil penalty orders

Division 1—Civil penalty provisions

80U  Civil penalty provisions

A subsection of this Act (or a section of this Act that is not divided into subsections) is a civil penalty provision if the words “civil penalty” and one or more amounts in penalty units are set out at the foot of the subsection (or section).

80V  Ancillary contravention of civil penalty provisions

(1) An entity must not:
   (a) attempt to contravene a civil penalty provision; or
   (b) aid, abet, counsel or procure a contravention of a civil penalty provision; or
   (c) induce (by threats, promises or otherwise) a contravention of a civil penalty provision; or
   (d) be in any way, directly or indirectly, knowingly concerned in, or party to, a contravention of a civil penalty provision; or
   (e) conspire with others to effect a contravention of a civil penalty provision.

(2) An entity that contravenes subsection (1) in relation to a civil penalty provision is taken to have contravened the provision.
Part VIB  Civil penalty orders
Division 2  Obtaining a civil penalty order

Section 80W

Division 2—Obtaining a civil penalty order

80W  Civil penalty orders

Application for order

(1) The Commissioner may apply to the Federal Court or Federal Circuit Court for an order that an entity, that is alleged to have contravened a civil penalty provision, pay the Commonwealth a pecuniary penalty.

(2) The Commissioner must make the application within 6 years of the alleged contravention.

Court may order entity to pay pecuniary penalty

(3) If the court is satisfied that the entity has contravened the civil penalty provision, the court may order the entity to pay to the Commonwealth such pecuniary penalty for the contravention as the court determines to be appropriate.

Note: Subsection (5) sets out the maximum penalty that the court may order the entity to pay.

(4) An order under subsection (3) is a civil penalty order.

Determining pecuniary penalty

(5) The pecuniary penalty must not be more than:

(a) if the entity is a body corporate—5 times the amount of the pecuniary penalty specified for the civil penalty provision; or

(b) otherwise—the amount of the pecuniary penalty specified for the civil penalty provision.

(6) In determining the pecuniary penalty, the court must take into account all relevant matters, including:

(a) the nature and extent of the contravention; and

(b) the nature and extent of any loss or damage suffered because of the contravention; and
(c) the circumstances in which the contravention took place; and  
(d) whether the entity has previously been found by a court in  
proceedings under this Act to have engaged in any similar  
conduct.

80X Civil enforcement of penalty

(1) A pecuniary penalty is a debt payable to the Commonwealth.

(2) The Commonwealth may enforce a civil penalty order as if it were  
an order made in civil proceedings against the entity to recover a  
debt due by the entity. The debt arising from the order is taken to  
be a judgement debt.

80Y Conduct contravening more than one civil penalty provision

(1) If conduct constitutes a contravention of 2 or more civil penalty  
provisions, proceedings may be instituted under this Division  
against an entity in relation to the contravention of any one or more  
of those provisions.

(2) However, the entity is not liable to more than one pecuniary  
penalty under this Division in relation to the same conduct.

80Z Multiple contraventions

(1) The Federal Court or Federal Circuit Court may make a single civil  
penalty order against an entity for multiple contraventions of a civil  
penalty provision if:  
(a) proceedings for the contraventions are founded on the same  
facts; or  
(b) the contraventions form, or are part of, a series of  
contraventions of the same or a similar character.

(2) However, the pecuniary penalty must not exceed the sum of the  
maximum pecuniary penalties that could be ordered if a separate  
civil penalty order were made for each of the contraventions.
Part VIB Civil penalty orders
Division 2 Obtaining a civil penalty order

Section 80ZA

Note: In determining the pecuniary penalty, the court must take into account all relevant matters including the matters mentioned in subsection 80W(6).

80ZA Proceedings may be heard together

The Federal Court or Federal Circuit Court may direct that 2 or more proceedings for civil penalty orders are to be heard together.

80ZB Civil evidence and procedure rules for civil penalty orders

The Federal Court or Federal Circuit Court must apply the rules of evidence and procedure for civil matters when hearing proceedings for a civil penalty order.

80ZC Contravening a civil penalty provision is not an offence

A contravention of a civil penalty provision is not an offence.
Division 3—Civil proceedings and criminal proceedings

80ZD Civil proceedings after criminal proceedings

The Federal Court or Federal Circuit Court must not make a civil penalty order against an entity for a contravention of a civil penalty provision if the entity has been convicted of an offence constituted by conduct that is the same, or substantially the same, as the conduct constituting the contravention.

80ZE Criminal proceedings during civil proceedings

(1) Proceedings for a civil penalty order against an entity for a contravention of a civil penalty provision are stayed if:
   (a) criminal proceedings are commenced or have already been commenced against the entity for an offence; and
   (b) the offence is constituted by conduct that is the same, or substantially the same, as the conduct alleged to constitute the contravention.

(2) The proceedings for the civil penalty order may be resumed if the entity is not convicted of the offence. Otherwise:
   (a) the proceedings are dismissed; and
   (b) costs must not be awarded in relation to the proceedings.

80ZF Criminal proceedings after civil proceedings

Criminal proceedings may be commenced against an entity for conduct that is the same, or substantially the same, as conduct that would constitute a contravention of a civil penalty provision regardless of whether a civil penalty order has been made against the entity in relation to the contravention.
80ZG Evidence given in proceedings for civil penalty order not admissible in criminal proceedings

(1) Evidence of information given, or evidence of production of documents, by an individual is not admissible in criminal proceedings against the individual if:
   (a) the individual previously gave the evidence or produced the documents in proceedings for a civil penalty order against the individual for an alleged contravention of a civil penalty provision (whether or not the order was made); and
   (b) the conduct alleged to constitute the offence is the same, or substantially the same, as the conduct alleged to constitute the contravention.

(2) However, subsection (1) does not apply to criminal proceedings in relation to the falsity of the evidence given by the individual in the proceedings for the civil penalty order.
Part VII—Privacy Advisory Committee

81 Interpretation

In this Part, unless the contrary intention appears:

Advisory Committee means the Privacy Advisory Committee established by subsection 82(1).

member means a member of the Advisory Committee.

82 Establishment and membership

(1) A Privacy Advisory Committee is established.

(2) The Advisory Committee shall consist of:

(a) the Commissioner; and

(aa) the Privacy Commissioner (within the meaning of the Australian Information Commissioner Act 2010); and

(b) not more than 8 other members.

(3) A member other than the Commissioner and Privacy Commissioner (within the meaning of that Act):

(a) shall be appointed by the Governor-General; and

(b) shall be appointed as a part-time member.

(4) An appointed member holds office, subject to this Act, for such period, not exceeding 5 years, as is specified in the instrument of the member’s appointment, but is eligible for re-appointment.

(5) The Commissioner shall be convenor of the Committee.

(6) The Governor-General shall so exercise the power of appointment conferred by subsection (3) that a majority of the appointed members are persons who are neither officers nor employees, nor members of the staff of an authority or instrumentality, of the Commonwealth.
Part VII  Privacy Advisory Committee

Section 83

(7) Of the appointed members:
   (a) at least one must be a person who has had at least 5 years’ experience at a high level in industry or commerce; and
   (aa) at least one must be a person who has had at least 5 years’ experience at a high level in public administration, or the service of a government or an authority of a government; and
   (ab) at least one must be a person who has had extensive experience in health privacy; and
   (b) at least one must be a person who has had at least 5 years’ experience in the trade union movement; and
   (c) at least one must be a person who has had extensive experience in information and communication technologies; and
   (d) at least one must be appointed to represent general community interests, including interests relating to social welfare; and
   (e) at least one must be a person who has had extensive experience in the promotion of civil liberties.

(10) An appointed member holds office on such terms and conditions (if any) in respect of matters not provided for by this Act as are determined, in writing, by the Governor-General.

(11) The performance of a function of the Advisory Committee is not affected because of a vacancy or vacancies in the membership of the Advisory Committee.

83 Functions

The functions of the Advisory Committee are:
   (a) on its own initiative, or when requested by the Commissioner, to advise the Commissioner on matters relevant to his or her functions;
   (b) to recommend material to the Commissioner for inclusion in rules or guidelines to be issued by the Commissioner pursuant to his or her functions; and
(c) subject to any direction given by the Commissioner, to engage in and promote community education, and community consultation, in relation to the protection of individual privacy.

84 Leave of absence

The convenor may, on such terms and conditions as the convenor thinks fit, grant to another member leave to be absent from a meeting of the Advisory Committee.

85 Removal and resignation of members

(1) The Governor-General may terminate the appointment of an appointed member for misbehaviour or physical or mental incapacity.

(2) The Governor-General shall terminate the appointment of an appointed member if the member:

(a) becomes bankrupt, applies to take the benefit of any law for the relief of bankrupt or insolvent debtors, compounds with the member’s creditors or makes an assignment of the member’s remuneration for their benefit;

(b) fails, without reasonable excuse, to comply with the member’s obligations under section 86; or

(c) is absent, without the leave of the convenor, from 3 consecutive meetings of the Advisory Committee.

(3) An appointed member may resign from office by delivering a signed notice of resignation to the Governor-General.

86 Disclosure of interests of members

(1) A member who has a direct or indirect pecuniary interest in a matter being considered or about to be considered by the Advisory Committee, being an interest that could conflict with the proper performance of that member’s functions in relation to the consideration of the matter, shall, as soon as practicable after the
Part VII  Privacy Advisory Committee

Section 87

relevant facts have come to the knowledge of that member, disclose the nature of that interest at a meeting of the Advisory Committee.

(2) A disclosure under subsection (1) at a meeting of the Advisory Committee shall be recorded in the minutes of the meeting.

87 Meetings of Advisory Committee

(1) The convenor may convene such meetings of the Advisory Committee as the convenor considers necessary for the performance of the Committee’s functions.

(2) Meetings of the Advisory Committee shall be held at such places and at such times as the convenor determines.

(3) The convenor shall preside at all meetings of the Advisory Committee at which the convenor is present.

(4) If, at a meeting of the Advisory Committee, the convenor is not present, the members who are present shall elect one of their number to preside at the meeting.

(5) At a meeting of the Advisory Committee:
   (a) 3 members constitute a quorum;
   (b) all questions shall be decided by a majority of votes of the members present and voting; and
   (c) the person presiding has a deliberative vote and, in the event of an equality of votes, also has a casting vote.

(6) The Advisory Committee shall keep a record of its proceedings.

88 Travel allowance

An appointed member is entitled to be paid travelling allowance in accordance with the regulations.
Part VIII—Obligations of confidence

89 Obligations of confidence to which Part applies

Unless the contrary intention appears, a reference in this Part to an obligation of confidence is a reference to an obligation of confidence:

(a) to which an agency or a Commonwealth officer is subject, however the obligation arose; or

(b) that arises under or by virtue of the law in force in the Australian Capital Territory; or

(c) that arises under or by virtue of a Norfolk Island enactment that is in force.

90 Application of Part

(1) This Part applies where a person (in this Part called a confidant) is subject to an obligation of confidence to another person (in this Part called a confider) in respect of personal information, whether the information relates to the confider or to a third person, being an obligation in respect of a breach of which relief may be obtained (whether in the exercise of a discretion or not) in legal proceedings.

(2) This Part does not apply where a criminal penalty only may be imposed in respect of the breach.

91 Effect of Part on other laws

This Part does not, except to the extent that it does so expressely or by necessary implication, limit or restrict the operation of any other law or of any principle or rule of the common law or of equity, being a law, principle or rule:

(a) under or by virtue of which an obligation of confidence exists; or
Part VIII  Obligations of confidence

Section 92

(b) that has the effect of restricting or prohibiting, or imposing a liability (including a criminal liability) on a person in respect of, a disclosure or use of information.

92 Extension of certain obligations of confidence

Where a person has acquired personal information about another person and the first-mentioned person knows or ought reasonably to know that the person from whom he or she acquired the information was subject to an obligation of confidence with respect to the information, the first-mentioned person, whether he or she is in the Australian Capital Territory or not, is subject to a like obligation.

93 Relief for breach etc. of certain obligations of confidence

(1) A confider may recover damages from a confidant in respect of a breach of an obligation of confidence with respect to personal information.

(2) Subsection (1) does not limit or restrict any other right that the confider has to relief in respect of the breach.

(3) Where an obligation of confidence exists with respect to personal information about a person other than the confider, whether the obligation arose under a contract or otherwise, the person to whom the information relates has the same rights against the confidant in respect of a breach or threatened breach of the obligation as the confider has.

94 Jurisdiction of courts

(1) The jurisdiction of the courts of the Australian Capital Territory extends to matters arising under this Part.

(2) Subsection (1) does not deprive a court of a State or of another Territory of any jurisdiction that it has.
Part IX—Miscellaneous

95 Medical research guidelines

(1) The CEO of the National Health and Medical Research Council may, with the approval of the Commissioner, issue guidelines for the protection of privacy by agencies in the conduct of medical research.

(2) The Commissioner shall not approve the issue of guidelines unless he or she is satisfied that the public interest in the promotion of research of the kind to which the guidelines relate outweighs to a substantial degree the public interest in maintaining adherence to the Australian Privacy Principles.

(3) Guidelines shall be issued by being published in the Gazette.

(4) Where:
   (a) but for this subsection, an act done by an agency would breach an Australian Privacy Principle; and
   (b) the act is done in the course of medical research and in accordance with guidelines under subsection (1);
the act shall be regarded as not breaching that Australian Privacy Principle.

95A Guidelines for Australian Privacy Principles about health information

Overview

(1) This section allows the Commissioner to approve for the purposes of the Australian Privacy Principles guidelines that are issued by the CEO of the National Health and Medical Research Council or a prescribed authority.
Part IX Miscellaneous

Section 95A

Approving guidelines for use and disclosure

(2) For the purposes of paragraph 16B(3)(c), the Commissioner may, by notice in the Gazette, approve guidelines that relate to the use and disclosure of health information for the purposes of research, or the compilation or analysis of statistics, relevant to public health or public safety.

Public interest test

(3) The Commissioner may give an approval under subsection (2) only if satisfied that the public interest in the use and disclosure of health information for the purposes mentioned in that subsection in accordance with the guidelines substantially outweighs the public interest in maintaining the level of privacy protection afforded by the Australian Privacy Principles (disregarding subsection 16B(3)).

Approving guidelines for collection

(4) For the purposes of subparagraph 16B(2)(d)(iii), the Commissioner may, by notice in the Gazette, approve guidelines that relate to the collection of health information for the purposes of:

(a) research, or the compilation or analysis of statistics, relevant to public health or public safety; or

(b) the management, funding or monitoring of a health service.

Public interest test

(5) The Commissioner may give an approval under subsection (4) only if satisfied that the public interest in the collection of health information for the purposes mentioned in that subsection in accordance with the guidelines substantially outweighs the public interest in maintaining the level of privacy protection afforded by the Australian Privacy Principles (disregarding subsection 16B(2)).

Revocation of approval

(6) The Commissioner may, by notice in the Gazette, revoke an approval of guidelines under this section if he or she is no longer
satisfied of the matter that he or she had to be satisfied of to approve the guidelines.

95AA Guidelines for Australian Privacy Principles about genetic information

Overview

(1) This section allows the Commissioner to approve for the purposes of the Australian Privacy Principles guidelines that are issued by the National Health and Medical Research Council.

Approving guidelines for use and disclosure

(2) For the purposes of paragraph 16B(4)(c), the Commissioner may, by legislative instrument, approve guidelines that relate to the use and disclosure of genetic information for the purposes of lessening or preventing a serious threat to the life, health or safety of an individual who is a genetic relative of the individual to whom the genetic information relates.

95B Requirements for Commonwealth contracts

(1) This section requires an agency entering into a Commonwealth contract to take contractual measures to ensure that a contracted service provider for the contract does not do an act, or engage in a practice, that would breach an Australian Privacy Principle if done or engaged in by the agency.

(2) The agency must ensure that the Commonwealth contract does not authorise a contracted service provider for the contract to do or engage in such an act or practice.

(3) The agency must also ensure that the Commonwealth contract contains provisions to ensure that such an act or practice is not authorised by a subcontract.
Part IX Miscellaneous

Section 95C

(4) For the purposes of subsection (3), a subcontract is a contract under which a contracted service provider for the Commonwealth contract is engaged to provide services to:

(a) another contracted service provider for the Commonwealth contract; or

(b) any agency;

for the purposes (whether direct or indirect) of the Commonwealth contract.

(5) This section applies whether the agency is entering into the Commonwealth contract on behalf of the Commonwealth or in the agency’s own right.

95C Disclosure of certain provisions of Commonwealth contracts

If a person asks a party to a Commonwealth contract to be informed of the content of provisions (if any) of the contract that are inconsistent with a registered APP code binding a party to the contract or with an Australian Privacy Principle, the party requested must inform the person in writing of that content (if any).

96 Review by the Administrative Appeals Tribunal

(1) An application may be made to the Administrative Appeals Tribunal for review of the following decisions of the Commissioner:

(a) a decision under subsection 26H(1) not to register an APP code developed by an APP code developer;

(b) a decision under subsection 26S(1) not to register a CR code developed by a CR code developer;

(ba) a decision under subsection 26WQ(7) to refuse an application for a declaration;

(bb) a decision to make a declaration under paragraph 26WQ(1)(d);

(bc) a decision under subsection 26WR(1) to give a direction;

(c) a decision under subsection 52(1) or (1A) to make a determination;
(d) a decision under subsection 73(1A) to dismiss an application;
(e) a decision under section 95 to refuse to approve the issue of guidelines;
(f) a decision under subsection 95A(2) or (4) or 95AA(2) to refuse to approve guidelines;
(g) a decision under subsection 95A(6) to revoke an approval of guidelines.

(2) An application under paragraph (1)(a) may only be made by the APP code developer that developed the APP code.

(2A) An application under paragraph (1)(ba) may only be made by:
(a) the entity that made the application for a declaration; or
(b) if another entity’s compliance with subsection 26WL(2) is affected by the decision to refuse the application for a declaration—that other entity.

(2B) An application under paragraph (1)(bb) may only be made by:
(a) the entity to whom notice of the declaration was given; or
(b) if another entity’s compliance with subsection 26WL(2) is affected by the declaration—that other entity.

(2C) An application under paragraph (1)(bc) may only be made by the entity to whom the direction was given.

(2D) For the purposes of subsections (2A), (2B) and (2C), entity has the same meaning as in Part IIIC.

(3) An application under paragraph (1)(b) may only be made by the CR code developer that developed the CR code.

98 Injunctions

(1) Where a person has engaged, is engaging or is proposing to engage in any conduct that constituted or would constitute a contravention of this Act, the Federal Court or the Federal Circuit Court may, on the application of the Commissioner or any other person, grant an injunction restraining the person from engaging in the conduct and,
Part IX  Miscellaneous

Section 98

if in the court’s opinion it is desirable to do so, requiring the person to do any act or thing.

(2) Where:
   (a) a person has refused or failed, or is refusing or failing, or is proposing to refuse or fail, to do an act or thing; and
   (b) the refusal or failure was, is, or would be a contravention of this Act;
the Federal Court or the Federal Circuit Court may, on the application of the Commissioner or any other person, grant an injunction requiring the first-mentioned person to do that act or thing.

(3) Where an application is made to the court for an injunction under this section, the court may, if in the court’s opinion it is desirable to do so, before considering the application, grant an interim injunction restraining a person from engaging in conduct of the kind referred to in that subsection pending the determination of the application.

(4) The court may discharge or vary an injunction granted under this section.

(5) The power of the court to grant an injunction restraining a person from engaging in conduct of a particular kind may be exercised:
   (a) if the court is satisfied that the person has engaged in conduct of that kind—whether or not it appears to the court that the person intends to engage again, or to continue to engage, in conduct of that kind; or
   (b) if it appears to the court that, in the event that an injunction is not granted, it is likely that the person will engage in conduct of that kind—whether or not the person has previously engaged in conduct of that kind and whether or not there is an imminent danger of substantial damage to any person if the first-mentioned person engages in conduct of that kind.

(6) The power of the court to grant an injunction requiring a person to do a particular act or thing may be exercised:
Section 98A

(a) if the court is satisfied that the person has refused or failed to do that act or thing—whether or not it appears to the court that the person intends to refuse or fail again, or to continue to refuse or fail, to do that act or thing; or

(b) if it appears to the court that, in the event that an injunction is not granted, it is likely that the person will refuse or fail to do that act or thing—whether or not the person has previously refused or failed to do that act or thing and whether or not there is an imminent danger of substantial damage to any person if the first-mentioned person refuses or fails to do that act or thing.

(7) Where the Commissioner makes an application to the court for the grant of an injunction under this section, the court shall not require the Commissioner or any other person, as a condition of the granting of an interim injunction, to give any undertakings as to damages.

(8) The powers conferred on the court under this section are in addition to, and not in derogation of, any powers of the court, whether conferred by this Act or otherwise.

98A Treatment of partnerships

(1) If, apart from this subsection, this Act would impose an obligation on a partnership, the obligation is imposed instead on each partner but may be discharged by any of the partners.

(2) If, apart from this subsection, an offence against this Act would be committed by a partnership, the offence is taken to have been committed by each partner.

(3) If, apart from this subsection, a partnership would contravene a civil penalty provision, the contravention is taken to have been committed by each partner.

(4) A partner does not commit an offence against this Act because of subsection (2), or contravene a civil penalty provision because of subsection (3), if the partner:
Part IX Miscellaneous

Section 98B

(a) does not know of the circumstances that constitute the contravention of the provision concerned; or
(b) knows of those circumstances but takes all reasonable steps to correct the contravention as soon as possible after the partner becomes aware of those circumstances.

Note: In criminal proceedings, a defendant bears an evidential burden in relation to the matters in subsection (4) (see subsection 13.3(3) of the Criminal Code).

98B Treatment of unincorporated associations

(1) If, apart from this subsection, this Act would impose an obligation on an unincorporated association, the obligation is imposed instead on each member of the association’s committee of management but may be discharged by any of the members.

(2) If, apart from this subsection, an offence against this Act would be committed by an unincorporated association, the offence is taken to have been committed by each member of the association’s committee of management.

(3) If, apart from this subsection, an unincorporated association would contravene a civil penalty provision, the contravention is taken to have been committed by each member of the association’s committee of management.

(4) A member of an unincorporated association’s committee of management does not commit an offence against this Act because of subsection (2), or contravene a civil penalty provision because of subsection (3), if the member:

(a) does not know of the circumstances that constitute the contravention of the provision concerned; or
(b) knows of those circumstances but takes all reasonable steps to correct the contravention as soon as possible after the member becomes aware of those circumstances.

Note: In criminal proceedings, a defendant bears an evidential burden in relation to the matters in subsection (4) (see subsection 13.3(3) of the Criminal Code).
98C Treatment of trusts

(1) If, apart from this subsection, this Act would impose an obligation on a trust, the obligation is imposed instead on each trustee of the trust but may be discharged by any of the trustees.

(2) If, apart from this subsection, an offence against this Act would be committed by a trust, the offence is taken to have been committed by each trustee of the trust.

(3) If, apart from this subsection, a trust would contravene a civil penalty provision, the contravention is taken to have been committed by each trustee of the trust.

(4) A trustee of a trust does not commit an offence against this Act because of subsection (2), or contravene a civil penalty provision because of subsection (3), if the trustee:
   (a) does not know of the circumstances that constitute the contravention of the provision concerned; or
   (b) knows of those circumstances but takes all reasonable steps to correct the contravention as soon as possible after the trustee becomes aware of those circumstances.

Note: In criminal proceedings, a defendant bears an evidential burden in relation to the matters in subsection (4) (see subsection 13.3(3) of the Criminal Code).

99A Conduct of directors, employees and agents

(1) Where, in proceedings for an offence against this Act or for a civil penalty order, it is necessary to establish the state of mind of a body corporate in relation to particular conduct, it is sufficient to show:
   (a) that the conduct was engaged in by a director, employee or agent of the body corporate within the scope of his or her actual or apparent authority; and
   (b) that the director, employee or agent had the state of mind.

(2) Any conduct engaged in on behalf of a body corporate by a director, employee or agent of the body corporate within the scope
Part IX  Miscellaneous

Section 99A

of his or her actual or apparent authority is to be taken, for the purposes of a prosecution for an offence against this Act or proceedings for a civil penalty order, to have been engaged in also by the body corporate unless the body corporate establishes that the body corporate took reasonable precautions and exercised due diligence to avoid the conduct.

(3) Where, in proceedings for an offence against this Act or for a civil penalty order, it is necessary to establish the state of mind of a person other than a body corporate in relation to particular conduct, it is sufficient to show:
   (a) that the conduct was engaged in by an employee or agent of the person within the scope of his or her actual or apparent authority; and
   (b) that the employee or agent had the state of mind.

(4) Any conduct engaged in on behalf of a person other than a body corporate by an employee or agent of a person within the scope of his or her actual or apparent authority is to be taken, for the purposes of a prosecution for an offence against this Act or proceedings for a civil penalty order, to have been engaged in also by the first-mentioned person unless the first-mentioned person establishes that the first-mentioned person took reasonable precautions and exercised due diligence to avoid the conduct.

(5) Where:
   (a) a person other than a body corporate is convicted of an offence; and
   (b) the person would not have been convicted of the offence if subsections (3) and (4) had not been enacted;
the person is not liable to be punished by imprisonment for that offence.

(6) A reference in subsection (1) or (3) to the state of mind of a person includes a reference to:
   (a) the knowledge, intention, opinion, belief or purpose of the person; and
Section 100

(b) the person’s reasons for the intention, opinion, belief or purpose.

(7) A reference in this section to a director of a body corporate includes a reference to a constituent member of a body corporate incorporated for a public purpose by a law of the Commonwealth, of a State or of a Territory.

(8) A reference in this section to engaging in conduct includes a reference to failing or refusing to engage in conduct.

100 Regulations

(1) The Governor-General may make regulations, not inconsistent with this Act, prescribing matters:
   (a) required or permitted by this Act to be prescribed; or
   (b) necessary or convenient to be prescribed for carrying out or giving effect to this Act.

(2) Before the Governor-General makes regulations for the purposes of Australian Privacy Principle 9.3 prescribing a government related identifier, an organisation or a class of organisations, and circumstances, the Minister must be satisfied that:
   (a) the relevant agency or State or Territory authority or, if the relevant agency or State or Territory authority has a principal executive, the principal executive:
       (i) has agreed that the adoption, use or disclosure of the identifier by the organisation, or the class of organisations, in the circumstances is appropriate; and
       (ii) has consulted the Commissioner about that adoption, use or disclosure; and
   (b) the adoption, use or disclosure of the identifier by the organisation, or the class of organisations, in the circumstances can only be for the benefit of the individual to whom the identifier relates.

(3) Subsection (2) does not apply to the making of regulations for the purposes of Australian Privacy Principle 9.3 that relate to the use
or disclosure of a government related identifier by an organisation, or a class of organisations, in particular circumstances if:

(a) the identifier is a kind commonly used in the processing of pay, or deductions from pay, of Commonwealth officers, or a class of Commonwealth officers; and

(b) the circumstances of the use or disclosure of the identifier relate to the provision by:
   (i) the organisation; or
   (ii) the class of organisations;

of superannuation services (including the management, processing, allocation and transfer of superannuation contributions) for the benefit of Commonwealth officers or the class of Commonwealth officers; and

(c) before the regulations are made, the Minister consults the Commissioner about the proposed regulations.
Schedule 1—Australian Privacy Principles

Note: See section 14.

Overview of the Australian Privacy Principles

Overview

This Schedule sets out the Australian Privacy Principles.

Part 1 sets out principles that require APP entities to consider the privacy of personal information, including ensuring that APP entities manage personal information in an open and transparent way.

Part 2 sets out principles that deal with the collection of personal information including unsolicited personal information.

Part 3 sets out principles about how APP entities deal with personal information and government related identifiers. The Part includes principles about the use and disclosure of personal information and those identifiers.

Part 4 sets out principles about the integrity of personal information. The Part includes principles about the quality and security of personal information.

Part 5 sets out principles that deal with requests for access to, and the correction of, personal information.

Australian Privacy Principles

The Australian Privacy Principles are:

Australian Privacy Principle 1—open and transparent management of personal information
<table>
<thead>
<tr>
<th>Australian Privacy Principle 2—anonymity and pseudonymity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australian Privacy Principle 3—collection of solicited</td>
</tr>
<tr>
<td>personal information</td>
</tr>
<tr>
<td>Australian Privacy Principle 4—dealing with unsolicited</td>
</tr>
<tr>
<td>personal information</td>
</tr>
<tr>
<td>Australian Privacy Principle 5—notification of the collection of personal information</td>
</tr>
<tr>
<td>Australian Privacy Principle 6—use or disclosure of personal information</td>
</tr>
<tr>
<td>Australian Privacy Principle 7—direct marketing</td>
</tr>
<tr>
<td>Australian Privacy Principle 8—cross-border disclosure of personal information</td>
</tr>
<tr>
<td>Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers</td>
</tr>
<tr>
<td>Australian Privacy Principle 10—quality of personal information</td>
</tr>
<tr>
<td>Australian Privacy Principle 11—security of personal information</td>
</tr>
<tr>
<td>Australian Privacy Principle 12—access to personal information</td>
</tr>
<tr>
<td>Australian Privacy Principle 13—correction of personal information</td>
</tr>
</tbody>
</table>
Part 1—Consideration of personal information privacy

1 Australian Privacy Principle 1—open and transparent management of personal information

1.1 The object of this principle is to ensure that APP entities manage personal information in an open and transparent way.

Compliance with the Australian Privacy Principles etc.

1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity’s functions or activities that:

(a) will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and

(b) will enable the entity to deal with inquiries or complaints from individuals about the entity’s compliance with the Australian Privacy Principles or such a code.

APP Privacy policy

1.3 An APP entity must have a clearly expressed and up-to-date policy (the APP privacy policy) about the management of personal information by the entity.

1.4 Without limiting subclause 1.3, the APP privacy policy of the APP entity must contain the following information:

(a) the kinds of personal information that the entity collects and holds;

(b) how the entity collects and holds personal information;

(c) the purposes for which the entity collects, holds, uses and discloses personal information;
Clause 2

(d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;
(e) how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;
(f) whether the entity is likely to disclose personal information to overseas recipients;
(g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

Availability of APP privacy policy etc.

1.5 An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available:
   (a) free of charge; and
   (b) in such form as is appropriate.

Note: An APP entity will usually make its APP privacy policy available on the entity’s website.

1.6 If a person or body requests a copy of the APP privacy policy of an APP entity in a particular form, the entity must take such steps as are reasonable in the circumstances to give the person or body a copy in that form.

2 Australian Privacy Principle 2—anonymity and pseudonymity

2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

2.2 Subclause 2.1 does not apply if, in relation to that matter:
   (a) the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or
Clause 2

(b) it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.
Part 2—Collection of personal information

3 Australian Privacy Principle 3—collection of solicited personal information

Personal information other than sensitive information

3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity’s functions or activities.

3.2 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity’s functions or activities.

Sensitive information

3.3 An APP entity must not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information and:
   (i) if the entity is an agency—the information is reasonably necessary for, or directly related to, one or more of the entity’s functions or activities; or
   (ii) if the entity is an organisation—the information is reasonably necessary for one or more of the entity’s functions or activities; or

(b) subclause 3.4 applies in relation to the information.

3.4 This subclause applies in relation to sensitive information about an individual if:

(a) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or
Clause 3

(b) a permitted general situation exists in relation to the collection of the information by the APP entity; or

(c) the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; or

(d) the APP entity is an enforcement body and the entity reasonably believes that:
   (i) if the entity is the Immigration Department—the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or
   (ii) otherwise—the collection of the information is reasonably necessary for, or directly related to, one or more of the entity’s functions or activities; or

(e) the APP entity is a non-profit organisation and both of the following apply:
   (i) the information relates to the activities of the organisation;
   (ii) the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

Note: For permitted general situation, see section 16A. For permitted health situation, see section 16B.

Means of collection

3.5 An APP entity must collect personal information only by lawful and fair means.

3.6 An APP entity must collect personal information about an individual only from the individual unless:
(a) if the entity is an agency:
   (i) the individual consents to the collection of the information from someone other than the individual; or
Clause 4

(ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or

(b) it is unreasonable or impracticable to do so.

Solicited personal information

3.7 This principle applies to the collection of personal information that is solicited by an APP entity.

4 Australian Privacy Principle 4—dealing with unsolicited personal information

4.1 If:
   (a) an APP entity receives personal information; and
   (b) the entity did not solicit the information;
the entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information.

4.2 The APP entity may use or disclose the personal information for the purposes of making the determination under subclause 4.1.

4.3 If:
   (a) the APP entity determines that the entity could not have collected the personal information; and
   (b) the information is not contained in a Commonwealth record;
the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

4.4 If subclause 4.3 does not apply in relation to the personal information, Australian Privacy Principles 5 to 13 apply in relation to the information as if the entity had collected the information under Australian Privacy Principle 3.
5 Australian Privacy Principle 5—notification of the collection of personal information

5.1 At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

(a) to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or

(b) to otherwise ensure that the individual is aware of any such matters.

5.2 The matters for the purposes of subclause 5.1 are as follows:

(a) the identity and contact details of the APP entity;

(b) if:
   
   (i) the APP entity collects the personal information from someone other than the individual; or
   
   (ii) the individual may not be aware that the APP entity has collected the personal information;

   the fact that the entity so collects, or has collected, the information and the circumstances of that collection;

(c) if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order—the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection);

(d) the purposes for which the APP entity collects the personal information;

(e) the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;

(f) any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity;
 Clause 5

(g) that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;
(h) that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;
(i) whether the APP entity is likely to disclose the personal information to overseas recipients;
(j) if the APP entity is likely to disclose the personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.
Part 3—Dealing with personal information

6 Australian Privacy Principle 6—use or disclosure of personal information

Use or disclosure

6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless:
   (a) the individual has consented to the use or disclosure of the information; or
   (b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.

Note: Australian Privacy Principle 8 sets out requirements for the disclosure of personal information to a person who is not in Australia or an external Territory.

6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:
   (a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:
      (i) if the information is sensitive information—directly related to the primary purpose; or
      (ii) if the information is not sensitive information—related to the primary purpose; or
   (b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or
   (c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or
(d) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or
(e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Note: For permitted general situation, see section 16A. For permitted health situation, see section 16B.

6.3 This subclause applies in relation to the disclosure of personal information about an individual by an APP entity that is an agency if:
(a) the agency is not an enforcement body; and
(b) the information is biometric information or biometric templates; and
(c) the recipient of the information is an enforcement body; and
(d) the disclosure is conducted in accordance with the guidelines made by the Commissioner for the purposes of this paragraph.

6.4 If:
(a) the APP entity is an organisation; and
(b) subsection 16B(2) applied in relation to the collection of the personal information by the entity;
the entity must take such steps as are reasonable in the circumstances to ensure that the information is de-identified before the entity discloses it in accordance with subclause 6.1 or 6.2.

Written note of use or disclosure

6.5 If an APP entity uses or discloses personal information in accordance with paragraph 6.2(e), the entity must make a written note of the use or disclosure.

Related bodies corporate

6.6 If:
Clause 7

(a) an APP entity is a body corporate; and
(b) the entity collects personal information from a related body corporate;
this principle applies as if the entity’s primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.

Exceptions

6.7 This principle does not apply to the use or disclosure by an organisation of:
(a) personal information for the purpose of direct marketing; or
(b) government related identifiers.

7 Australian Privacy Principle 7—direct marketing

Direct marketing

7.1 If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Exceptions—personal information other than sensitive information

7.2 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:
(a) the organisation collected the information from the individual; and
(b) the individual would reasonably expect the organisation to use or disclose the information for that purpose; and
(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and
Clause 7

(d) the individual has not made such a request to the organisation.

7.3 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

(a) the organisation collected the information from:
   (i) the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or
   (ii) someone other than the individual; and
(b) either:
   (i) the individual has consented to the use or disclosure of the information for that purpose; or
   (ii) it is impracticable to obtain that consent; and
(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and
(d) in each direct marketing communication with the individual:
   (i) the organisation includes a prominent statement that the individual may make such a request; or
   (ii) the organisation otherwise draws the individual’s attention to the fact that the individual may make such a request; and
(e) the individual has not made such a request to the organisation.

Exception—sensitive information

7.4 Despite subclause 7.1, an organisation may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.
Exception—contracted service providers

7.5 Despite subclause 7.1, an organisation may use or disclose personal information for the purpose of direct marketing if:
   (a) the organisation is a contracted service provider for a Commonwealth contract; and
   (b) the organisation collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract; and
   (c) the use or disclosure is necessary to meet (directly or indirectly) such an obligation.

Individual may request not to receive direct marketing communications etc.

7.6 If an organisation (the first organisation) uses or discloses personal information about an individual:
   (a) for the purpose of direct marketing by the first organisation; or
   (b) for the purpose of facilitating direct marketing by other organisations;
the individual may:
   (c) if paragraph (a) applies—request not to receive direct marketing communications from the first organisation; and
   (d) if paragraph (b) applies—request the organisation not to use or disclose the information for the purpose referred to in that paragraph; and
   (e) request the first organisation to provide its source of the information.

7.7 If an individual makes a request under subclause 7.6, the first organisation must not charge the individual for the making of, or to give effect to, the request and:
   (a) if the request is of a kind referred to in paragraph 7.6(c) or (d)—the first organisation must give effect to the request within a reasonable period after the request is made; and
Clause 8

(b) if the request is of a kind referred to in paragraph 7.6(e)—the organisation must, within a reasonable period after the request is made, notify the individual of its source unless it is impracticable or unreasonable to do so.

Interaction with other legislation

7.8 This principle does not apply to the extent that any of the following apply:
   (a) the Do Not Call Register Act 2006;
   (b) the Spam Act 2003;
   (c) any other Act of the Commonwealth, or a Norfolk Island enactment, prescribed by the regulations.

8 Australian Privacy Principle 8—cross-border disclosure of personal information

8.1 Before an APP entity discloses personal information about an individual to a person (the overseas recipient):
   (a) who is not in Australia or an external Territory; and
   (b) who is not the entity or the individual;
   the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.

8.2 Subclause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:
   (a) the entity reasonably believes that:
       (i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least
substantially similar to the way in which the Australian Privacy Principles protect the information; and
(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

(b) both of the following apply:
(i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure;
(ii) after being so informed, the individual consents to the disclosure; or

(c) the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or

(e) the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or

(f) the entity is an agency and both of the following apply:
(i) the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;
(ii) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

Note: For permitted general situation, see section 16A.
Clause 9

9 Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers

Adoption of government related identifiers

9.1 An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless:

(a) the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(b) subclause 9.3 applies in relation to the adoption.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Use or disclosure of government related identifiers

9.2 An organisation must not use or disclose a government related identifier of an individual unless:

(a) the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation’s activities or functions; or

(b) the use or disclosure of the identifier is reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or

(c) the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the identifier; or

(e) the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(f) subclause 9.3 applies in relation to the use or disclosure.

Note 1: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Note 2: For permitted general situation, see section 16A.
Regulations about adoption, use or disclosure

9.3 This subclause applies in relation to the adoption, use or disclosure by an organisation of a government related identifier of an individual if:

(a) the identifier is prescribed by the regulations; and
(b) the organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations; and
(c) the adoption, use or disclosure occurs in the circumstances prescribed by the regulations.

Note: There are prerequisites that must be satisfied before the matters mentioned in this subclause are prescribed, see subsections 100(2) and (3).
Part 4—Integrity of personal information

10 Australian Privacy Principle 10—quality of personal information

10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete.

10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

11 Australian Privacy Principle 11—security of personal information

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and
(b) from unauthorised access, modification or disclosure.

11.2 If:

(a) an APP entity holds personal information about an individual; and
(b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and
(c) the information is not contained in a Commonwealth record; and
(d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.
Part 5—Access to, and correction of, personal information

12 Australian Privacy Principle 12—access to personal information

Access

12.1 If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

Exception to access—agency

12.2 If:

(a) the APP entity is an agency; and
(b) the entity is required or authorised to refuse to give the individual access to the personal information by or under:
   (i) the Freedom of Information Act; or
   (ii) any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents;

then, despite subclause 12.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access.

Exception to access—organisation

12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:

(a) the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or
(b) giving access would have an unreasonable impact on the privacy of other individuals; or
Schedule 1  Australian Privacy Principles  
Part 5  Access to, and correction of, personal information

Clause 12

(c) the request for access is frivolous or vexatious; or
(d) the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings; or
(e) giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
(f) giving access would be unlawful; or
(g) denying access is required or authorised by or under an Australian law or a court/tribunal order; or
(h) both of the following apply:
   (i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity’s functions or activities has been, is being or may be engaged in;
   (ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or
(i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or
(j) giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

Dealing with requests for access

12.4 The APP entity must:
(a) respond to the request for access to the personal information:
   (i) if the entity is an agency—within 30 days after the request is made; or
   (ii) if the entity is an organisation—within a reasonable period after the request is made; and
(b) give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.
Other means of access

12.5 If the APP entity refuses:
   (a) to give access to the personal information because of subclause 12.2 or 12.3; or
   (b) to give access in the manner requested by the individual;
the entity must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the entity and the individual.

12.6 Without limiting subclause 12.5, access may be given through the use of a mutually agreed intermediary.

Access charges

12.7 If the APP entity is an agency, the entity must not charge the individual for the making of the request or for giving access to the personal information.

12.8 If:
   (a) the APP entity is an organisation; and
   (b) the entity charges the individual for giving access to the personal information;
the charge must not be excessive and must not apply to the making of the request.

Refusal to give access

12.9 If the APP entity refuses to give access to the personal information because of subclause 12.2 or 12.3, or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out:
   (a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and
   (b) the mechanisms available to complain about the refusal; and
   (c) any other matter prescribed by the regulations.
Clause 13

12.10 If the APP entity refuses to give access to the personal information because of paragraph 12.3(j), the reasons for the refusal may include an explanation for the commercially sensitive decision.

13 Australian Privacy Principle 13—correction of personal information

Correction

13.1 If:
   (a) an APP entity holds personal information about an individual; and
   (b) either:
      (i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading; or
      (ii) the individual requests the entity to correct the information;
the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.

Notification of correction to third parties

13.2 If:
   (a) the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and
   (b) the individual requests the entity to notify the other APP entity of the correction;
the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.
Refusal to correct information

13.3 If the APP entity refuses to correct the personal information as requested by the individual, the entity must give the individual a written notice that sets out:
(a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and
(b) the mechanisms available to complain about the refusal; and
(c) any other matter prescribed by the regulations.

Request to associate a statement

13.4 If:
(a) the APP entity refuses to correct the personal information as requested by the individual; and
(b) the individual requests the entity to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading;
the entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

Dealing with requests

13.5 If a request is made under subclause 13.1 or 13.4, the APP entity:
(a) must respond to the request:
   (i) if the entity is an agency—within 30 days after the request is made; or
   (ii) if the entity is an organisation—within a reasonable period after the request is made; and
(b) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be).
Endnotes

Endnote 1—About the endnotes

The endnotes provide information about this compilation and the compiled law.

The following endnotes are included in every compilation:

Endnote 1—About the endnotes
Endnote 2—Abbreviation key
Endnote 3—Legislation history
Endnote 4—Amendment history

Abbreviation key—Endnote 2

The abbreviation key sets out abbreviations that may be used in the endnotes.

Legislation history and amendment history—Endnotes 3 and 4

Amending laws are annotated in the legislation history and amendment history.

The legislation history in endnote 3 provides information about each law that
has amended (or will amend) the compiled law. The information includes
commencement details for amending laws and details of any application, saving
or transitional provisions that are not included in this compilation.

The amendment history in endnote 4 provides information about amendments at
the provision (generally section or equivalent) level. It also includes information
about any provision of the compiled law that has been repealed in accordance
with a provision of the law.

Editorial changes

The Legislation Act 2003 authorises First Parliamentary Counsel to make
editorial and presentational changes to a compiled law in preparing a
compilation of the law for registration. The changes must not change the effect
of the law. Editorial changes take effect from the compilation registration date.

If the compilation includes editorial changes, the endnotes include a brief
outline of the changes in general terms. Full details of any changes can be
obtained from the Office of Parliamentary Counsel.

Misdescribed amendments

A misdescribed amendment is an amendment that does not accurately describe
the amendment to be made. If, despite the misdescription, the amendment can

332

Privacy Act 1988

Compilation No. 78

Compilation date: 1/7/18

Registered: 30/7/18
Endnotes

Endnote 1—About the endnotes

be given effect as intended, the amendment is incorporated into the compiled law and the abbreviation “(md)” added to the details of the amendment included in the amendment history.

If a misdescribed amendment cannot be given effect as intended, the abbreviation “(md not incorp)” is added to the details of the amendment included in the amendment history.
### Endnote 3—Legislation history

<table>
<thead>
<tr>
<th>Act</th>
<th>Number and year</th>
<th>Assent</th>
<th>Commencement</th>
<th>Application, saving and transitional provisions</th>
</tr>
</thead>
</table>

as amended by

<table>
<thead>
<tr>
<th>Act</th>
<th>Number and year</th>
<th>Assent</th>
<th>Commencement</th>
<th>Application, saving and transitional provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industrial Relations Legislation Amendment Act 1991</td>
<td>122, 1991</td>
<td>27 June 1991</td>
<td>s 31(2) and Sch: 10 Dec 1991 (s 2(3) and gaz 1991, No S332)</td>
<td>s 31(2)</td>
</tr>
</tbody>
</table>

---

_Endnote 3—Legislation history

**Privacy Act 1988**

Compilation No. 78

Compilation date: 1/7/18

Registered: 30/7/18

Authorized Version C2018C00292 registered 30/07/2018
### Endnotes

#### Endnote 3—Legislation history

<table>
<thead>
<tr>
<th>Act</th>
<th>Number and year</th>
<th>Assent</th>
<th>Commencement</th>
<th>Application, saving and transitional provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Law and Justice Legislation Amendment Act (No. 4) 1992</td>
<td>143, 1992</td>
<td>7 Dec 1992</td>
<td>Sch: 7 Dec 1992 (s 2(1))</td>
<td>—</td>
</tr>
<tr>
<td>National Health Amendment Act 1993</td>
<td>28, 1993</td>
<td>9 June 1993</td>
<td>s 7 and 8: 9 June 1993 (s 2)</td>
<td>—</td>
</tr>
<tr>
<td>Law and Justice Legislation Amendment Act 1993</td>
<td>13, 1994</td>
<td>18 Jan 1994</td>
<td>s 7–16 and Note 1 of Notes about section headings: 18 Jan 1994 (s 2(1))</td>
<td>s 16</td>
</tr>
<tr>
<td>Law and Justice Legislation Amendment Act 1997</td>
<td>34, 1997</td>
<td>17 Apr 1997</td>
<td>Sch 13: 17 Apr 1997 (s 2(1))</td>
<td>—</td>
</tr>
</tbody>
</table>

---

Privacy Act 1988

Compilation No. 78

Compilation date: 1/7/18

Registered: 30/7/18
### Endnote 3—Legislation history

<table>
<thead>
<tr>
<th>Act</th>
<th>Number and year</th>
<th>Assent</th>
<th>Commencement</th>
<th>Application, saving and transitional provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hearing Services and AGHS Reform Act 1997</td>
<td>82, 1997</td>
<td>18 June 1997</td>
<td>Sch 4 (items 1, 2, 4–12): 18 June 1997 (s 2(1))&lt;br&gt;Sch 4 (item 3): never commenced (s 2(3))</td>
<td>Sch 4 (item 12)</td>
</tr>
</tbody>
</table>

as amended by

<table>
<thead>
<tr>
<th>Act</th>
<th>Number and year</th>
<th>Assent</th>
<th>Commencement</th>
<th>Application, saving and transitional provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statute Law Revision Act 2005</td>
<td>100, 2005</td>
<td>6 July 2005</td>
<td>Sch 2 (item 20): 18 June 1997 (s 2(1) item 38)</td>
<td>—</td>
</tr>
<tr>
<td>Statute Law Revision Act 2006</td>
<td>9, 2006</td>
<td>23 Mar 2006</td>
<td>Sch 2 (item 19): 18 June 1997 (s 2(1) item 34)</td>
<td>—</td>
</tr>
</tbody>
</table>

---

*Privacy Act 1988* 337

Compilation No. 78

Compilation date: 1/7/18

Registered: 30/7/18
### Endnotes

#### Endnote 3—Legislation history

<table>
<thead>
<tr>
<th>Act</th>
<th>Number and year</th>
<th>Assent</th>
<th>Commencement</th>
<th>Application, saving and transitional provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>as amended by</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disability Discrimination and Other Human Rights Legislation Amendment Act 2009</td>
<td>70, 2009</td>
<td>8 July 2009</td>
<td>Sch 3 (items 58, 59): 5 Aug 2009 (s 2(1) item 7)</td>
<td>—</td>
</tr>
<tr>
<td>Australian Federal Police Legislation Amendment Act 2000</td>
<td>9, 2000</td>
<td>7 Mar 2000</td>
<td>Sch 2 (items 42–46) and Sch 3 (items 20, 29, 34, 35): 2 July 2000 (s 2(1) and gaz 2000, No S328)</td>
<td>Sch 3 (items 20, 29, 34, 35)</td>
</tr>
<tr>
<td>Privacy Amendment (Private Sector) Act 2000</td>
<td>155, 2000</td>
<td>21 Dec 2000</td>
<td>Sch 1: 21 Dec 2001 (s 2(1)) Sch 3 (items 3, 4): 21 Dec 2000 (s 2(2))</td>
<td>Sch 1 (items 37, 53, 57, 76, 100, 124, 130 and Sch 3 (item 4))</td>
</tr>
<tr>
<td>Law and Justice Legislation Amendment (Application of Criminal Code) Act 2001</td>
<td>24, 2001</td>
<td>6 Apr 2001</td>
<td>s 4(1), (2) and Sch 40 (items 1–9, 11–13): 24 May 2001 (s 2(1)(a)) Sch 40 (item 10): 21 Dec 2001 (s 2(7))</td>
<td>s 4(1) and (2)</td>
</tr>
</tbody>
</table>

338

*Privacy Act 1988*

Compilation No. 78

Compilation date: 1/7/18

Registered: 30/7/18
### Endnote 3—Legislation history

<table>
<thead>
<tr>
<th>Act</th>
<th>Number and year</th>
<th>Assent</th>
<th>Commencement</th>
<th>Application, saving and transitional provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>as amended by</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Abolition of Compulsory Age Retirement (Statutory Officeholders) Act 2001</td>
<td>159, 2001</td>
<td>1 Oct 2001</td>
<td>Sch 1 (items 82–84, 97): 29 Oct 2001 (s 2(1))</td>
<td>Sch 1 (item 97)</td>
</tr>
<tr>
<td>Privacy Amendment Act 2004</td>
<td>49, 2004</td>
<td>21 Apr 2004</td>
<td>21 Apr 2004 (s 2)</td>
<td>Sch 1 (items 3, 5)</td>
</tr>
<tr>
<td>as amended by</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Statute Law Revision Act 2006</td>
<td>9, 2006</td>
<td>23 Mar 2006</td>
<td>Sch 2 (item 21): 21 Apr 2004 (s 2(1) item 36)</td>
<td>—</td>
</tr>
<tr>
<td>Administrative Appeals Tribunal Amendment Act 2005</td>
<td>38, 2005</td>
<td>1 Apr 2005</td>
<td>Sch 1 (item 229): 16 May 2005 (s 2(1) item 6)</td>
<td>—</td>
</tr>
<tr>
<td>Statute Law Revision Act 2005</td>
<td>100, 2005</td>
<td>6 July 2005</td>
<td>Sch 1 (item 38): 6 July 2005 (s 2(1) item 21)</td>
<td>—</td>
</tr>
<tr>
<td>Intelligence Services Legislation Amendment Act 2005</td>
<td>128, 2005</td>
<td>4 Nov 2005</td>
<td>Sch 6: 2 Dec 2005 (s 2(1) item 2)</td>
<td>—</td>
</tr>
</tbody>
</table>

*Privacy Act 1988*

 Compilation No. 78  
 Compilation date: 1/7/18  
 Registered: 30/7/18
### Endnote 3—Legislation history

<table>
<thead>
<tr>
<th>Act</th>
<th>Number and year</th>
<th>Assent</th>
<th>Commencement</th>
<th>Application, saving and transitional provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statute Law Revision Act 2006</td>
<td>9, 2006</td>
<td>23 Mar 2006</td>
<td>Sch 1 (item 21): 21 Dec 2001 (s 2(1) item 13)</td>
<td>—</td>
</tr>
<tr>
<td>Postal Industry Ombudsman Act 2006</td>
<td>25, 2006</td>
<td>6 Apr 2006</td>
<td>Sch 1 (items 17–19, 20(2)): 6 Oct 2006 (s 2(1) item 2)</td>
<td>Sch 1 (item 20(2))</td>
</tr>
<tr>
<td><strong>as amended by</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>National Health and Medical Research Council Amendment Act 2006</td>
<td>50, 2006</td>
<td>9 June 2006</td>
<td>Sch 1 (item 115): 1 July 2006 (s 2(1) item 2)</td>
<td>—</td>
</tr>
<tr>
<td>Law Enforcement Integrity Commissioner (Consequential Amendments) Act 2006</td>
<td>86, 2006</td>
<td>30 June 2006</td>
<td>Sch 1 (items 48–53): 30 Dec 2006 (s 2(1) item 2)</td>
<td>—</td>
</tr>
<tr>
<td>Privacy Legislation Amendment Act 2006</td>
<td>99, 2006</td>
<td>14 Sept 2006</td>
<td>Sch 1 (item 2) and Sch 2: 14 Sept 2006 (s 2)</td>
<td>—</td>
</tr>
<tr>
<td>Privacy Legislation Amendment (Emergencies and Disasters) Act 2006</td>
<td>148, 2006</td>
<td>6 Dec 2006</td>
<td>Sch 1: 7 Dec 2006 (s 2)</td>
<td>—</td>
</tr>
</tbody>
</table>

340 *Privacy Act 1988*
### Endnote 3—Legislation history

<table>
<thead>
<tr>
<th>Act</th>
<th>Number and year</th>
<th>Assent</th>
<th>Commencement</th>
<th>Application, saving and transitional provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customs Legislation Amendment (Name Change) Act 2009</td>
<td>33, 2009</td>
<td>22 May 2009</td>
<td>Sch 2 (item 46): 23 May 2009 (s 2)</td>
<td>—</td>
</tr>
<tr>
<td>Fair Work (State Referral and Consequential and Other Amendments) Act 2009</td>
<td>54, 2009</td>
<td>25 June 2009</td>
<td>Sch 16 (items 1–3): 1 July 2009 (s 2(1) item 39)</td>
<td>—</td>
</tr>
<tr>
<td>Disability Discrimination and Other Human Rights Legislation Amendment Act 2009</td>
<td>70, 2009</td>
<td>8 July 2009</td>
<td>Sch 3 (items 47–57): 5 Aug 2009 (s 2(1) item 7)</td>
<td>—</td>
</tr>
<tr>
<td>Crimes Legislation Amendment (Serious and Organised Crime) Act (No. 2) 2010</td>
<td>4, 2010</td>
<td>19 Feb 2010</td>
<td>Sch 10 (item 23): 20 Feb 2010 (s 2(1) item 13)</td>
<td>—</td>
</tr>
</tbody>
</table>

*Privacy Act 1988*  
Compilation No. 78  
Compilation date: 1/7/18  
Registered: 30/7/18
### Endnotes

#### Endnote 3—Legislation history

<table>
<thead>
<tr>
<th>Act</th>
<th>Number and year</th>
<th>Assent</th>
<th>Commencement</th>
<th>Application, saving and transitional provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statute Law Revision Act 2010</td>
<td>8, 2010</td>
<td>1 Mar 2010</td>
<td>Sch 5 (items 77, 78): 1 Mar 2010 (s 2(1) item 35)</td>
<td>—</td>
</tr>
<tr>
<td>Freedom of Information Amendment (Reform) Act 2010</td>
<td>51, 2010</td>
<td>31 May 2010</td>
<td>Sch 3 (item 38), Sch 5 (items 52–58) and Sch 7: 1 Nov 2010 (s 2(1) items 6, 7)</td>
<td>Sch 7</td>
</tr>
<tr>
<td>Healthcare Identifiers (Consequential Amendments) Act 2010</td>
<td>73, 2010</td>
<td>28 June 2010</td>
<td>Sch 2 (items 1–7): 29 June 2010 (s 2(1) item 3) Sch 2 (items 8–11): 30 Jan 2012 (s 2(1) item 4)</td>
<td>—</td>
</tr>
<tr>
<td>Territories Law Reform Act 2010</td>
<td>139, 2010</td>
<td>10 Dec 2010</td>
<td>Sch 1 (item 76): 11 Dec 2010 (s 2(1) item 2) Sch 1 (items 244–297): 1 Jan 2011 (s 2(1) item 10)</td>
<td>Sch 1 (item 297)</td>
</tr>
<tr>
<td>Tax Laws Amendment (Confidentiality of Taxpayer Information) Act 2010</td>
<td>145, 2010</td>
<td>16 Dec 2010</td>
<td>Sch 2 (items 62, 63): 17 Dec 2010 (s 2(1) item 2)</td>
<td>—</td>
</tr>
<tr>
<td>Statute Law Revision Act 2011</td>
<td>5, 2011</td>
<td>22 Mar 2011</td>
<td>Sch 1 (items 93–95): 22 Mar 2011 (s 2(1) item 2)</td>
<td>—</td>
</tr>
</tbody>
</table>

342  
*Privacy Act 1988*

Compilation No. 78  
Compilation date: 1/7/18  
Registered: 30/7/18
### Endnote 3—Legislation history

<table>
<thead>
<tr>
<th>Act</th>
<th>Number and year</th>
<th>Assent</th>
<th>Commencement</th>
<th>Application, saving and transitional provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education Services for Overseas Students Legislation Amendment Act 2011</td>
<td>11, 2011</td>
<td>8 Apr 2011</td>
<td>Sch 2 (items 5–7): 9 Apr 2011 (s 2(1) item 2)</td>
<td>—</td>
</tr>
<tr>
<td>Acts Interpretation Amendment Act 2011</td>
<td>46, 2011</td>
<td>27 June 2011</td>
<td>Sch 2 (items 915–922) and Sch 3 (items 10, 11): 27 Dec 2011 (s 2(1) items 7, 12)</td>
<td>Sch 3 (items 10, 11)</td>
</tr>
<tr>
<td>Crimes Legislation Amendment (Powers and Offences) Act 2012</td>
<td>24, 2012</td>
<td>4 Apr 2012</td>
<td>Sch 4 (item 52): 5 Apr 2012 (s 2(1) item 7)</td>
<td>—</td>
</tr>
<tr>
<td>Telecommunications Interception and Other Legislation Amendment (State Bodies) Act 2012</td>
<td>74, 2012</td>
<td>27 June 2012</td>
<td>Sch 1 (items 2, 28): 10 Feb 2013 (s 2(1) item 2)</td>
<td>Sch 1 (item 28)</td>
</tr>
<tr>
<td>Freedom of Information Amendment (Parliamentary Budget Office) Act 2012</td>
<td>177, 2012</td>
<td>4 Dec 2012</td>
<td>Sch 1 (item 13): 4 Dec 2012 (s 2)</td>
<td>—</td>
</tr>
<tr>
<td>Privacy Amendment (Enhancing Privacy Protection) Act 2012</td>
<td>197, 2012</td>
<td>12 Dec 2012</td>
<td>Sch 1–4: 12 Mar 2014 (s 2(1) item 2) Sch 6 (items 1, 5): 12 Dec 2012 (s 2(1) items 16, 18) Sch 6 (items 2–4, 6–14, 16–19): 12 Mar 2014 (s 2(1) items 17, 19)</td>
<td>Sch 6 (items 1–14, 16–19)</td>
</tr>
</tbody>
</table>

*Privacy Act 1988* 343

Compilation No. 78  
Compilation date: 1/7/18  
Registered: 30/7/18
### Endnotes

#### Endnote 3—Legislation history

<table>
<thead>
<tr>
<th>Act</th>
<th>Number and year</th>
<th>Assent</th>
<th>Commencement</th>
<th>Application, saving and transitional provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>as amended by</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Statute Law Revision Act (No. 1) 2015</td>
<td>5, 2015</td>
<td>25 Feb 2015</td>
<td>Sch 2 (items 4, 5): 12 Mar 2014 (s 2(1) item 6)</td>
<td>—</td>
</tr>
<tr>
<td>Public Service Amendment Act 2013</td>
<td>2, 2013</td>
<td>14 Feb 2013</td>
<td>Sch 3 (items 14, 15): 1 July 2013 (s 2(1) item 2)</td>
<td>—</td>
</tr>
<tr>
<td>Federal Circuit Court of Australia (Consequential Amendments) Act 2013</td>
<td>13, 2013</td>
<td>14 Mar 2013</td>
<td>Sch 1 (items 468, 469) and Sch 2 (item 1): 12 Apr 2013 (s 2(1) items 2, 3)</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sch 3 (items 83–91): 12 Mar 2014 (s 2(1) item 16)</td>
<td></td>
</tr>
<tr>
<td>Statute Law Revision Act (No. 1) 2015</td>
<td>5, 2015</td>
<td>25 Feb 2015</td>
<td>Sch 1 (item 35): 25 Mar 2015 (s 2(1) item 2)</td>
<td>—</td>
</tr>
<tr>
<td>Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015</td>
<td>39, 2015</td>
<td>13 Apr 2015</td>
<td>Sch 1 (items 1H, 1J, 7): 13 Oct 2015 (s 2(1) item 2) Sch 1 (items 8–12): 13 Apr 2015 (s 2(1) items 1, 3)</td>
<td>Sch 1 (items 7–12)</td>
</tr>
</tbody>
</table>

---

344

Privacy Act 1988

Compilation No. 78

Compilation date: 1/7/18

Registered: 30/7/18
## Endnotes

### Endnote 3—Legislation history

<table>
<thead>
<tr>
<th>Act</th>
<th>Number and year</th>
<th>Assent</th>
<th>Commencement</th>
<th>Application, saving and transitional provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customs and Other Legislation Amendment (Australian Border Force) Act 2015</td>
<td>41, 2015</td>
<td>20 May 2015</td>
<td>Sch 5 (items 141, 142) and Sch 9: 1 July 2015 (s 2(1) items 2, 7)</td>
<td>Sch 5 (item 142) and Sch 9</td>
</tr>
<tr>
<td><strong>as amended by</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Australian Border Force Amendment (Protected Information) Act 2017</td>
<td>115, 2017</td>
<td>30 Oct 2017</td>
<td>Sch 1 (item 26): 1 July 2015 (s 2(1) item 2)</td>
<td>—</td>
</tr>
<tr>
<td>Norfolk Island Legislation Amendment Act 2015</td>
<td>59, 2015</td>
<td>26 May 2015</td>
<td>Sch 1 (items 150–175) and Sch 2 (items 356–396): 18 June 2015 (s 2(1) items 2, 6) and Sch 1 (items 184–203): 27 May 2015 (s 2(1) item 3) Sch 2 (items 299–305): 1 July 2016 (s 2(1) item 5)</td>
<td>Sch 1 (items 184–203) and Sch 2 (items 356–396)</td>
</tr>
<tr>
<td><strong>as amended by</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Territories Legislation Amendment Act 2016</td>
<td>33, 2016</td>
<td>23 Mar 2016</td>
<td>Sch 2: 24 Mar 2016 (s 2(1) item 2)</td>
<td>—</td>
</tr>
<tr>
<td>Biosecurity (Consequential Amendments and Transitional Provisions) Act 2015</td>
<td>62, 2015</td>
<td>16 June 2015</td>
<td>Sch 2 (item 53) and Sch 4: 16 June 2016 (s 2(1) items 2, 4)</td>
<td>Sch 3 and 4</td>
</tr>
<tr>
<td><strong>as amended by</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

*Privacy Act 1988*  
Compilation No. 78  
Compilation date: 1/7/18  
Registered: 30/7/18
## Endnotes

### Endnote 3—Legislation history

<table>
<thead>
<tr>
<th>Act</th>
<th>Number and year</th>
<th>Assent</th>
<th>Commencement</th>
<th>Application, saving and transitional provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crimes Legislation Amendment (Powers, Offences and Other Measures) Act 2015</td>
<td>153, 2015</td>
<td>26 Nov 2015</td>
<td>Sch 15 (items 11, 12): 27 Nov 2015 (s 2(1) item 3)</td>
<td>—</td>
</tr>
<tr>
<td>Defence Legislation Amendment (First Principles) Act 2015</td>
<td>164, 2015</td>
<td>2 Dec 2015</td>
<td>Sch 2 (items 69, 80): 1 July 2016 (s 2(1) item 2)</td>
<td>Sch 2 (item 80)</td>
</tr>
<tr>
<td>Statute Law Revision Act (No. 1) 2016</td>
<td>4, 2016</td>
<td>11 Feb 2016</td>
<td>Sch 4 (items 1, 232): 10 Mar 2016 (s 2(1) item 6)</td>
<td>—</td>
</tr>
<tr>
<td>Courts Administration Legislation Amendment Act 2016</td>
<td>24, 2016</td>
<td>18 Mar 2016</td>
<td>Sch 5 (item 28): 1 July 2016 (s 2(1) item 7)</td>
<td>Sch 6</td>
</tr>
<tr>
<td>Australian Crime Commission Amendment (National Policing Information) Act 2016</td>
<td>45, 2016</td>
<td>5 May 2016</td>
<td>Sch 2 (items 9–11): 1 July 2016 (s 2(1) item 1)</td>
<td>Sch 2 (items 10, 11)</td>
</tr>
</tbody>
</table>
### Endnotes

#### Endnote 3—Legislation history

<table>
<thead>
<tr>
<th>Act</th>
<th>Number and year</th>
<th>Assent</th>
<th>Commencement</th>
<th>Application, saving and transitional provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Law Enforcement Legislation Amendment (State Bodies and Other Measures) Act 2016</td>
<td>86, 2016</td>
<td>30 Nov 2016</td>
<td>Sch 1 (items 1, 56–58): 1 Dec 2016 (s 2(1) items 2, 4)</td>
<td>Sch 1 (items 1, 50, 54–58)</td>
</tr>
<tr>
<td>Privacy Amendment (Notifiable Data Breaches) Act 2017</td>
<td>12, 2017</td>
<td>22 Feb 2017</td>
<td>Sch 1: 22 Feb 2018 (s 2(1) item 2)</td>
<td>Sch 1 (item 6)</td>
</tr>
<tr>
<td>Public Governance and Resources Legislation Amendment Act (No. 1) 2017</td>
<td>92, 2017</td>
<td>23 Aug 2017</td>
<td>Sch 3 (items 5–10) and Sch 4: 23 Aug 2017 (s 2(1) item 1)</td>
<td>Sch 4</td>
</tr>
<tr>
<td>Regulatory Powers (Standardisation Reform) Act 2017</td>
<td>124, 2017</td>
<td>6 Nov 2017</td>
<td>Sch 13: awaiting commencement (s 2(1) item 3)</td>
<td>Sch 13 (items 10–12)</td>
</tr>
<tr>
<td>Intelligence Services Amendment (Establishment of the Australian Signals Directorate) Act 2018</td>
<td>25, 2018</td>
<td>11 Apr 2018</td>
<td>Sch 1 (items 86–89, 100–110): 1 July 2018 (s 2(1) items 2, 3)</td>
<td>Sch 1 (items 100–108)</td>
</tr>
</tbody>
</table>
### Endnote 4—Amendment history

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preamble</td>
<td>am No 70, 2009</td>
</tr>
<tr>
<td><strong>Part I</strong></td>
<td></td>
</tr>
<tr>
<td>s 2A</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 3</td>
<td>am No 116, 1990; No 155, 2000; No 197, 2012</td>
</tr>
<tr>
<td>s 3A</td>
<td>ad No 24, 2001</td>
</tr>
<tr>
<td>s 4</td>
<td>am No 92, 1994; No 59, 2015</td>
</tr>
<tr>
<td>s 5</td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 5A</td>
<td>ad No 116, 1990</td>
</tr>
<tr>
<td>s 5B</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>am No 49, 2004; No 197, 2012</td>
</tr>
<tr>
<td><strong>Part II</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Division 1</strong></td>
<td></td>
</tr>
<tr>
<td>Division 1 heading</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 6</td>
<td>am No 11, 1990; No 116, 1990; No 28, 1991; No 136, 1991; No 143, 1992; No 13, 1994; No 92, 1994; No 177, 1994; No 34, 1997; No 82, 1997; No 48, 1998; No 44, 1999; No 146, 1999; No 161, 1999; No 155, 2000; No 55, 2001; No 125, 2002; No 135, 2003; No 100, 2005; No 86, 2006; No 99, 2006; No 158, 2007; No 113, 2008; No 144, 2008; No 33, 2009; No 54, 2009; No 102, 2009; No 51, 2010; No 73, 2010; No 139, 2010; No 3, 2011; No 60, 2011; No 74, 2012; No 197, 2012; No 13, 2013; No 39, 2015; No 41, 2015; No 59, 2015; No 62, 2015; No 153, 2015; No 157, 2015; No 164, 2015; No 45, 2016; No 86, 2016; No 12, 2017; No 92, 2017; No 124, 2017; No 25, 2018</td>
</tr>
<tr>
<td>s 6AA</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 6A</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td>s 6B</td>
<td>am No 113, 2008; No 197, 2012</td>
</tr>
<tr>
<td>s 6BA</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>am No 113, 2008; No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>ad No 197, 2012</td>
</tr>
</tbody>
</table>

348

*Privacy Act 1988*

Compilation No. 78  
Compilation date: 1/7/18  
Registered: 30/7/18
Endnote 4—Amendment history

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>s 6C</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>am No 139, 2010; No 46, 2011; No 197, 2012; No 39, 2015; No 59, 2015; No 126, 2015</td>
</tr>
<tr>
<td>s 6D</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>am No 197, 2012</td>
</tr>
<tr>
<td>s 6DA</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td>s 6E</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>am No 170, 2006; No 54, 2009; No 46, 2011; No 60, 2011; No 126, 2015</td>
</tr>
<tr>
<td>s 6EA</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>am No 197, 2012</td>
</tr>
<tr>
<td>s 6F</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>am No 46, 2011; No 197, 2012; No 126, 2015</td>
</tr>
<tr>
<td>s 6FA</td>
<td>ad No 157, 2015</td>
</tr>
<tr>
<td>s 6FB</td>
<td>ad No 157, 2015</td>
</tr>
</tbody>
</table>

Division 2

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>s 6L</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 6M</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 6N</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 6P</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 6Q</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 6R</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 6S</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 6T</td>
<td>ad No 197, 2012</td>
</tr>
</tbody>
</table>
### Endnote 4—Amendment history

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>s 6U.........................</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 6V.........................</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Division 3</strong></td>
<td></td>
</tr>
<tr>
<td>Division 3 heading</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 7 .........................</td>
<td>am No 75, 1990; No 116, 1990; No 13, 1994; No 84, 1994; No 92, 1994; No 177, 1994; No 82, 1997 (as am by No 100, 2005 and No 9, 2006); No 155, 2000; No 125, 2002; No 128, 2005; No 86, 2006; No 158, 2007; No 102, 2009; No 139, 2010; No 197, 2012; No 108, 2014; No 59, 2015; No 25, 2018</td>
</tr>
<tr>
<td>s 7A..........................</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td>s 7B..........................</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td>s 7C..........................</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td>s 8 .........................</td>
<td>am No 116, 1990; No 113, 1990; No 139, 2010; No 197, 2012</td>
</tr>
<tr>
<td>s 9 .........................</td>
<td>am No 28, 1991; No 139, 2010</td>
</tr>
<tr>
<td>s 10 .........................</td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 11 .........................</td>
<td>am No 28, 1991; No 139, 2010</td>
</tr>
<tr>
<td>s 11A.........................</td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 11B.........................</td>
<td>ad No 116, 1990</td>
</tr>
<tr>
<td>s 12 .........................</td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 12A.........................</td>
<td>ad No 116, 1990</td>
</tr>
<tr>
<td>s 12B.........................</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td><strong>Part III</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Division 1</strong></td>
<td></td>
</tr>
<tr>
<td>Division 1 heading</td>
<td>ad No 155, 2000</td>
</tr>
</tbody>
</table>

---

**Privacy Act 1988**

Compilation No. 78

Compilation date: 1/7/18

Registered: 30/7/18
### Endnotes

#### Endnote 4—Amendment history

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>s 13..................</td>
<td>am No 116, 1990; Nos 20 and 194, 1991; No 28, 1993; No 155, 2000; No 131, 2009; No 73, 2010; No 60, 2011</td>
</tr>
<tr>
<td></td>
<td>rs No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>am No 12, 2017</td>
</tr>
<tr>
<td>s 13A................</td>
<td>ad No 155, 2000; No 60, 2011</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 13B................</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>am No 197, 2012</td>
</tr>
<tr>
<td>s 13C................</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>am No 197, 2012</td>
</tr>
<tr>
<td>s 13D................</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>am No 197, 2012</td>
</tr>
<tr>
<td>s 13E................</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>rs No 197, 2012</td>
</tr>
<tr>
<td>s 13F................</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>rs No 197, 2012</td>
</tr>
<tr>
<td>s 13G................</td>
<td>ad No 197, 2012</td>
</tr>
</tbody>
</table>

#### Division 2

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Division 2 heading</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>rs No 197, 2012</td>
</tr>
<tr>
<td>Division 2..........</td>
<td>rs No 197, 2012</td>
</tr>
<tr>
<td>s 14................</td>
<td>rs No 197, 2012</td>
</tr>
<tr>
<td>s 15................</td>
<td>am No 139, 2010</td>
</tr>
<tr>
<td></td>
<td>rs No 197, 2012</td>
</tr>
<tr>
<td>s 15B..............</td>
<td>ad No 139, 2010</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 16................</td>
<td>rs No 197, 2012</td>
</tr>
<tr>
<td>s 16A..............</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>rs No 197, 2012</td>
</tr>
<tr>
<td>s 16B..............</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>rs No 197, 2012</td>
</tr>
</tbody>
</table>

---

*Privacy Act 1988*

Compilation No. 78  
Compilation date: 1/7/18  
Registered: 30/7/18

Authorised Version C2018C00292 registered 30/07/2018
Endnotes

Endnote 4—Amendment history

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>s 16C..................</td>
<td>am No 157, 2015</td>
</tr>
<tr>
<td></td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>rs No 197, 2012</td>
</tr>
<tr>
<td>Division 3 .........</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 16D–16F ...........</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
</tbody>
</table>

Division 4

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Division 4 heading</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td>s 17 ................</td>
<td>am No 116, 1990; No 145, 2010; No 5, 2011</td>
</tr>
<tr>
<td></td>
<td>rs No 197, 2012</td>
</tr>
<tr>
<td>s 18 ................</td>
<td>am No 197, 2012</td>
</tr>
<tr>
<td>Division 5 heading</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>Division 5 ..........</td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 18A ...............</td>
<td>ad No 116, 1990</td>
</tr>
<tr>
<td></td>
<td>am No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 18B ...............</td>
<td>ad No 116, 1990</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>Part IIIA ..........</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 18BA ..............</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 18BAA ............</td>
<td>ad No 49, 2004</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 18BB–18BI ..........</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
</tbody>
</table>

Part IIIA

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part IIIA ..........</td>
<td>ad No 116, 1990</td>
</tr>
<tr>
<td></td>
<td>rs No 197, 2012</td>
</tr>
</tbody>
</table>

Privacy Act 1988

Compilation No. 78
Compilation date: 1/7/18
Registered: 30/7/18

Authorised Version C2018C00292 registered 30/07/2018
### Endnote 4—Amendment history

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Division 1</strong></td>
<td></td>
</tr>
<tr>
<td>s 18C, 18D</td>
<td>ad No 116, 1990</td>
</tr>
<tr>
<td></td>
<td>am No 24, 2001</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 18E, 18F</td>
<td>ad No 116, 1990</td>
</tr>
<tr>
<td></td>
<td>am No 143, 1992; No 34, 1997</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 18G</td>
<td>ad No 116, 1990</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 18H</td>
<td>ad No 116, 1990</td>
</tr>
<tr>
<td></td>
<td>am No 136, 1991</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 18J</td>
<td>ad No 116, 1990</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 18K</td>
<td>ad No 116, 1990</td>
</tr>
<tr>
<td></td>
<td>am No 136, 1991; No 143, 1992; No 24, 2001; No 125, 2002; No 135, 2001; No 86, 2006; No 24, 2012</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 18L</td>
<td>ad No 116, 1990</td>
</tr>
<tr>
<td></td>
<td>am No 136, 1991; No 143, 1992; No 24, 2001</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 18M</td>
<td>ad No 116, 1990</td>
</tr>
<tr>
<td></td>
<td>rs No 136, 1991</td>
</tr>
<tr>
<td></td>
<td>am No 143, 1992</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 18N</td>
<td>ad No 116, 1990</td>
</tr>
<tr>
<td></td>
<td>am No 136, 1991; No 143, 1992; No 13, 1994; No 24, 2001</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 18NA</td>
<td>ad No 34, 1997</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 18P</td>
<td>ad No 116, 1990</td>
</tr>
</tbody>
</table>
Endnotes

Endnote 4—Amendment history

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>s 18Q</td>
<td>am No 136, 1991; No 143, 1992</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 18R, 18S</td>
<td>ad No 116, 1990</td>
</tr>
<tr>
<td></td>
<td>am No 136, 1991; No 143, 1992; No 24, 2001</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 18T, 18U</td>
<td>ad No 116, 1990</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 18V</td>
<td>ad No 116, 1990</td>
</tr>
<tr>
<td></td>
<td>am No 136, 1991</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 19</td>
<td>ad No 2, 2000</td>
</tr>
<tr>
<td></td>
<td>rep No 51, 2010</td>
</tr>
<tr>
<td></td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>ad No 13, 2013</td>
</tr>
<tr>
<td>s 19</td>
<td>am No 59, 1995</td>
</tr>
<tr>
<td>renum s 19A</td>
<td>No 2, 2000</td>
</tr>
<tr>
<td>s 19A</td>
<td>rep No 51, 2010</td>
</tr>
</tbody>
</table>

Division 2

Subdivision A

| s 20               | am No 159, 2001 |
|                    | rep No 51, 2010 |
|                    | ad No 197, 2012 |

Subdivision B

| s 20B              | ad No 197, 2012 |

Subdivision C

| s 20C              | ad No 197, 2012 |
| s 20D              | ad No 197, 2012 |

Privacy Act 1988

Compilation No. 78  Compilation date: 1/7/18  Registered: 30/7/18
## Endnote 4—Amendment history

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Subdivision D</strong></td>
<td></td>
</tr>
<tr>
<td>s 20E</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 20F</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 20G</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 20H</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 20J</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 20K</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 20L</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 20M</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Subdivision E</strong></td>
<td></td>
</tr>
<tr>
<td>s 20N</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 20P</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 20Q</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Subdivision F</strong></td>
<td></td>
</tr>
<tr>
<td>s 20R</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 20S</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 20T</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 20U</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Subdivision G</strong></td>
<td></td>
</tr>
<tr>
<td>s 20V</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 20W</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 20X</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 20Y</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 20Z</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 20ZA</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Division 3</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Subdivision A</strong></td>
<td></td>
</tr>
<tr>
<td>s 21</td>
<td>am No 59, 1995</td>
</tr>
<tr>
<td></td>
<td>rep No 51, 2010</td>
</tr>
<tr>
<td></td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 21A</td>
<td>ad No 197, 2012</td>
</tr>
</tbody>
</table>

Privacy Act 1988

Compilation No. 78
Compilation date: 1/7/18
Registered: 30/7/18

Authorised Version C2018C00292 registered 30/07/2018
## Endnotes

### Endnote 4—Amendment history

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Subdivision B</strong></td>
<td></td>
</tr>
<tr>
<td>s 21B</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Subdivision C</strong></td>
<td></td>
</tr>
<tr>
<td>s 21C</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 21D</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 21E</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 21F</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Subdivision D</strong></td>
<td></td>
</tr>
<tr>
<td>s 21G</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 21H</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 21J</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 21K</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 21L</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 21M</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 21N</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 21NA</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 21P</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Subdivision E</strong></td>
<td></td>
</tr>
<tr>
<td>s 21Q</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 21R</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 21S</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Subdivision F</strong></td>
<td></td>
</tr>
<tr>
<td>s 21T</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 21U</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 21V</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 21W</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Division 4</strong></td>
<td></td>
</tr>
<tr>
<td>s 22</td>
<td>rs No 122, 1991</td>
</tr>
<tr>
<td></td>
<td>am No 146, 1999</td>
</tr>
<tr>
<td></td>
<td>rep No 51, 2010</td>
</tr>
<tr>
<td></td>
<td>ad No 197, 2012</td>
</tr>
</tbody>
</table>
## Endnotes

### Endnote 4—Amendment history

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Subdivision A</strong></td>
<td></td>
</tr>
<tr>
<td>s 22A</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Subdivision B</strong></td>
<td></td>
</tr>
<tr>
<td>s 22B</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 22C</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 22D</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 22E</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 22F</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Division 5</strong></td>
<td></td>
</tr>
<tr>
<td>s 23</td>
<td>rep No 51, 2010</td>
</tr>
<tr>
<td></td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 23A</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 23B</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 23C</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Division 6</strong></td>
<td></td>
</tr>
<tr>
<td>s 24</td>
<td>rep No 51, 2010</td>
</tr>
<tr>
<td></td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 24A</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Division 7</strong></td>
<td></td>
</tr>
<tr>
<td>s 25</td>
<td>am No 122, 1991</td>
</tr>
<tr>
<td></td>
<td>rep No 51, 2010</td>
</tr>
<tr>
<td></td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>am No 13, 2013; No 124, 2017</td>
</tr>
<tr>
<td>s 25A</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>am No 13, 2013; No 124, 2017</td>
</tr>
<tr>
<td><strong>Part III B</strong></td>
<td></td>
</tr>
<tr>
<td>Part III B</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Division 1</strong></td>
<td></td>
</tr>
<tr>
<td>s 26</td>
<td>rep No 51, 2010</td>
</tr>
<tr>
<td></td>
<td>ad No 197, 2012</td>
</tr>
</tbody>
</table>

---

*Privacy Act 1988*

Compilation No. 78  
Compilation date: 1/7/18  
Registered: 30/7/18
### Endnotes

#### Endnote 4—Amendment history

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Division 2</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Subdivision A</strong></td>
<td></td>
</tr>
<tr>
<td>s 26A</td>
<td>ad No 2, 2000</td>
</tr>
<tr>
<td></td>
<td>am No 146, 1999</td>
</tr>
<tr>
<td></td>
<td>rep No 51, 2010</td>
</tr>
<tr>
<td></td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 26B</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>am No 126, 2015</td>
</tr>
<tr>
<td>s 26C</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 26D</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Subdivision B</strong></td>
<td></td>
</tr>
<tr>
<td>s 26E</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 26F</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 26G</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 26H</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Subdivision C</strong></td>
<td></td>
</tr>
<tr>
<td>s 26J</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 26K</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Division 3</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Subdivision A</strong></td>
<td></td>
</tr>
<tr>
<td>s 26L</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 26M</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>am No 126, 2015</td>
</tr>
<tr>
<td>s 26N</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Subdivision B</strong></td>
<td></td>
</tr>
<tr>
<td>s 26P</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 26Q</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 26R</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 26S</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Subdivision C</strong></td>
<td></td>
</tr>
<tr>
<td>s 26T</td>
<td>ad No 197, 2012</td>
</tr>
</tbody>
</table>

358  

*Privacy Act 1988*

Compilation No. 78  
Compilation date: 1/7/18  
Registered: 30/7/18
## Endnotes

### Endnote 4—Amendment history

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Division 4</strong></td>
<td></td>
</tr>
<tr>
<td>s 26U..</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 26V..</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 26W..</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Part IIIIC</strong></td>
<td></td>
</tr>
<tr>
<td>Part IIIIC..</td>
<td>ad No 12, 2017</td>
</tr>
<tr>
<td><strong>Division 1</strong></td>
<td></td>
</tr>
<tr>
<td>s 26WA..</td>
<td>ad No 12, 2017</td>
</tr>
<tr>
<td>s 26WB..</td>
<td>ad No 12, 2017</td>
</tr>
<tr>
<td>s 26WC..</td>
<td>ad No 12, 2017</td>
</tr>
<tr>
<td>s 26WD..</td>
<td>ad No 12, 2017</td>
</tr>
<tr>
<td><strong>Division 2</strong></td>
<td></td>
</tr>
<tr>
<td>s 26WE..</td>
<td>ad No 12, 2017</td>
</tr>
<tr>
<td>s 26WF..</td>
<td>ad No 12, 2017</td>
</tr>
<tr>
<td>s 26WG..</td>
<td>ad No 12, 2017</td>
</tr>
<tr>
<td><strong>Division 3</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Subdivision A</strong></td>
<td></td>
</tr>
<tr>
<td>s 26WH..</td>
<td>ad No 12, 2017</td>
</tr>
<tr>
<td>s 26WJ..</td>
<td>ad No 12, 2017</td>
</tr>
<tr>
<td><strong>Subdivision B</strong></td>
<td></td>
</tr>
<tr>
<td>s 26WK..</td>
<td>ad No 12, 2017</td>
</tr>
<tr>
<td>s 26WL..</td>
<td>ad No 12, 2017</td>
</tr>
<tr>
<td>s 26WM..</td>
<td>ad No 12, 2017</td>
</tr>
<tr>
<td>s 26WN..</td>
<td>ad No 12, 2017</td>
</tr>
<tr>
<td>s 26WP..</td>
<td>ad No 12, 2017</td>
</tr>
<tr>
<td>s 26WQ..</td>
<td>ad No 12, 2017</td>
</tr>
<tr>
<td></td>
<td>am No 25, 2018</td>
</tr>
<tr>
<td><strong>Subdivision C</strong></td>
<td></td>
</tr>
<tr>
<td>s 26WR..</td>
<td>ad No 12, 2017</td>
</tr>
<tr>
<td></td>
<td>am No 25, 2018</td>
</tr>
<tr>
<td>s 26WS..</td>
<td>ad No 12, 2017</td>
</tr>
</tbody>
</table>
## Endnotes

### Endnote 4—Amendment history

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>s 26WT</td>
<td>ad No 12, 2017</td>
</tr>
<tr>
<td>Part IV</td>
<td></td>
</tr>
<tr>
<td>Part IV heading</td>
<td>rs No 2, 2000; No 51, 2010</td>
</tr>
<tr>
<td>Division heading</td>
<td>rs No 2, 2000</td>
</tr>
<tr>
<td></td>
<td>rep No 51, 2010</td>
</tr>
<tr>
<td>Division 1</td>
<td>rep No 51, 2010</td>
</tr>
<tr>
<td>Division 2</td>
<td></td>
</tr>
<tr>
<td>s 27</td>
<td>am No 20, 1991; No 28, 1993; No 155, 2000; No 49, 2004; No 139, 2010</td>
</tr>
<tr>
<td></td>
<td>rs No 197, 2012</td>
</tr>
<tr>
<td>s 27A</td>
<td>ad No 73, 2010</td>
</tr>
<tr>
<td></td>
<td>am No 73, 2010</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 28</td>
<td>am No 116, 1990; No 131, 2009; No 73, 2010</td>
</tr>
<tr>
<td></td>
<td>rs No 197, 2012</td>
</tr>
<tr>
<td>s 28A</td>
<td>ad No 116, 1990</td>
</tr>
<tr>
<td></td>
<td>am No 131, 2009; No 73, 2010</td>
</tr>
<tr>
<td></td>
<td>rs No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>am No 59, 2015</td>
</tr>
<tr>
<td>s 28B</td>
<td>ad No 131, 2009</td>
</tr>
<tr>
<td></td>
<td>am No 73, 2010</td>
</tr>
<tr>
<td></td>
<td>rs No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>am No 59, 2015</td>
</tr>
<tr>
<td>s 29</td>
<td>am No 116, 1990; No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>rs No 197, 2012</td>
</tr>
<tr>
<td>Division 3</td>
<td></td>
</tr>
<tr>
<td>s 30</td>
<td>am No 116, 1990; No 155, 2000; No 139, 2010; No 197, 2012; No 59, 2015</td>
</tr>
<tr>
<td>s 31</td>
<td>am No 20, 1991; No 155, 2000; No 51, 2010; No 197, 2012</td>
</tr>
<tr>
<td>s 32</td>
<td>am No 116, 1990 (as am by No 165, 1992); No 20, 1991; No 49, 2004 (as am by No 9, 2006); No 51, 2010; No 197, 2012</td>
</tr>
</tbody>
</table>

360 Privacy Act 1988

Compilation No. 78

Compilation date: 1/7/18  
Registered: 30/7/18

Authorised Version C2018C00292 registered 30/07/2018
### Endnotes

#### Endnote 4—Amendment history

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>s 33</td>
<td>am No 92, 1994; No 139, 2010</td>
</tr>
<tr>
<td>s 33B</td>
<td>ad No 139, 2010</td>
</tr>
<tr>
<td></td>
<td>rep No 59, 2015</td>
</tr>
<tr>
<td><strong>Division 3A</strong></td>
<td></td>
</tr>
<tr>
<td>Division 3A</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 33C</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 33D</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Division 3B</strong></td>
<td></td>
</tr>
<tr>
<td>Division 3B</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>rep No 124, 2017</td>
</tr>
<tr>
<td>s 33E</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>rep No 124, 2017</td>
</tr>
<tr>
<td>s 33F</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>am No 13, 2013</td>
</tr>
<tr>
<td></td>
<td>rep No 124, 2017</td>
</tr>
<tr>
<td><strong>Division 4</strong></td>
<td></td>
</tr>
<tr>
<td>s 34</td>
<td>am Nos 51 and 139, 2010; No 177 and 197, 2012; No 59, 2015</td>
</tr>
<tr>
<td>s 35A</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Part V</strong></td>
<td></td>
</tr>
<tr>
<td>Part V heading</td>
<td>rs No 197, 2012</td>
</tr>
<tr>
<td><strong>Division 1A</strong></td>
<td></td>
</tr>
<tr>
<td>Division 1A</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 36A</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td><strong>Division 1</strong></td>
<td></td>
</tr>
<tr>
<td>s 36</td>
<td>am No 11, 1990; No 13, 1994; Nos 2 and 155, 2000; No 51, 2010; No 197, 2012</td>
</tr>
<tr>
<td>s 37</td>
<td>am No 92, 1994; No 177, 1994; No 82, 1997; No 155, 2000; No 139, 2010; No 197, 2012; No 59, 2015; No 24, 2016; No 92, 2017</td>
</tr>
<tr>
<td>s 38</td>
<td>rs No 13, 1994</td>
</tr>
<tr>
<td></td>
<td>am No 155, 2000; No 197, 2012</td>
</tr>
<tr>
<td>s 38A</td>
<td>ad No 13, 1994</td>
</tr>
</tbody>
</table>
### Endnote 4—Amendment history

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>s 38B.........................</td>
<td>ad No 13, 1994</td>
</tr>
<tr>
<td></td>
<td>am No 197, 2012</td>
</tr>
<tr>
<td>s 38C.........................</td>
<td>ad No 13, 1994</td>
</tr>
<tr>
<td>s 39.........................</td>
<td>rs No 13, 1994</td>
</tr>
<tr>
<td>s 40.........................</td>
<td>am No 155, 2000; No 197, 2012</td>
</tr>
<tr>
<td>s 40A.........................</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>rs No 197, 2012</td>
</tr>
<tr>
<td>s 41.........................</td>
<td>am No 155, 2000; No 49, 2004; No 197, 2012</td>
</tr>
<tr>
<td>s 42.........................</td>
<td>am No 155, 2000; No 197, 2012</td>
</tr>
<tr>
<td>s 43.........................</td>
<td>am No 155, 2000; No 139, 2010; No 197, 2012; No 59, 2015</td>
</tr>
<tr>
<td>s 43A.........................</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 44.........................</td>
<td>am No 34, 1997; No 197, 2012</td>
</tr>
<tr>
<td>s 46.........................</td>
<td>am No 155, 2000; No 24, 2001; No 197, 2012; No 4, 2016; No 61, 2016</td>
</tr>
<tr>
<td>s 48.........................</td>
<td>am No 155, 2000</td>
</tr>
<tr>
<td>s 49.........................</td>
<td>am No 116, 1990; No 24, 2001; No 73, 2010; No 60, 2011; No 197, 2012</td>
</tr>
<tr>
<td>s 49A.........................</td>
<td>ad No 131, 2009</td>
</tr>
<tr>
<td>s 50.........................</td>
<td>am No 146, 1999; No 25, 2006 (as am by No 73, 2008); No 70, 2009; No 139, 2010; No 11, 2011; No 197, 2012 (as am by No 5, 2015); No 2, 2013; No 5, 2015; No 59, 2015</td>
</tr>
<tr>
<td>s 50A.........................</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>am No 197, 2012</td>
</tr>
</tbody>
</table>

#### Division 2

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>s 52.........................</td>
<td>am No 116, 1990; No 13, 1994; No 155, 2000; No 197, 2012</td>
</tr>
<tr>
<td>s 53.........................</td>
<td>rs No 13, 1994</td>
</tr>
<tr>
<td>s 53A.........................</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td>s 53B.........................</td>
<td>am No 197, 2012</td>
</tr>
</tbody>
</table>

#### Division 3

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Division 3 heading..................</td>
<td>rs No 155, 2000</td>
</tr>
</tbody>
</table>

---

**Privacy Act 1988**

Compilation No. 78

Compilation date: 1/7/18

Registered: 30/7/18
### Provision affected | How affected
--- | ---
Division 3 | rs No 13, 1994; No 59, 1995
s 54 | rs No 13, 1994
| am No 177, 1994
| rs No 59, 1995
| am No 82, 1997; No 155, 2000; No 9, 2006; No 197, 2012; No 92, 2017
s 55 | rs No 13, 1994; No 59, 1995; No 155, 2000; No 197, 2012
s 55A | ad No 155, 2000
| am No 197, 2012; No 13, 2013
s 55B | ad No 155, 2000
| am No 197, 2012
s 56 | rs No 13, 1994
| rep No 59, 1995

### Division 4

Division 4 heading | am No 116, 1990
| rs No 13, 1994
Division 4 | rs No 13, 1994
s 57 | rs No 13, 1994
| am No 177, 1994; No 82, 1997; No 197, 2012; No 92, 2017
s 58 | rs No 13, 1994; No 197, 2012
s 59 | rs No 13, 1994
| am No 197, 2012
s 60 | am No 116, 1990
| rs No 13, 1994
| am No 139, 2010; No 197, 2012
s 61 | rs No 13, 1994
| am No 38, 2005
| rep No 197, 2012
s 62 | rs No 13, 1994
| am No 155, 2000; No 197, 2012; No 13, 2013

### Division 5
### Endnotes

#### Endnote 4—Amendment history

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>s 63</td>
<td>rs No 13, 1994</td>
</tr>
<tr>
<td></td>
<td>am No 59, 1995; No 155, 2000; No 197, 2012; No 13, 2013</td>
</tr>
<tr>
<td>s 64</td>
<td>am No 155, 2000; No 197, 2012</td>
</tr>
<tr>
<td>s 65</td>
<td>am No 24, 2001; No 61, 2016</td>
</tr>
<tr>
<td>s 66</td>
<td>am No 155, 2000; No 24, 2001; No 139, 2010; No 59, 2015; No 61, 2016</td>
</tr>
<tr>
<td>s 67</td>
<td>am No 155, 2000; No 197, 2012</td>
</tr>
<tr>
<td>s 68</td>
<td>am No 116, 1990; No 155, 2000; No 139, 2010; No 197, 2012; No 59, 2015</td>
</tr>
<tr>
<td>s 68A</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td>s 69</td>
<td>am No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 70</td>
<td>am No 125, 2002; No 86, 2006; No 139, 2010; No 59, 2015</td>
</tr>
<tr>
<td>s 70A</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 70B</td>
<td>ad No 155, 2000</td>
</tr>
</tbody>
</table>

#### Part VI

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part VI heading</td>
<td>rs No 155, 2000</td>
</tr>
</tbody>
</table>

#### Division 1

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Division 1 heading</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td>s 72</td>
<td>am No 155, 2000; No 197, 2012</td>
</tr>
<tr>
<td>s 73</td>
<td>am No 155, 2000; No 50, 2006; No 197, 2012</td>
</tr>
<tr>
<td>s 74</td>
<td>am No 197, 2012</td>
</tr>
<tr>
<td>s 75</td>
<td>am No 155, 2000; No 197, 2012</td>
</tr>
<tr>
<td>s 76</td>
<td>am No 155, 2000</td>
</tr>
<tr>
<td>s 77</td>
<td>am No 155, 2000</td>
</tr>
<tr>
<td>s 79</td>
<td>am No 155, 2000; No 197, 2012</td>
</tr>
<tr>
<td>s 80</td>
<td>am No 5, 2011</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
</tbody>
</table>

#### Division 2

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Division 2 heading</td>
<td>ad No 155, 2000</td>
</tr>
</tbody>
</table>
### Endnote 4—Amendment history

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>s 80A....................</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>am No 197, 2012</td>
</tr>
<tr>
<td>s 80B....................</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>am No 197, 2012</td>
</tr>
<tr>
<td>s 80C....................</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 80D....................</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td></td>
<td>am No 197, 2012</td>
</tr>
<tr>
<td><strong>Division 3</strong></td>
<td></td>
</tr>
<tr>
<td>Division 3 heading</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td>s 80E....................</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td><strong>Part VIA</strong></td>
<td></td>
</tr>
<tr>
<td>Part VIA..................</td>
<td>ad No 148, 2006</td>
</tr>
<tr>
<td><strong>Division 1</strong></td>
<td></td>
</tr>
<tr>
<td>s 80F....................</td>
<td>ad No 148, 2006</td>
</tr>
<tr>
<td>s 80G....................</td>
<td>ad No 148, 2006</td>
</tr>
<tr>
<td></td>
<td>am No 139, 2010; No 46, 2011</td>
</tr>
<tr>
<td>s 80H....................</td>
<td>ad No 148, 2006</td>
</tr>
<tr>
<td></td>
<td>am No 197, 2012</td>
</tr>
<tr>
<td><strong>Division 2</strong></td>
<td></td>
</tr>
<tr>
<td>ss 80J, 80K............</td>
<td>ad No 148, 2006</td>
</tr>
<tr>
<td>s 80L....................</td>
<td>ad No 148, 2006</td>
</tr>
<tr>
<td></td>
<td>am No 8, 2010</td>
</tr>
<tr>
<td>ss 80M, 80N............</td>
<td>ad No 148, 2006</td>
</tr>
<tr>
<td><strong>Division 3</strong></td>
<td></td>
</tr>
<tr>
<td>s 80P....................</td>
<td>ad No 148, 2006</td>
</tr>
<tr>
<td></td>
<td>am No 197, 2012; No 108, 2014</td>
</tr>
<tr>
<td><strong>Division 4</strong></td>
<td></td>
</tr>
<tr>
<td>s 80Q....................</td>
<td>ad No 148, 2006</td>
</tr>
<tr>
<td></td>
<td>am No 197, 2012</td>
</tr>
<tr>
<td>s 80R....................</td>
<td>ad No 148, 2006</td>
</tr>
</tbody>
</table>
### Endnote 4—Amendment history

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>ss 80S, 80T</td>
<td>ad No 148, 2006</td>
</tr>
<tr>
<td>Part VIB</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>rs No 124, 2017</td>
</tr>
<tr>
<td>Division 1</td>
<td></td>
</tr>
<tr>
<td>s 80U</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>rs No 124, 2017</td>
</tr>
<tr>
<td>s 80V</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>rs No 124, 2017</td>
</tr>
<tr>
<td>Division 2</td>
<td></td>
</tr>
<tr>
<td>s 80W</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>am No 13, 2013</td>
</tr>
<tr>
<td></td>
<td>rs No 124, 2017</td>
</tr>
<tr>
<td>s 80X</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>rep No 124, 2017</td>
</tr>
<tr>
<td>s 80Y</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>rep No 124, 2017</td>
</tr>
<tr>
<td>s 80Z</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>am No 13, 2013</td>
</tr>
<tr>
<td></td>
<td>rep No 124, 2017</td>
</tr>
<tr>
<td>s 80ZA</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>am No 13, 2013</td>
</tr>
<tr>
<td></td>
<td>rep No 124, 2017</td>
</tr>
<tr>
<td>s 80ZB</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>am No 13, 2013</td>
</tr>
<tr>
<td></td>
<td>rep No 124, 2017</td>
</tr>
<tr>
<td>s 80ZC</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>rep No 124, 2017</td>
</tr>
<tr>
<td>Division 3</td>
<td></td>
</tr>
<tr>
<td>s 80ZD</td>
<td>ad No 197, 2012</td>
</tr>
</tbody>
</table>
### Endnote 4—Amendment history

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>s 80ZE</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>rep No 124, 2017</td>
</tr>
<tr>
<td>s 80ZF</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>rep No 124, 2017</td>
</tr>
<tr>
<td>s 80ZG</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td></td>
<td>rep No 124, 2017</td>
</tr>
</tbody>
</table>

#### Part VII
- s 82: am No 159, 2001; No 197, 2012
- s 83: am No 2, 2000; No 197, 2012

#### Part VIII
- s 89: am No 139, 2010

#### Part IX
- s 95: am No 50, 2006; No 197, 2012
- s 95A: ad No 155, 2000
- s 95AA: ad No 99, 2006
- s 95B: ad No 155, 2000
- s 95C: ad No 155, 2000
- s 96: am No 2, 2000
- s 97: am No 155, 2000
- s 98: am No 155, 2000; No 13, 2013

---

**Privacy Act 1988**

Compilation No. 78  
Compilation date: 1/7/18  
Registered: 30/7/18
Endnotes

Endnote 4—Amendment history

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>s 98A</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 98B</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 98C</td>
<td>ad No 197, 2012</td>
</tr>
<tr>
<td>s 99</td>
<td>am No 11, 1990; No 2, 2000; rep No 51, 2010</td>
</tr>
<tr>
<td>s 99A</td>
<td>ad No 116, 1990; am No 155, 2000; No 24, 2001; No 4, 2010; No 197, 2012; No 124, 2017</td>
</tr>
<tr>
<td>s 100</td>
<td>am No 155, 2000; No 49, 2004; No 197, 2012</td>
</tr>
<tr>
<td>Part X</td>
<td>rep No 197, 2012</td>
</tr>
<tr>
<td>s 101</td>
<td>rep No 197, 2012</td>
</tr>
</tbody>
</table>

Schedule 1

Schedule 1 rs No 197, 2012

Part 1

c 1 ad No 197, 2012

c 2 ad No 197, 2012

Part 2

c 3 ad No 197, 2012

c 4 ad No 197, 2012

c 5 ad No 197, 2012

Part 3

c 6 ad No 197, 2012

c 7 ad No 197, 2012

c 8 ad No 197, 2012

c 9 ad No 197, 2012

Part 4

c 10 ad No 197, 2012

c 11 ad No 197, 2012

Part 5

c 12 ad No 197, 2012

c 13 ad No 197, 2012

368 Privacy Act 1988

Compilation No. 78
Compilation date: 1/7/18
Registered: 30/7/18

Authorised Version C2018C00292 registered 30/07/2018
## Endnotes

**Endnote 4—Amendment history**

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule 2</td>
<td>rep No 145, 2010</td>
</tr>
<tr>
<td>Introduction</td>
<td>am No 51, 2010</td>
</tr>
<tr>
<td>c 1–5</td>
<td>rep No 145, 2010</td>
</tr>
<tr>
<td>c 6</td>
<td>am No 51, 2010</td>
</tr>
<tr>
<td>c 7</td>
<td>rep No 145, 2010</td>
</tr>
<tr>
<td>Schedule 3</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td>c 1</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td>c 2</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td>c 3–6</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td>c 7</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td>c 8, 9</td>
<td>ad No 155, 2000</td>
</tr>
<tr>
<td>c 10</td>
<td>ad No 155, 2000</td>
</tr>
</tbody>
</table>

---

*Privacy Act 1988*

Compilation No. 78  
Compilation date: 1/7/18  
Registered: 30/7/18
Australian Privacy Principles guidelines

Privacy Act 1988
The Office of the Australian Information Commissioner (OAIC) was established on 1 November 2010 by the *Australian Information Commissioner Act 2010*.

All OAIC publications can be made available in a range of accessible formats for people with disabilities. If you require assistance, please contact the OAIC.

Date of initial publication: February 2014, revised 1 March 2014 and 31 March 2015.

**Creative Commons**

[Image: Creative Commons logo]

With the exception of the Commonwealth Coat of Arms, and to the extent that copyright subsists in a third party, these guidelines, its logo and front page design are licensed under a Creative Commons Attribution 3.0 Australia licence [http://creativecommons.org/licenses/by/3.0/au/](http://creativecommons.org/licenses/by/3.0/au/)

To the extent that copyright subsists in third party quotes it remains with the original owner and permission may be required to reuse the material.

Content from these guidelines should be attributed as: Office of the Australian Information Commissioner, Australian Privacy Principles guidelines.

Enquiries regarding the licence and use of the guidelines are welcome at:

Office of the Australian Information Commissioner  
GPO Box 2999 Canberra ACT 2601  
Telephone: 02 9284 9800  
TTY: 1800 620 241 (no voice calls)  
Email: enquiries@oaic.gov.au  
Web: [www.oaic.gov.au](http://www.oaic.gov.au)
Preface

The Privacy Act 1988 (Privacy Act) s 28(1)(a) provides that the Australian Information Commissioner may make guidelines for the ‘avoidance of acts or practices that may or might be interferences with the privacy of individuals, or which may otherwise have any adverse effects on the privacy of individuals’. Additionally, s 28(1)(c)(i) provides that one of the functions of the Commissioner is to promote an understanding and acceptance of the Australian Privacy Principles (APPs) and the objects of those principles.

The Australian Privacy Principles guidelines (APP guidelines) outline:

- the mandatory requirements in the APPs, which are set out in Schedule 1 of the Privacy Act
- the Information Commissioner’s interpretation of the APPs, including the matters that the Office of the Australian Information Commissioner may take into account when exercising functions and powers relating to the APPs
- examples that explain how the APPs may apply to particular circumstances
- good privacy practice to supplement minimum compliance with the mandatory requirements in the APPs.

The APP guidelines are not legally binding and do not constitute legal advice about how an entity should comply with the APPs in particular circumstances. An entity may wish to seek independent legal advice where appropriate.

The APP guidelines may be updated from time to time, including to take account of changes in the Privacy Act or other legislation, determinations made under s 52 of the Privacy Act and relevant tribunal and court decisions.

Prof. John McMillan
Australian Information Commissioner
Contents

General matters
   Chapter A: Introductory matters
   Chapter B: Key concepts
   Chapter C: Permitted general situations
   Chapter D: Permitted health situations

Part 1 — Consideration of personal information privacy
   Chapter 1: APP 1 — Open and transparent management of personal information
   Chapter 2: APP 2 — Anonymity and pseudonymity

Part 2 — Collection of personal information
   Chapter 3: APP 3 — Collection of solicited personal information
   Chapter 4: APP 4 — Dealing with unsolicited personal information
   Chapter 5: APP 5 — Notification of the collection of personal information

Part 3 — Dealing with personal information
   Chapter 6: APP 6 — Use or disclosure of personal information
   Chapter 7: APP 7 — Direct marketing
   Chapter 8: APP 8 — Cross-border disclosure of personal information
   Chapter 9: APP 9 — Adoption, use or disclosure of government related identifiers

Part 4 — Integrity of personal information
   Chapter 10: APP 10 — Quality of personal information
   Chapter 11: APP 11 — Security of personal information

Part 5 — Access to, and correction of, personal information
   Chapter 12: APP 12 — Access to personal information
   Chapter 13: APP 13 — Correction of personal information

A comprehensive contents page appears at the beginning of each Chapter of the APP guidelines.
Chapter A: Introductory matters

Version 1.1, March 2015

Purpose ........................................................................................................................................ 2
Australian Privacy Principles (APPs).......................................................................................... 2
Who is covered by the APPs? ...................................................................................................... 4
  Do the APPs apply to a contracted service provider under a Commonwealth contract? . 4
  Do the APPs apply to a credit reporting participant? ............................................................... 5
  Do the APPs apply to an APP entity bound by a registered APP Code? ............................... 5
Are APP entities responsible for acts and practices of, and disclosures to, staff? ................. 5
What happens if an APP entity breaches an APP? .................................................................... 5
References in the APP guidelines ............................................................................................... 6
Where do I get more information? ............................................................................................. 6
APP guidelines and Australian Capital Territory public sector agencies ............................... 6
Purpose

A.1 The Australian Information Commissioner\(^1\) issues these Australian Privacy Principles guidelines (APP guidelines) under s 28(1) of the *Privacy Act 1988* (Privacy Act).\(^2\) These guidelines are not a legislative instrument (s 28(4)).

A.2 The APP guidelines outline:

- the mandatory requirements in the Australian Privacy Principles (APPs), which are set out in Schedule 1 of the Privacy Act — generally indicated by ‘must’ or ‘is required to’
- the Information Commissioner’s interpretation of the APPs, including the matters that the Office of the Australian Information Commissioner (OAIC) may take into account when exercising functions and powers relating to the APPs — generally indicated by ‘should’ or ‘is expected to’
- examples that explain how the APPs may apply to particular circumstances — generally indicated by ‘for example’ or ‘examples include’. Any examples given are not intended to be prescriptive or exhaustive of how an entity may comply with the mandatory requirements in the APPs; the particular circumstances of an entity will also be relevant
- good privacy practice to supplement minimum compliance with the mandatory requirements in the APPs — generally indicated by ‘could’.

A.3 The APP guidelines are not legally binding and do not constitute legal advice about how an entity should comply with the APPs in particular circumstances. An entity may wish to seek independent legal advice where appropriate.

A.4 The APP guidelines may also provide relevant guidance for Australian Capital Territory (ACT) public sector agencies covered by the Territory Privacy Principles in the ACT *Information Privacy Act 2014* (see paragraphs A.29 – A.32 below).

Australian Privacy Principles (APPs)

A.5 The APP guidelines should be read together with the full text of the APPs in the Privacy Act.\(^3\)

A.6 The APPs are legally binding principles which are the cornerstone of the privacy protection framework in the Privacy Act.\(^4\) The APPs set out standards, rights and obligations in relation to handling, holding, accessing and correcting personal information. They apply

---

\(^1\) In the APP guidelines, where the Information Commissioner is referred to in a paragraph, all subsequent references to ‘the Commissioner’ within that paragraph also relate to the Information Commissioner.

\(^2\) Section 28(1) of the Privacy Act sets out the guidance related functions of the Information Commissioner, including ‘making guidelines for the avoidance of acts or practices that may or might be interferences with the privacy of individuals, or which may otherwise have any adverse effects on the privacy of individuals’.


\(^4\) Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 52.
to most Australian Government (and Norfolk Island Government) agencies and some private sector organisations — collectively referred to as APP entities (see paragraphs A.12–A.14).5

A.7 The APPs are principles-based law. This provides APP entities with the flexibility to tailor their personal information handling practices to their diverse needs and business models, and to the diverse needs of individuals.6 The APPs are also technology neutral, applying equally to paper-based and digital environments. This is intended to preserve their relevance and applicability, in a context of continually changing and emerging technologies.

A.8 The APPs are structured to reflect the personal information lifecycle. They are grouped into five parts:

- Part 1 — Consideration of personal information privacy (APPs 1 and 2)
- Part 2 — Collection of personal information (APPs 3, 4 and 5)
- Part 3 — Dealing with personal information (APPs 6, 7, 8 and 9)
- Part 4 — Integrity of personal information (APPs 10 and 11)
- Part 5 — Access to, and correction of, personal information (APPs 12 and 13).

A.9 The requirements in each of these principles interact with and complement each other. For example, when collecting personal information, an APP entity should consider the requirements in Part 2 as well as in Part 4 concerning the integrity of the information.

A.10 In developing the APP guidelines, the Information Commissioner has had regard to the objects of the Privacy Act, stated in s 2A:

- promoting the protection of the privacy of individuals
- recognising that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities
- providing the basis for nationally consistent regulation of privacy and the handling of personal information
- promoting responsible and transparent handling of personal information by entities
- facilitating an efficient credit reporting system while ensuring that the privacy of individuals is respected
- facilitating the free flow of information across national borders while ensuring that the privacy of individuals is respected
- providing a means for individuals to complain about an alleged interference with their privacy
- implementing Australia’s international obligation in relation to privacy.

A.11 The structure of the APP guidelines reflects the structure of the APPs: APPs 1 to 13 are each dealt with in separate chapters. The number of the chapter corresponds to the number of the APP. Chapters A to D contain guidance on general matters, including an

5 The APPs do not apply to Australian Capital Territory Government agencies. Rather, the IPPs continue to apply. The Privacy Act 1988, as in operation on 1 July 1994, continues to apply to ACT Government agencies pursuant to the Australian Capital Territory Government Service (Consequential Provisions) Act 1994.
6 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 52.
explanation of key concepts that are used throughout the APPs and the APP guidelines (Chapter B), and guidance on permitted general situations (Chapter C) and permitted health situations (Chapter D), which are also relevant to a number of APPs.

Who is covered by the APPs?

A.12 The APPs apply to APP entities (s 15). The term ‘APP entity’ means an agency or organisation (s 6(1)) and is discussed in more detail in Chapter B (Key concepts).

A.13 The APPs extend to an act or practice of an APP entity occurring outside Australia and the external Territories (s 5B). However, if the APP entity is an organisation, the organisation must also have an Australian link (s 5B(1A)). The term ‘Australian link’ is discussed in Chapter B (Key concepts).

A.14 In some circumstances, an act or practice of an APP entity is exempt from the Privacy Act, including the APPs. For example, an act done, or a practice engaged in by a Federal Court is exempt, except for acts or practices in respect of a matter of an administrative nature (s 7(1)(a)(ii) and (b)). The ‘employee records’ exemption (s 7B(3)) is an example of an exemption that applies to an act or practice of an organisation.

Do the APPs apply to a contracted service provider under a Commonwealth contract?

A.15 Special provisions apply to a contracted service provider (including a subcontractor) handling personal information under a Commonwealth contract. The term ‘contracted service provider’ is defined in s 6(1) and includes an organisation that is or was a party to a Commonwealth contract and that is or was responsible for providing services to an agency under that contract. The term also includes a sub-contractor for the contract. The term ‘Commonwealth contract’ is also defined in s 6(1) to mean a contract, to which the Commonwealth, Norfolk Island or an agency is or was a party, under which services are to be, or were to be, provided to an agency.

A.16 An agency entering into a Commonwealth contract must take contractual measures to ensure that the other party (the contracted service provider) does not do an act, or engage in a practice, that would breach an APP if done or engaged in by the agency (s 95B). In effect, s 95B ensures that the contracted service provider complies with the APPs as if it were an agency in respect of its activities under the contract. However, it is the contract that is the primary source of the contracted service provider’s privacy obligations in relation to its activities under the contract.

A.17 If a provision of a Commonwealth contract authorises an organisation that is a contracted service provider to do an act or practice that would otherwise breach the APPs, an act done or practice engaged in for the purposes of meeting that obligation will not breach the APPs (s 6A(2)). A contract may include such a provision where, for example, the APPs contain different requirements for agencies and organisations. An act done or practice engaged in by the contracted service provider that is contrary to or inconsistent with such a contractual provision, is an ‘interference with the privacy of an individual’ (s 13(3)) (see paragraph 4 below).
Do the APPs apply to a credit reporting participant?

A.18 Part IIIA of the Privacy Act contains requirements for the handling of credit-related personal information by credit reporting participants, including credit reporting bodies, credit providers and some other third party recipients of that information. The provisions in Pt IIIA make clear whether the obligations in Pt IIIA replace relevant APPs or apply in addition to relevant APPs.

A.19 The APPs will apply to any credit reporting participant that is an APP entity in relation to the handling of personal information not regulated by Pt IIIA.7

Do the APPs apply to an APP entity bound by a registered APP Code?

A.20 A ‘registered APP code’ is defined as an APP code that is included on the Codes Register and that is in force (s 26B(1)). A registered APP code does not replace the APPs for the entities which it binds, but operates in addition to the requirements of the APPs.8 Therefore, an APP entity that is bound by an APP code must comply with both the APPs and the APP code.

A.21 Registered APP codes are discussed in more detail in Chapter B (Key concepts).

Are APP entities responsible for acts and practices of, and disclosures to, staff?

A.22 An act done or practice engaged in by a person in one of the following categories is taken to be an act done or practice engaged in by the APP entity:

• a person employed by, or in the service of an APP entity, in performing the duties of the person’s employment

• a person on behalf of an unincorporated body or other body that is established by or under a Commonwealth (or Norfolk Island) enactment, for the purpose of assisting or performing functions in connection with an APP entity

• a member, staff member or special member of the Australian Federal Police in performing duties as such a member (s 8(1)).

A.23 Information disclosed to a person or member in one of the preceding categories is also taken to be information disclosed to the APP entity.

What happens if an APP entity breaches an APP?

A.24 An act or practice of an APP entity that occurs on or after 12 March 2014 and that breaches an APP in relation to personal information about an individual, is ‘an interference with the privacy’ of the individual (s 13(1)).

A.25 The Information Commissioner has powers to investigate possible interferences with privacy, either following a complaint by the individual concerned or on the Commissioner’s own initiative (Part V of the Privacy Act). Where an individual makes a

8 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 199.
complaint, the Commissioner will generally attempt to conciliate the complaint (s 40A). The Commissioner also has a range of enforcement powers and other remedies available.

References in the APP guidelines

A.26 The APP guidelines distinguish between mandatory requirements under the APPs, the Information Commissioner’s interpretation of the APPs and good practice privacy guidance as discussed in paragraph A.2 above.

A.27 In the APP guidelines:
- a reference to a paragraph is to a paragraph of text in the same chapter of these guidelines
- a reference to a section of an Act is to a section of the Privacy Act or other Act as specified.

Where do I get more information?

A.28 The Office of the Australian Information Commissioner (OAIC) has developed a range of materials to assist APP entities to comply with the Privacy Act, and to provide information to individuals. These include guides, agency and business resources, fact sheets and frequently asked questions. The resources are available on the OAIC website, see <www.oaic.gov.au>.

APP guidelines and Australian Capital Territory public sector agencies

A.29 The ACT Information Privacy Act 2014 regulates how personal information is handled by ACT public sector agencies. The Information Privacy Act includes a set of Territory Privacy Principles (TPPs), which cover the collection, use, storage and disclosure of personal information, and an individual’s access to and correction of that information.

A.30 Under an arrangement between the ACT Government and the Australian Government, the Information Commissioner is exercising some of the functions of the ACT Information Privacy Commissioner. These responsibilities include handling privacy complaints against, and receiving data breach notifications from, ACT public sector agencies, and conducting assessments of ACT public sector agencies’ compliance with the Information Privacy Act.

A.31 The TPPs are substantially similar to the APPs. The main differences are:
- there is no TPP equivalent to APP 7 (direct marketing) or APP 9 (adoption, use or disclosure of government related identifiers)
- the TPPs and the Information Privacy Act do not cover personal health information or health records.

A.32 Given these similarities, the information, examples and good privacy practices outlined in the APP guidelines may assist the general public and ACT public sector agencies.

---

9 For more information about the TPPs, including how they differ from the APPs, see www.oaic.gov.au
to interpret and apply the TPPs. The guidelines should be read with reference to the full text of the TPPs and the Information Privacy Act.\textsuperscript{10}

Chapter B: Key concepts

Version 1.2, March 2015

APP entity .............................................................................................................................. 3
Australian Link ..................................................................................................................... 5
Carries on business in Australia ......................................................................................... 5
Carry on business ............................................................................................................... 5
In Australia ......................................................................................................................... 6
Personal information collected ‘in Australia’ ..................................................................... 7
Collects .................................................................................................................................. 7
Commonwealth record ....................................................................................................... 8
Consent ................................................................................................................................. 9
Express or implied consent ................................................................................................. 9
Voluntary ............................................................................................................................. 10
Bundled consent ................................................................................................................. 10
Informed ............................................................................................................................... 11
Current and specific .......................................................................................................... 11
Capacity ............................................................................................................................... 11
Children and young people .............................................................................................. 12
De-identification ................................................................................................................ 13
Disclosure ............................................................................................................................ 13
Enforcement body .............................................................................................................. 15
Enforcement related activities ............................................................................................ 16
Health information ............................................................................................................ 16
Health Service ................................................................................................................... 17
Holds ................................................................................................................................. 18
Immigration Department .................................................................................................... 19
Personal information ......................................................................................................... 19
Meaning of ‘reasonably identifiable’ ................................................................................ 20
Deceased persons ............................................................................................................. 21
Purpose ............................................................................................................................... 21
Primary purpose and secondary purpose ........................................................................ 21
Describing the primary purpose ....................................................................................... 22
Reasonable, Reasonably ................................................................................................. 22
<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reasonable steps</td>
<td>23</td>
</tr>
<tr>
<td>Reasonably believes</td>
<td>23</td>
</tr>
<tr>
<td>Reasonably necessary and necessary</td>
<td>24</td>
</tr>
<tr>
<td>Recognised external dispute resolution scheme</td>
<td>25</td>
</tr>
<tr>
<td>Registered APP code</td>
<td>25</td>
</tr>
<tr>
<td>Related body corporate</td>
<td>26</td>
</tr>
<tr>
<td>Required or authorised by or under an Australian law or a court/tribunal order</td>
<td>26</td>
</tr>
<tr>
<td>Meaning of ‘required’</td>
<td>26</td>
</tr>
<tr>
<td>Meaning of ‘authorised’</td>
<td>26</td>
</tr>
<tr>
<td>Meaning of ‘Australian law’</td>
<td>27</td>
</tr>
<tr>
<td>Meaning of ‘court/tribunal order’</td>
<td>27</td>
</tr>
<tr>
<td>Sensitive information</td>
<td>27</td>
</tr>
<tr>
<td>Use</td>
<td>28</td>
</tr>
</tbody>
</table>
B.1 This Chapter outlines some key words and phrases that are used in the Privacy Act and the Australian Privacy Principles (APPs).

**APP entity**

B.2 An ‘APP entity’ is defined to be an agency or organisation (s 6(1)).

B.3 An ‘organisation’ is defined to be:

- an individual (including a sole trader)
- a body corporate
- a partnership
- any other unincorporated association, or
- a trust
  unless it is a small business operator, registered political party, State or Territory authority or a prescribed instrumentality of a State (s 6C).

B.4 The following terms are also defined in the Privacy Act: ‘small business operator’ (s 6D), ‘registered political party’ (s 6(1)) and ‘State or Territory authority’ (s 6C).

B.5 In general, a small business operator is an individual (including a sole trader), body corporate, partnership, unincorporated association or trust that has an annual turnover of $3,000,000 or less for a financial year, unless an exception applies (s 6D). If an exception applies this kind of business may be an organisation. The exceptions include businesses that:

- provide a health service and hold health information other than in an employee record
- disclose personal information about another individual for a benefit, service or advantage, or provide a benefit, service or advantage to collect personal information about another individual from anyone else, unless they do so with the consent of the individual or are required or authorised by or under legislation to do so
- are contracted service providers for a Commonwealth contract (s 6D(4)).

B.6 Following are two examples of how the second exception may apply:

- An example of an entity that discloses personal information for a benefit, service or advantage is an entity that sells a list of personal information to another entity so that the other entity can use that information for the purpose of direct marketing.
- An example of an entity that provides a benefit, service or advantage to collect personal information is a lobby group that pays another entity to collect information about the political preferences of an individual.

B.7 A non-APP entity may be treated as an organisation (and therefore as an APP entity) in certain circumstances, for example, a small business operator that is related to an organisation covered by the Privacy Act (s 6D(9)) or an entity that chooses to be
treated as an organisation (s 6EA). Also, some small business operators are treated as organisations (and therefore an APP entity) in relation to the following activities they carry out:

- activities of reporting entities or authorised agents relating to the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* and its Regulations and Rules (s 6E(1A))
- certain acts and practices in connection with the operation of a residential tenancy database (s 6E(2)) and regulation 7 of Privacy Regulation 2013
- activities related to the conduct of a protection action ballot (s 6E(1)(B)).

B.8 ‘Agency’ refers to Australian Government (and Norfolk Island Government) agencies, but does not include State and Territory agencies. An ‘agency’ is defined to be:

- a Minister
- a Department
- a body (whether incorporated or not), or a tribunal, established or appointed for a public purpose by or under a Commonwealth enactment, not being:
  - an incorporated company, society or association; or
  - an organisation that is registered under the *Fair Work (Registered Organisations) Act 2009* or a branch of such an organisation
- a body established or appointed by the Governor-General, or by a Minister, other than by or under a Commonwealth enactment
- a person holding or performing the duties of an office established by or under, or an appointment made under, a Commonwealth enactment, other than a person who, by virtue of holding that office, is the Secretary of a Department
- a person holding or performing the duties of an appointment, being an appointment made by the Governor-General, or by a Minister, other than under a Commonwealth enactment
- a federal court
- the Australian Federal Police
- a Norfolk Island agency
- the nominated AGHS company
- an eligible hearing service provider, or

---

1 See also, s 6F which describes when a state instrumentality will be treated as an organisation.

2 The APPs do not apply to Australian Capital Territory Government agencies. Rather, the IPPs continue to apply. The Privacy Act 1988, as in operation on 1 July 1994, continues to apply to ACT Government agencies, being the date on which the *Australian Capital Territory Government Service (Consequential Provisions) Act 1994* commenced. Amendments to the Privacy Act made after that date do not apply to ACT agencies.

3 Nominated AGHS company means ‘a company that (a) is the nominated company (within the meaning of Part 2 of the *Hearing Services and AGHS Reform Act 1997*); and (b) is either (i) Commonwealth owned (within the meaning of that Part); or (ii) a corporation’ (s 6(1)).
• the service operator under the Healthcare Identifiers Act 2010 (s 6(1)).

B.9 Section 6(5) clarifies that a person shall not be taken to be an agency merely because the person is the holder of, or performs the duties of, certain offices, such as a judicial office or of an office of magistrate.

**Australian Link**

B.10 The APPs extend to an act done, or practice engaged in, outside Australia and the external Territories by an organisation, or small business operator, that has an Australian link (s 5B(1A)).

B.11 An organisation or small business operator has an Australian link where it is:

• an Australian citizen or a person whose continued presence in Australia is not subject to a legal time limitation
• a partnership formed, or a trust created, in Australia or an external Territory
• a body corporate incorporated in Australia or an external Territory, or
• an unincorporated association that has its central management and control in Australia or an external Territory (s 5B(2)).

B.12 An organisation that does not fall within one of those categories will also have an Australian link where:

• it carries on business in Australia or an external Territory, and
• it collected or held personal information in Australia or an external Territory, either before or at the time of the act or practice (s 5B(3)).

**Carries on business in Australia**

B.13 The phrase ‘carries on business in Australia’ in s 5B(3)(c) is not defined in the Privacy Act. However, it arises in other areas of law, including corporations and consumer law. Guidance may be drawn from judicial consideration of the phrase in those contexts.

B.14 The two elements – ‘carries on business’ and ‘in Australia’ – are connected but can be considered separately. Australian courts have held that both are questions of fact. An assessment should be made having regard to all relevant circumstances, particularly the nature of the enterprise conducted by an entity, and the particular Act being applied. In this instance, it is the Privacy Act being applied.

**Carry on business**

B.15 The general law concept of ‘carrying on business’ has been said to ‘generally involve conducting some form of commercial enterprise, systematically and regularly

---

4 See Luckins v Highway Motel (Carnavon) Pty Ltd (1975) 133 CLR 164, per Stephen J, at [186]; Bray v Hoffman-La Roche Ltd (2002) 118 FCR 1; ASIC v Active Super (No 1) [2012] FCA 1519 at [47]
with a view to profit\(^6\); or to embrace ‘activities undertaken as a commercial enterprise in
the nature of a going concern, that is, activities engaged in for the purpose of profit on a
continuous and repetitive basis’.\(^7\)

B.16 The focus of those definitions upon conducting or establishing a commercial
enterprise for the purpose of profit is important. Nevertheless, a necessary modification
of the concept in the context of the Privacy Act is that the Act can apply to a non-profit
entity that is an ‘organisation’ as defined in s 6C(1). As to those entities, the more
important element may be the repetition of commercial acts on a systematic or
continuing basis as part of the activities of the entity.

In Australia

B.17 Whether a business is carried on ‘in Australia’ focusses upon whether activity is
undertaken in Australia as part of the entity’s business. There is ‘a need for some physical
activity in Australia through human instrumentalities, being activity that itself forms part
of the course of conducting business’.\(^8\) However, as noted in another decision, ‘provided
that there are acts within Australia which are part of the company's business, the
company will be doing business in Australia although the bulk of its business is conducted
elsewhere and it maintains no office in Australia’.\(^9\)

B.18 An important consideration in applying this territorial requirement in the context
of the Privacy Act is that the Act, though technologically-neutral, operates in an
environment where personal information is regularly collected, held, used and disclosed
online by organisations that may simultaneously carry on business through the web in
many countries. In addition, an object of the Privacy Act is to ‘promote the protection of
the privacy of individuals’ (s 2A(a)), which requires that regard be had to contemporary
and practical circumstances.

B.19 In this context, factors that may be considered in assessing if an entity carries on
business in Australia include whether:

- the entity has a place of business in Australia
- people who undertake business acts for the entity are located in Australia – for
  example, an entity may carry on business in Australia where an agent acting on its
  behalf carries on its business from some fixed place in Australia\(^10\)
- the entity has a website that offers goods or services to countries including
  Australia
- Australia is one of the countries on the drop-down menu appearing on the entity’s
  website

---

\(^6\) Gebo Investments (Labuan) Ltd v Signatory Investments Pty Ltd [2005] NSWSC 544, at [38]
\(^7\) Hope v Council of the City of Bathurst (1980) 144 CLR 1 at [8]. For a discussion of the indicia of a ‘business’,
see On Call Interpreters and Translators Agency Pty Ltd v Commissioner of Taxation (No 3) [2011] FCA 366
at [217] – [281]
\(^8\) Gebo Investments (Labuan) Ltd v Signatory Investments Pty Ltd [2005] NSWSC 544 at [33]
\(^9\) Australian Securities and Investments Commission v ActiveSuper Pty Ltd (No 1) [2012] FCA 1519 at [47]
\(^10\) Bray v F Hoffman-La Roche Ltd (2002) 118 FCR 1 at [62]
• web content that forms part of carrying on the business, was uploaded by or on behalf of the entity, in Australia
• business or purchase orders are assessed or acted upon in Australia
• the entity is the registered proprietor of trademarks in Australia.  

B.20 The presence or absence of one of these factors may not be determinative in assessing whether an entity carries on business in Australia. For example, where an entity does not have a place of business in Australia, this does not necessarily mean that it does not carry on business in Australia.

B.21 An entity will not generally be regarded as carrying on business in Australia solely on the basis that a purchase order can be placed in Australia or that it has a website that can be accessed from Australia.  

**Personal information collected ‘in Australia’**

B.22 Personal information is collected ‘in Australia’ under s 5B(3)(c), if it is collected from an individual who is physically present in Australia or an external Territory, regardless of where the collecting entity is located or incorporated. An example is the collection of personal information from an individual who is physically located in Australia or an external Territory, via a website that is hosted outside Australia. This applies even if the website is owned by a company that is located outside of Australia or that is not incorporated in Australia.  

**Collects**

B.23 An APP entity collects personal information ‘only if the entity collects the personal information for inclusion in a record or generally available publication’ (s 6(1)).

B.24 The term ‘record’ is defined in s 6(1) and includes a document or an electronic or other device. Some items are excluded from the definition, such as anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition, and Commonwealth records in the open access period.

B.25 The term ‘generally available publication’ is defined in s 6(1) to mean a ‘magazine, book, article, newspaper or other publication that is, or will be, generally available to members of the public’, regardless of the form in which it is published and whether it is available on payment of a fee.

B.26 An APP entity does not collect personal information where that information is acquired but not included in a record or generally available publication. For example, a newspaper article containing personal information will not be ‘collected’ by the entity unless, for example, a clipping of the article is kept and stored with other documents held by the entity or the article is scanned and saved into the entity’s electronic database.

---

11 *Australian Wool Innovation Ltd v Newkirk* (no 3) [2005] FCA 1308 at [34]
12 *Gebo Investments (Labuan) Ltd v Signatory Investments Pty Ltd* [2005] NSWSC 544
13 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 218.
Chapter B: Key concepts

B.27 The concept of ‘collection’ applies broadly, and includes gathering, acquiring or obtaining personal information from any source and by any means, including from:

- individuals
- other entities
- generally available publications
- surveillance cameras, where an individual is identifiable or reasonably identifiable
- information associated with web browsing, such as personal information collected by cookies\(^{14}\)
- biometric technology, such as voice or facial recognition.

B.28 Collection may also take place when an APP entity generates personal information from other data it holds, such as the generation of an audit log.

Commonwealth record

B.29 A ‘Commonwealth record’ has the same meaning as in the *Archives Act 1983* (Archives Act) (s 6(1)).

B.30 The Archives Act states that a ‘Commonwealth record’ means:

- a record\(^{15}\) that is the property of the Commonwealth or a Commonwealth institution, or
- a record that is deemed to be a Commonwealth record either by a regulation made under the Archives Act or under s 22 of the Archives Act (which applies to records kept by a Royal Commission or Commission of inquiry) (s 3(1)).

B.31 Some categories of records are excluded from that definition:

- ‘exempt material’, which includes, for example, material included in the memorial collection of the Australian War Memorial, and material included in the collections maintained by the National Library of Australia, the National Gallery of Australia, the National Portrait Gallery of Australia, and the National Museum of Australia
- a register or guide maintained by the Archives, namely, the Australian National Register of Records, Australian National Guide to Archival Material or Australian National Register of Research Involving Archives (see Part VIII, Archives Act).

\(^{14}\) Analytical information collected from cookies (e.g., the number of times a page was visited) will not be personal information under the Privacy Act unless an individual is reasonably identifiable (see paragraphs B.85–B.96 below).

\(^{15}\) ‘Record’ is defined in s 3(1) of the Archives Act as ‘a document, or an object, in any form (including any electronic form) that is, or has been, kept by reason of: (a) any information or matter that it contains or that can be obtained from it; or (b) its connection with any event, person, circumstance or thing’.
B.32 It is likely that all or most personal information collected or received by an agency will be included in a ‘Commonwealth record’. Where an organisation is a contracted service provider under a Commonwealth contract, the records collected, received or held by that organisation under the contract may also be Commonwealth records.

B.33 APPs 4.3 and 11.2 require the destruction or de-identification of personal information in certain circumstances (see Chapters 4 and 11). These requirements do not apply to information contained in a Commonwealth record. Retention, destruction and alteration of Commonwealth records is governed by the Archives Act. A Commonwealth record can, as a general rule, only be destroyed or altered in accordance with s 24 of the Archives Act. The grounds on which this may be done include with the permission of the National Archives of Australia (as set out in a records disposal authority) or in accordance with ‘normal administrative practice’. Further information about Archives Act requirements is available from the National Archives of Australia at <www.naa.gov.au>.

Consent

B.34 Consent is relevant to the operation of a number of APPs. In some, consent is an exception to a general prohibition against personal information being handled in a particular way (for example, APPs 3.3(a) and 6.1(a)). In others, consent provides authority to handle personal information in a particular way (for example, APPs 7.3, 7.4 and 8.2(b)).

B.35 Consent means ‘express consent or implied consent’ (s 6(1)). The four key elements of consent are:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent.

Express or implied consent

B.36 Express consent is given explicitly, either orally or in writing. This could include a handwritten signature, an oral statement, or use of an electronic medium or voice signature to signify agreement.

B.37 Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the APP entity.

B.38 An APP entity should not assume that an individual has consented to a collection, use or disclosure that appears to be advantageous to that person. Nor can an entity establish implied consent by asserting that if the individual knew about the benefits of the collection, use or disclosure, they would probably consent to it.

B.39 Generally, it should not be assumed that an individual has given consent on the basis alone that they did not object to a proposal to handle personal information in a particular way. An APP entity cannot infer consent simply because it provided an individual with notice of a proposed collection, use or disclosure of personal information. It will be difficult for an entity to establish that an individual’s silence can be taken as
consent. Consent may not be implied if an individual’s intent is ambiguous or there is reasonable doubt about the individual’s intention.

B.40 Use of an opt-out mechanism to infer an individual’s consent will only be appropriate in limited circumstances, as the individual’s intention in failing to opt-out may be ambiguous. An APP entity will be in a better position to establish the individual’s implied consent the more that the following factors, where relevant, are met:

- the opt out option was clearly and prominently presented
- it is likely that the individual received and read the information about the proposed collection, use or disclosure, and the option to opt out
- the individual was given information on the implications of not opting out
- the opt out option was freely available and not bundled with other purposes
- it was easy for the individual to exercise the option to opt out, for example, there was little or no financial cost or effort required by the individual
- the consequences of failing to opt out are not serious
- an individual who opts out at a later time will, as far as practicable, be placed in the position as if they had opted out earlier.

B.41 An APP entity should generally seek express consent from an individual before handling the individual’s sensitive information, given the greater privacy impact this could have.

B.42 An APP entity should as far as practicable implement procedures and systems to obtain and record consent. This may resolve any doubt about whether consent was given (either on the basis of express or implied consent).

Voluntary

B.43 Consent is voluntary if an individual has a genuine opportunity to provide or withhold consent. Consent is not voluntary where there is duress, coercion or pressure that could overpower the person’s will.

B.44 Factors relevant to deciding whether consent is voluntary include:

- the alternatives open to the individual, if they choose not to consent
- the seriousness of any consequences if an individual refuses to consent
- any adverse consequences for family members or associates of the individual if the individual refuses to consent.

Bundled consent

B.45 Bundled consent refers to the practice of an APP entity ‘bundling’ together multiple requests for an individual’s consent to a wide range of collections, uses and disclosures of personal information, without giving the individual the opportunity to choose which collections, uses and disclosures they agree to and which they do not.

B.46 This practice has the potential to undermine the voluntary nature of the consent. If a bundled consent is contemplated, an APP entity could consider whether:
• it is practicable and reasonable to give the individual the opportunity to refuse consent to one or more proposed collections, uses and/or disclosures

• the individual will be sufficiently informed about each of the proposed collections, uses and/or disclosures

• the individual will be advised of the consequences (if any) of failing to consent to one or more of the proposed collections, uses and/or disclosures (see also, discussion of ‘informed’ below).

Informed

B.47 An individual must be aware of the implications of providing or withholding consent, for example, whether access to a service will be denied if consent is not given to collection of a specific item of personal information. An APP entity should ensure that an individual is properly and clearly informed about how their personal information will be handled, so they can decide whether to give consent (see also, discussion of ‘capacity’ below). The information should be written in plain English, without legal or industry jargon.

Current and specific

B.48 An APP entity should generally seek consent from an individual for collection and proposed uses and disclosures of personal information at the time the information is collected. Alternatively, if consent was not sought at the time of collection, or that consent did not cover a proposed use or disclosure, an entity should seek the individual’s consent at the time of the use or disclosure.

B.49 Consent given at a particular time in particular circumstances cannot be assumed to endure indefinitely. It is good practice to inform the individual of the period for which the consent will be relied on in the absence of a material change of circumstances.

B.50 An APP entity should not seek a broader consent than is necessary for its purposes, for example, consent for undefined future uses, or consent to ‘all legitimate uses or disclosures’ (see also, discussion of ‘bundled consent’ above). When seeking consent, an entity should describe the purpose to which it relates. The level of specificity required will depend on the circumstances, including the sensitivity of the personal information.

B.51 An individual may withdraw their consent at any time, and this should be an easy and accessible process. Once an individual has withdrawn consent, an APP entity can no longer rely on that past consent for any future use or disclosure of the individual’s personal information. Individuals should be made aware of the potential implications of withdrawing consent, such as no longer being able to access a service.

Capacity

B.52 An individual must have the capacity to consent. This means that the individual is capable of understanding the nature of a consent decision, including the effect of giving or withholding consent, forming a view based on reasoned judgement and how to communicate a consent decision. An APP entity can ordinarily presume that an individual...
has the capacity to consent, unless there is something to alert it otherwise, for example, the individual is a child or young person (see below). If an entity is uncertain as to whether an individual has capacity to consent at a particular time, it should not rely on any statement of consent given by the individual at that time.

B.53 Issues that could affect an individual’s capacity to consent include:

- age
- physical or mental disability
- temporary incapacity, for example during a psychotic episode, a temporary psychiatric illness, or because the individual is unconscious, in severe distress or suffering dementia
- limited understanding of English.

B.54 An APP entity should consider whether any such issue could be addressed by providing the individual with appropriate support to enable them to have capacity to consent. If an individual does not have capacity to consent, even with support or the provision of additional resources such as an interpreter or alternative communication methods, and consent is required, an entity should consider who can act on the individual’s behalf. Options include:

- a guardian
- someone with an enduring power of attorney
- a person recognised by other relevant laws, for example in NSW, a ‘person responsible’ under the Guardianship Act 1987 (NSW) (this may be an individual’s spouse, partner, carer, family member or close friend), or
- a person who has been nominated in writing by the individual while they were capable of giving consent.

B.55 An individual who lacks the capacity to consent should nevertheless be involved, as far as practicable, in any decision-making process. To the extent practicable in the circumstances, an APP entity should ensure that privacy issues are discussed with individuals who have impaired decision making capacity in a way that is understandable and comprehensible.

Children and young people

B.56 The Privacy Act does not specify an age after which individuals can make their own privacy decisions. An APP entity will need to determine on a case-by-case basis whether an individual under the age of 18 has the capacity to consent.

B.57 As a general principle, an individual under the age of 18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person, for example, if the child is young or lacks the maturity or understanding to do so themselves.

B.58 If it is not practicable or reasonable for an APP entity to assess the capacity of individuals under the age of 18 on a case-by-case basis, the entity may presume that an
individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise. An individual aged under 15 is presumed not to have capacity to consent.

**De-identification**

B.59 Personal information is de-identified ‘if the information is no longer about an identifiable individual or an individual who is reasonably identifiable’ (s 6(1)). De-identified information is not ‘personal information’ (see paragraphs B.85–B.96).

B.60 De-identification involves removing or altering information that identifies an individual or is reasonably likely to do so. Generally, de-identification includes two steps:

- removing personal identifiers, such as an individual’s name, address, date of birth or other identifying information, and
- removing or altering other information that may allow an individual to be identified, for example, because of a rare characteristic of the individual, or a combination of unique or remarkable characteristics that enable identification.

B.61 De-identification may not altogether remove the risk that an individual can be re-identified. There may, for example, be a possibility that another dataset or other information could be matched with the de-identified information. The risk of re-identification must be actively assessed and managed to mitigate this risk. Relevant factors to consider when determining whether information has been effectively de-identified could include the cost, difficulty, practicality and likelihood of re-identification.\(^{16}\)

B.62 For more information on when and how to de-identify information, and how to manage and mitigate the risk of re-identification, see *Privacy Business Resource 4 — De-identification of Data and Information* and *Information Policy Agency Resource 1 — De-identification of Data and Information*.\(^{17}\)

**Disclosure**

B.63 Disclosure is not defined in the Privacy Act.

B.64 An APP entity discloses personal information when it makes it accessible or visible to others outside the entity and releases the subsequent handling of the personal information from its effective control. This focuses on the act done by the disclosing party, and not on the actions or knowledge of the recipient. Disclosure, in the context of the Privacy Act, can occur even where the personal information is already known to the recipient.\(^{18}\)

B.65 The release may be a proactive release, a release in response to a specific request, an accidental release or an unauthorised release by an employee.

---

\(^{16}\) Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 60.


\(^{18}\) For a similar approach to interpreting ‘disclosure’, see *Pratt Consolidated Holdings Pty Ltd v Commissioner of Taxation* [2011] AATA 907 at [112] – [119]
B.66 Examples include where an APP entity:

- shares a copy of personal information with another entity or individual
- disclose personal information to themselves, but in their capacity as a different entity
- publishes personal information whether intentionally or not\(^{19}\) and it is accessible to another entity or individual
- accidentally provides personal information to an unintended recipient\(^{20}\)
- displays a computer screen so that the personal information can be read by another entity or individual, for example at a reception counter or in an office.

B.67 Where an APP entity engages a contractor to perform services on its behalf, the provision of personal information to that contractor will in most circumstances be a disclosure (see paragraph B.144 for the limited circumstances where it will be a ‘use’).

B.68 ‘Disclosure’ is a separate concept from:

- ‘unauthorised access’ which is addressed in APP 11. An APP entity is not taken to have disclosed personal information where a third party intentionally exploits the entity’s security measures and gains unauthorised access to the information.\(^{21}\) Examples include unauthorised access following a cyber-attack\(^{22}\) or a theft, including where the third party then makes that personal information available to others outside the entity. However, where a third party gains unauthorised access, the entity may breach APP 11 if it did not take reasonable steps to protect the personal information from unauthorised access (see Chapter 11 (APP 11))

- ‘use’, which is discussed in paragraphs B.142–B.144 below. The concept of ‘use’ encompasses information handling and management activities occurring within an entity’s effective control, for example, when staff of an entity access, read, exchange or make decisions based on personal information the entity holds.

B.69 In a number of APPs the same requirements apply to the ‘use’ or ‘disclosure’ of personal information (for example, APP 6.1 (see Chapter 6), APP 7 (see Chapter 7), APP 9.2 (see Chapter 9) and APP 10.2 (see Chapter 10)). For these, it is not necessary to distinguish between a ‘use’ and a ‘disclosure’. However, the distinction is relevant to the following principles and exceptions that only apply to the ‘disclosure’ of personal information, and not to its ‘use’:

- section 16B(5) (see Chapter D)
- APP 1.4(f) and (g) (see Chapter 1)

---


\(^{20}\) The APP entity may also breach APP 11 if it did not take reasonable steps to protect the information from this unauthorised disclosure (see APP 11, Chapter 11).

\(^{21}\) The actions of an employee will be attributed to the APP entity where it was carried out ‘in the performance of the duties of the person’s employment’ (s 8(1)).

• APP 5.2(f), (i) and (j) (see Chapter 5)
• APP 6.3 (see Chapter 6)
• APP 8 (see Chapter 8)
• APP 11.1(b) (Chapter 11).

Enforcement body

B.70 ‘Enforcement body’ is defined to mean:

• the Australian Federal Police
• the Integrity Commissioner
• the Australian Crime Commission
• the CrimTrac Agency
• Customs
• the Immigration Department
• the Australian Prudential Regulation Authority
• the Australian Securities and Investments Commission
• the Office of the Director of Public Prosecutions, or a similar body established under a law of a State or Territory
• another Commonwealth agency, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law
• another Commonwealth agency, to the extent that it is responsible for administering a law relating to the protection of the public revenue
• a police force or service of a State or a Territory
• the New South Wales Crime Commission
• the Independent Commission Against Corruption of New South Wales
• the Police Integrity Commission of New South Wales
• the Office of Police Integrity of Victoria
• the Crime and Misconduct Commission of Queensland
• the Corruption and Crime Commission of Western Australia
• another prescribed authority or body that is established under a law of a State or Territory to conduct criminal investigations or inquiries
• a State or Territory authority, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law, or
• a State or Territory authority, to the extent that it is responsible for administering a law relating to the protection of the public revenue (s 6(1)).

**Enforcement related activities**

B.71 ‘Enforcement related activity’ is defined to mean:

- the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction
- the conduct of surveillance activities, intelligence gathering activities or monitoring activities
- the conduct of protective or custodial activities
- the enforcement of laws relating to the confiscation of the proceeds of crime
- the protection of the public revenue
- the prevention, detection, investigation or remedying of misconduct of a serious nature, or other conduct prescribed by the regulations
- the preparation for, or conduct of, proceedings before any court or tribunal, or the implementation of court/tribunal orders (s 6(1)).

B.72 This definition recognises that ‘enforcement related activities’ can include lawful surveillance, intelligence gathering or monitoring activities where there may not be an existing investigation. Those activities are distinct but may also overlap.

B.73 Examples of surveillance activities include optical surveillance of an individual or property where information obtained from that surveillance may lead to an investigation of a criminal offence. Examples of intelligence gathering include the collection of personal information about an individual to detect whether an offence has occurred, or to determine whether to initiate an investigation into that offence; the collection of information about whether an individual is planning to commit an offence and whether there are fellow criminal associates. Examples of monitoring activities include the monitoring by an enforcement body of a person who has presented themself to that body in compliance with a court order.

**Health information**

B.74 ‘Health information’ is defined to mean:

- information or an opinion, that is also personal information, about:
  - the health or a disability (at any time) of an individual, or
  - an individual’s expressed wishes about the future provision of health services to him or her, or

---

23 Addendum to the Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 3.
24 Addendum to the Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 3.
B.75 Examples of health information include:

- information about an individual's physical or mental health
- notes of an individual's symptoms or diagnosis and the treatment given
- specialist reports and test results
- appointment and billing details
- prescriptions and other pharmaceutical purchases
- dental records
- records held by a fitness club about an individual
- information about an individual's suitability for a job, if it reveals information about the individual's health
- an individual's healthcare identifier when it is collected to provide a health service
- any other personal information (such as information about an individual's date of birth, gender, race, sexuality, religion), collected for the purpose of providing a health service.

B.76 The definition of ‘sensitive information’ in s 6(1) includes health information. Sensitive information, including health information, attracts additional privacy protections compared to other types of personal information (see for example, APP 3 in Chapter 3). There are also a number of provisions and APPs that deal specifically with health information, including the ‘permitted health situation’ exceptions set out in s 16B (see Chapter D (Permitted health situations)).

Health Service

B.77 ‘Health service’ is defined to mean:

- an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the person performing it:
  - to assess, record, maintain or improve the individual's health, or
  - to diagnose the individual's illness or disability, or
to treat the individual's illness or disability or suspected illness or disability,
or

- the dispensing or prescription of a drug or medicinal preparation by a pharmacist (s 6(1)).

B.78 The Privacy Act generally applies to all organisations that provide a health service, including an organisation that is a small business. Examples of organisations that provide a health service include:

- traditional health service providers, such as private hospitals, day surgeries, medical practitioners, pharmacists and allied health professionals
- complementary therapists, such as naturopaths and chiropractors
- gyms and weight loss clinics
- child care centres, private schools and private tertiary educational institutions.

Holds

B.79 An APP entity ‘holds’ personal information if ‘the entity has possession or control of a record that contains the personal information’ (s 6(1)).

B.80 The term ‘record’ is defined in s 6(1) and includes a document or an electronic or other device. Some items are excluded from the definition, such as anything kept in a library, art gallery or museum for the purposes of reference study or exhibition and Commonwealth records in the open access period.

B.81 The term ‘holds’ extends beyond physical possession of a record to include a record that an APP entity has the right or power to deal with. Whether an APP entity ‘holds’ a particular item of personal information may therefore depend on the particular information collection, management and storage arrangements it has adopted. For example, an APP entity ‘holds’ personal information where:

- it physically possesses a record containing the personal information and can access that information physically or by use of an electronic device (such as decryption software)
- it has the right or power to deal with the personal information, even if it does not physically possess or own the medium on which the personal information is stored. For example, the entity has outsourced the storage of personal information to a third party but it retains the right to deal with it, including to access and amend that information.

B.82 An agency that has placed a record of personal information in the care of the National Archives of Australia, or in the custody of the Australian War Memorial, is considered to be the agency that holds the record for the purposes of the Privacy Act (s 10(4)).

25 Small businesses – namely, those with an annual turnover of $3 million or less – are generally exempt from the operation of the Privacy Act (s 6D). However, this exemption does not apply to an individual, body corporate, partnership, unincorporated association or trust that provides a health service to another individual and holds any health information except in an employee record (s 6D(4)(b)).
**Immigration Department**

B.83 ‘Immigration Department’ means ‘the Department administered by the Minister administering the *Migration Act 1958*’ (s 6(1)). Information about the particular Minister and Department that administer the *Migration Act 1958* can be found on ComLaw.26

B.84 The definition of ‘enforcement body’ includes the ‘Immigration Department’ (see paragraph B.70). This means that the exception in APP 3.4(d)(i) that permits the collection of sensitive information, and the exceptions in APPS 6.2(e) and 8.2(f) that permit the use and disclosure of personal information, extend to the ‘enforcement related activities’ of the Immigration Department (see Chapters 3, 6 and 8).27

**Personal information**

B.85 ‘Personal information’ is defined as any ‘information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not’ (s 6(1)).

B.86 Common examples are an individual’s name, signature, address, telephone number, date of birth, medical records, bank account details, employment details and commentary or opinion about a person.

B.87 Personal information of one individual may also be personal information of another individual. Examples include a marriage certificate that contains personal information of both parties to a marriage, and a vocational reference that includes personal information about both the author and the subject of the reference.

B.88 The personal information ‘about’ an individual may be broader than the item of information that identifies them. For example, a vocational reference or assessment may comment on a person’s career, performance, attitudes and aptitude. Similarly, the views expressed by the author of the reference may also be personal information about the author.

B.89 Personal information that has been de-identified will no longer be personal information. Personal information is de-identified if the information is no longer about an identifiable individual or an individual who is reasonably identifiable (see paragraph B.59).

B.90 What constitutes personal information will vary, depending on whether an individual can be identified or is reasonably identifiable in the particular circumstances.

---


27 For examples of the functions and activities of the Immigration Department that will be covered by the ‘enforcement related activity’ exceptions in APPs 3.4, 6.2 and 8.2, see Addendum to the Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 2.
Meaning of 'reasonably identifiable’

B.91 Whether an individual is ‘reasonably identifiable’ from particular information will depend on considerations that include:\(^{28}\)

- the nature and amount of information
- the circumstances of its receipt
- who will have access to the information
- other information either held by or available to the APP entity that holds the information
- whether it is possible for the individual or entity that holds the information to identify the individual, using available resources (including other information available to that individual or entity). Where it may be possible to identify an individual using available resources, the practicability, including the time and cost involved, will be relevant to deciding whether an individual is ‘reasonably identifiable’\(^{29}\)

- if the information is publically released, whether a reasonable member of the public who accesses that information would be able to identify the individual.

B.92 The following are given as examples of how those considerations may apply to particular items of information:

- Most entities and individuals would encounter difficulty in using a licence plate number to identify the registrant of a car, as they would not have access to the car registration database. By contrast, an agency or individual with access to that database may be able to identify the registrant. Accordingly, the licence plate number may be ‘personal information’ held by that agency or individual, but may not be personal information if held by another entity.

- Information that an unnamed person with a certain medical condition lives in a specific postcode area may not enable the individual to be identified, and would not therefore be personal information. By contrast, it may be personal information if held by an entity or individual with specific knowledge that could link an individual to the medical condition and the postcode.\(^{30}\)

- A common surname that is shared by many people may not be personal information that would reasonably identify a particular individual. However, combined with other information, such as address or other contact information, it may be personal information

B.93 Whether a person is ‘reasonably identifiable’ is an objective test that has practical regard to the context in which the issue arises. Even though it may be technically possible to identify an individual from information, if doing so is so impractical that there is almost

\(^{28}\) Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 61.
\(^{29}\) Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 61.
\(^{30}\) Autism Aspergers Advocacy Australia and Department of Families, Housing, Community Services and Indigenous Affairs [2012] AICmr 28 (12 November 2012), see FOI review decisions, OAIC website <www.oaic.gov.au>
no likelihood of it occurring, the information would not generally be regarded as ‘personal information’. An individual may not be reasonably identifiable if the steps required to do so are excessively time-consuming or costly in all the circumstances.

B.94 Where it is unclear whether an individual is ‘reasonably identifiable’, an APP entity should err on the side of caution and treat the information as personal information.

**Deceased persons**

B.95 The definition of ‘personal information’ in s 6(1) refers to information or an opinion about an ‘individual.’ An ‘individual’ means ‘a natural person’ (s 6(1)). The ordinary meaning of ‘natural person’ does not include deceased persons.

B.96 Information about a deceased person may include information about a living individual and be ‘personal information’ for the purposes of the Privacy Act. For example, information that a deceased person had an inheritable medical condition may indicate that the deceased person’s descendants have an increased risk of that condition. If the descendants are identifiable, that information would be personal information about the descendants. The privacy interests of family members could therefore be considered when handling information about deceased persons.

**Purpose**

B.97 The purpose of an action is the reason why it is done. The purpose for which an APP entity collects, holds, uses and discloses personal information can be relevant to:

- whether the entity is permitted to collect, use, disclose and retain personal information (APPs 3, 4, 6, 7, and 11)
- the matters that must be included in the entity’s APP Privacy Policy (APP 1) and in any collection notice to the individual (APP 5)
- the steps that must be taken to ensure the quality of personal information (APP 10) and to correct incorrect information (APP 13).

**Primary purpose and secondary purpose**

B.98 The purpose for which an APP entity collects personal information is known as the ‘primary purpose’ of collection. This is the specific function or activity for which the entity collects the personal information. If an APP entity uses or discloses the personal information for another purpose this is known as a ‘secondary purpose’. APP 6 sets out when an APP entity may use or disclose personal information for a secondary purpose (see Chapter 6 (APP 6)).

B.99 Where an APP entity collects personal information directly from an individual, the context will help in identifying the primary purpose of collection. For example, the individual may provide the personal information for a particular purpose, such as buying

---

31 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 61.
32 However, for the purposes of Part VIA, which deals with personal information in emergencies and disasters, the definition of ‘individual’ in s 6(1) is taken to include an individual who is not living (s 80G(2)).
a particular product or receiving a particular service. This is the primary purpose of
collection, even if the entity has additional secondary purposes in mind.

B.100  Where an APP entity receives unsolicited personal information or collects
personal information about an individual from a third party, the context will again be
relevant in identifying the primary purpose of collection. It will also be relevant to
consider the function or activity which the personal information is reasonably necessary
for, or to which it directly relates. In some instances, an APP entity that receives
unsolicited personal information and retains it will have no primary purpose of collection.
For example, where the entity could not have collected personal information under APP
3.1 but nevertheless retains it under APP 4, because the information is contained in a
Commonwealth record, or because it is not lawful or reasonable for the entity to destroy
it (see APP 4, Chapter 4).

Describing the primary purpose

B.101  How broadly a purpose can be described will depend on the circumstances and
should be determined on a case-by-case basis. In cases of ambiguity, and with a view to
protecting individual privacy, the primary purpose for collection, use or disclosure should
be construed narrowly rather than expansively.

B.102  The primary purpose may nevertheless be described in general terms, as long as
the description is adequate to inform an individual of how the APP entity may use or
disclose their personal information. A description – the information will be used ‘for the
functions of the entity’ – would generally be considered too broad. Instead, the primary
purpose of collection could be described as to:

• provide a particular banking service
• market particular goods or services, or types of goods or services, to the
  individual
• assess an applicant’s suitability for a job
• assess an applicant’s eligibility for a loan
• resolve a complaint
• provide further information about a particular service
• enable an agency to give someone a particular benefit or service.

B.103  An APP entity does not need to include in its description internal purposes that
form part of normal business practices, such as auditing, business planning, billing or de-
identifying personal information.

Reasonable, Reasonably

B.104  The terms ‘reasonable’ and ‘reasonably’ are used in the Privacy Act and APPs to
qualify a test or obligation. Examples include that ‘personal information’ is information
about an individual who is ‘reasonably’ identifiable (s 6(1)) and an APP entity must not
collect personal information unless it is ‘reasonably necessary’ for one or more of the
entity’s functions or activities (APP 3).
B.105 ‘Reasonable’ and ‘reasonably’ are not defined in the Privacy Act. The terms bear their ordinary meaning, as being based upon or according to reason and capable of sound explanation. What is reasonable is a question of fact in each individual case. It is an objective test that has regard to how a reasonable person, who is properly informed, would be expected to act in the circumstances. What is reasonable can be influenced by current standards and practices. It is the responsibility of an APP entity to be able to justify that its conduct was reasonable. In a related context, the High Court has observed that whether there are ‘reasonable grounds’ to support a course of action ‘requires the existence of facts which are sufficient to [persuade] a reasonable person’; it ‘involves an evaluation of the known facts, circumstances and considerations which may bear rationally upon the issue in question’. As that indicates, there may be a conflicting range of objective circumstances to be considered, and the factors in support of a conclusion should outweigh those against.

B.106 The terms ‘reasonable’ and ‘reasonably’ are discussed further in the APP guidelines, as they arise in the context of each of the relevant APPs.

**Reasonable steps**

B.107 A number of the APPs require an APP entity to ‘take such steps as are reasonable in the circumstances’ (for example, APP 1.2 (see Chapter 1), APP 8.1 (see Chapter 8) and APP 11 (see Chapter 11). The shorthand expression used in the APP guidelines is ‘reasonable steps’.

B.108 The ‘reasonable steps’ test is an objective test, and is to be applied in the same manner as ‘reasonable’ and ‘reasonably’. It is the responsibility of an APP entity to be able to justify that reasonable steps were taken.

B.109 Some APPs require an APP entity to take ‘such steps (if any) as are reasonable in the circumstances’ (for example, APP 5.1 (see Chapter 5), APP 10 (see Chapter 10), APP 12.5 (see Chapter 12), APPs 13.1 and 13.2 (see Chapter 13). The inclusion of ‘(if any)’ acknowledges that in some circumstances an entity will satisfy the requirement to take reasonable steps by taking no steps.

**Reasonably believes**

B.110 A number of the exceptions to the APPs require an APP entity to have a ‘reasonable belief’ about a particular matter (see for example, APP 3.4 (Chapter 3), APP 6.2(e) (Chapter 6), APP 8.2 (Chapter 8), Permitted general situations, (Chapter C)).

B.111 The phrase ‘reasonable belief’ is to be applied in the same manner as ‘reasonable’ and ‘reasonably’. That is, the APP entity must have a reasonable basis for the belief, and not merely a genuine or subjective belief. The requirement for a reasonable belief

---

35 *McKinnon v Secretary, Department of Treasury* (2006) 228 CLR 423 at 430 (Gleeson CJ & Kirby JJ).
36 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 54.
precludes arbitrary action, but may still leave something to surmise or conjecture.\(^{37}\) It is the responsibility of an entity to be able to justify its reasonable belief.

**Reasonably necessary and necessary**

B.112 A number of APPs require a collection, use or disclosure to be ‘reasonably necessary’ for a particular purpose – see APPs 3, 6, 8 and 9. Certain permitted general situations and permitted health situations refer to a collection, use or disclosure being ‘necessary’ for a particular purpose (see Chapters C and D), and APP 7 refers to a use or disclosure being ‘necessary’ to meet a contractual obligation (see Chapter 7).

B.113 The term ‘reasonable’ is discussed at paragraphs B.104–B.106. ‘Necessary’ is not defined in the Privacy Act. The High Court of Australia has noted that ‘there is, in Australia, a long history of judicial and legislative use of the term ‘necessary’, not as meaning essential or indispensable, but as meaning reasonably appropriate and adapted’.\(^{38}\) However, in the context of the Privacy Act, it would not be sufficient if the collection, use or disclosure is merely helpful, desirable or convenient.

B.114 The ‘reasonably necessary’ test is an objective test: whether a reasonable person who is properly informed would agree that the collection, use or disclosure is necessary. It is the responsibility of an APP entity to be able to justify that the particular collection, use or disclosure is reasonably necessary.

B.115 The test must be applied in a practical sense. For example, under APP 3 if an entity cannot in practice effectively pursue a function or activity without collecting personal information, the collection would usually be considered reasonably necessary for that function or activity. However, a collection, use or disclosure of personal information will not usually be considered reasonably necessary if there are reasonable alternatives available, for example, if de-identified information would be sufficient for the function or activity.

B.116 An APP entity cannot rely solely on normal business practice in assessing whether a collection, use or disclosure is reasonably necessary. The primary issue is whether, in the circumstances of a particular entity, a collection, use or disclosure is reasonably necessary for a particular function or activity.

B.117 The term ‘necessary’ rather than ‘reasonably necessary’ is used in certain permitted general situations and permitted health situations, and in APP 7. The context explains this different usage. For example, a permitted health situation may exist if the collection of personal information is ‘necessary’ for public health research that is conducted in accordance with relevant guidelines. Similarly, APP 7.5 refers to the use or disclosure of personal information for the purpose of direct marketing where that is ‘necessary’ to meet a contractual obligation. In some of the permitted general situations and permitted health situations the test is whether an APP entity ‘reasonably believes’ that the collection, use or disclosure of personal information is ‘necessary’ for a particular purpose, such as lessening or preventing a serious threat to a person’s health or safety.


Recognised external dispute resolution scheme

B.118 ‘Recognised external dispute resolution scheme’ is defined as ‘an external dispute resolution scheme recognised under section 35A’ (s 6(1)).

B.119 Section 35A(1) gives the Information Commissioner power to recognise an external dispute resolution scheme for an entity or a class of entities, or for a specified purpose. A register of recognised external dispute resolution schemes is maintained on the Office of the Australian Information Commissioner website.39

B.120 An individual who considers that an APP entity has interfered with their privacy may complain to a recognised EDR scheme of which the entity is a member, if the complaint falls within the scope of the EDR scheme’s recognition. For further discussion of recognised EDR schemes, and their role in handling privacy-related complaints, see Guidelines for Recognising External Dispute Resolution Schemes under s 35A of the Privacy Act.40

Registered APP code

B.121 A ‘registered APP code’ is defined as an APP code that is included on the Codes Register and that is in force (s 26B(1)). A registered APP code is a legislative instrument (s 26B(2)). The requirements in relation to registered APP codes are set out in Division 2 of Part IIIB.

B.122 An ‘APP code’ is defined as a written code of practice about information privacy (s 26C). It can be developed by an APP entity, either on its own initiative or on request from the Information Commissioner, or by the Information Commissioner directly (ss 26E and 26G). A code may be expressed to apply to all or a specified type of personal information, a specified activity or class of activities of an APP entity, a specified industry sector or professions or specified class of industry sectors or professions, or APP entities that use technology of a specified kind (s 26C(4)).

B.123 The Information Commissioner has power to approve and register an APP code (provided certain conditions are met) by including it on the Codes Register (s 26H).

B.124 Once an APP code is registered, an APP entity bound by the code must not do an act, or engage in a practice, that breaches that code. A breach of a registered APP code will be ‘an interference with the privacy of an individual’ by the entity under s 13(1)(b).

B.125 A registered APP code does not replace the APPs for the entities which it binds, but operates in addition to the requirements of the APPs.41 For further discussion about the development of APP codes, and the requirements and process for recognition, see the Code Development Guidelines.42

---

41 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 199.
Related body corporate

B.126 Section 6(8) provides that ‘the question whether bodies corporate are related to each other is determined in the manner in which that question is determined under the Corporations Act 2001’.

B.127 Section 13B(1) permits related bodies corporate to share personal information (other than sensitive information) in certain circumstances. The effect of s 13B(1) is discussed further in Chapter 3 (APP 3) and Chapter 6 (APP 6).

Required or authorised by or under an Australian law or a court/tribunal order

B.128 A number of the APPs provide an exception if an APP entity is ‘required or authorised by or under an Australian law or a court/tribunal order’ to act differently (for example, APP 3.4(a) (Chapter 3), APP 6.2(b) (Chapter 6) and APP 12.3(g) (Chapter 12)). Some other provisions refer more narrowly to an act that is ‘required by or under an Australian law (other than this Act)’ (s 16B(2) (Chapter D)) or ‘required by or under an Australian law, or a court order’ (APP 11.2(d) (Chapter 11)), and do not include an act that is ‘authorised’.

Meaning of ‘required’

B.129 An APP entity that is ‘required’ by an Australian law or a court/tribunal order to handle information in a particular way has a legal obligation to do so, and cannot choose to act differently. The obligation will usually be indicated by words such as ‘must’ or ‘shall’, and may be accompanied by a sanction for non-compliance.

Meaning of ‘authorised’

B.130 An APP entity that is ‘authorised’ under an Australian law or a court/tribunal order has discretion as to whether it will handle information in a particular way. The entity is permitted to take the action but is not required to do so. The authorisation may be indicated by a word such as ‘may’, but may also be implied rather than expressed in the law or order.

B.131 An APP entity may be impliedly authorised by law to handle personal information in a particular way, where a law requires or authorises a function or activity, and this directly entails the information handling practice. For example, a statute that authorises an APP entity to collect personal information about an individual from a third party implicitly authorises the entity to disclose the individual’s identity to the third party.

B.132 An act or practice is not ‘authorised’ solely because there is no law or court/tribunal order prohibiting it. Nor can an act or practice rely solely on a general or incidental authority conferred by statute upon an agency to do anything necessary or convenient for, or incidental to or consequential upon, the specific functions and powers of the agency. The reason is that the purpose of the APPs is to protect the privacy of individuals by imposing obligations on APP entities in handling personal information. A
law will not authorise an exception to those requirements unless it does so by clear and direct language.\textsuperscript{43}

**Meaning of ‘Australian law’**

B.133 ‘Australian law’ is defined as:
- an Act of the Commonwealth, or of a State or Territory
- regulations or any other instrument made under such an Act
- a Norfolk Island enactment, or
- a rule of common law or equity (s 6(1)).

B.134 The definition of Australian law does not include a contract.\textsuperscript{44} Consequently, an obligation imposed by contract upon a party to handle information in a particular way will not provide authority for the purposes of the ‘required or authorised by or under an Australian law or court/tribunal order’ exception.

**Meaning of ‘court/tribunal order’**

B.135 ‘Court/tribunal order’ is defined as an order, direction or other instrument made by a court, a tribunal, a judge, a magistrate, a person acting as a judge or magistrate, a judge or magistrate acting in a personal capacity, and a member or an officer of a tribunal (s 6(1)).

B.136 The definition applies to orders and the like issued by Commonwealth, State and Territory courts, tribunals and members and officers. The definition includes an order, direction or other instrument that is of an interim or interlocutory nature.

B.137 The reference to a judge or a magistrate acting in a personal capacity means that the definition applies to an order or direction issued by a judge or magistrate who has been appointed by government to an office or inquiry that involves the exercise of administrative or executive functions, including functions that are quasi-judicial in nature.\textsuperscript{45} An example is a judge who is appointed by government to conduct a royal commission.

**Sensitive information**

B.138 ‘Sensitive information’ is a subset of personal information and is defined as:
- information or an opinion (that is also personal information) about an individual’s:
  - racial or ethnic origin
  - political opinions
  - membership of a political association

\textsuperscript{43} See *Coco v The Queen* (1994) 179 CLR 427.

\textsuperscript{44} Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 55.

\textsuperscript{45} *Drake v Minister for Immigration & Ethnic Affairs* (1979) 2 ALD 60; 46 FLR 409; *Grollo v Palmer* (1995) 184 CLR 348.
Chapter B: Key concepts

- religious beliefs or affiliations
- philosophical beliefs
- membership of a professional or trade association
- membership of a trade union
- sexual orientation or practices, or
- criminal record

- health information about an individual (see paragraphs B.74–B.78)
- genetic information (that is not otherwise health information)
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or
- biometric templates (s 6(1)).

B.139 Information may be sensitive information where it clearly implies one of these matters. For example, many surnames have a particular racial or ethnic origin, but that alone will not constitute sensitive information that clearly indicates the racial or ethnic origin of an individual with that surname.

B.140 Terms such as ‘political opinions’ and ‘philosophical beliefs’ are not defined in the Privacy Act. They take their ordinary meaning and should be interpreted broadly. However, not every value, belief or opinion of an individual will be considered to be a political opinion or philosophical belief.

B.141 Sensitive information is generally afforded a higher level of privacy protection under the APPs than other personal information (for example, see APPs 3, 6 and 7). This recognises that inappropriate handling of sensitive information can have adverse consequences for an individual or those associated with the individual. For example, discrimination or mistreatment is sometimes based on a person’s race or ethnic origin or union membership. Mishandling of sensitive information may also cause humiliation or embarrassment or undermine an individual’s dignity.

Use

B.142 ‘Use’ is not defined in the Privacy Act. Use is a separate concept from disclosure, which is discussed at paragraphs B.63–B.68. As noted at paragraph B.69, many APP requirements apply to both the ‘use’ and ‘disclosure’ of personal information, and in those situations it is not necessary to distinguish both concepts.

B.143 Generally, an APP entity uses personal information when it handles and manages that information within the entity’s effective control. Examples include:

- the entity accessing and reading the personal information
- the entity searching records for the personal information
- the entity making a decision based on the personal information
- the entity passing the personal information from one part of the entity to another
B.144 In limited circumstances, providing personal information to a contractor to perform services on behalf of the APP entity may be a use, rather than a disclosure (see paragraph B.63–B.68). This occurs where the entity does not release the subsequent handling of personal information from its effective control. For example, if an entity provides personal information to a cloud service provider for the limited purpose of performing the services of storing and ensuring the entity may access the personal information, this may be a ‘use’ by the entity in the following circumstances:

- a binding contract between the entity and the provider requires the provider only to handle the personal information for these limited purposes
- the contract requires any subcontractors to agree to the same obligations, and
- the contract gives the entity effective control of how the information is handled by the provider. Issues to consider include whether the entity retains the right or power to access, change or retrieve the information, who else will be able to access the information and for what purposes, the security measures that will be used for the storage and management of the personal information (see also APP 11.1, Chapter 11) and whether the information can be retrieved or permanently deleted by the entity when no longer required or at the end of the contract.47

46 An APP entity is taken to have ‘used’ personal information where an employee gains unauthorised access ‘in the performance of the duties of the person’s employment’ (see s 8(1)).

Chapter C — Permitted general situations

Version 1.0, February 2014

What are permitted general situations? ................................................................. 2
Lessening or preventing a serious threat to life, health or safety ................................ 2
   Unreasonable or impracticable to obtain consent ........................................ 2
   Reasonably believes collection, use or disclosure is necessary ....................... 3
   Lessen or prevent a serious threat ............................................................... 4
Taking appropriate action in relation to suspected unlawful activity or serious misconduct ................................................................. 4
Locating a person reported as missing ............................................................... 5
Reasonably necessary for establishing, exercising or defending a legal or equitable claim 6
Reasonably necessary for a confidential alternative dispute resolution process ........ 7
Necessary for a diplomatic or consular function or activity .............................. 7
Necessary for certain Defence Force activities outside Australia ..................... 8
What are permitted general situations?

C.1 The information handling requirements imposed by some APPs do not apply if a ‘permitted general situation’ exists. This exception applies in relation to the collection of sensitive information (APP 3), the use or disclosure of personal information (APPs 6 and 8) and the use or disclosure of a government related identifier (APP 9). It is nevertheless open to an APP entity to comply with the APP requirements even though an exception applies.

C.2 There are seven permitted general situations listed in s 16A:

• lessening or preventing a serious threat to the life, health or safety of any individual, or to public health or safety (see APPs 3.4(b), 6.2(c), 8.2(d) and 9.2(d))
• taking appropriate action in relation to suspected unlawful activity or serious misconduct (see APPs 3.4(b), 6.2(c), 8.2(d) and 9.2(d))
• locating a person reported as missing (see APPs 3.4(c), 6.2(c) and 8.2(d))
• asserting a legal or equitable claim (see APPs 3.4(c) and 6.2(c))
• conducting an alternative dispute resolution process (see APPs 3.4(b) and 6.2(c))
• performing diplomatic or consular functions – this permitted general situation only applies to agencies (see APP 3.4(b), 6.2(c) and 8.2(d))
• conducting specified Defence Force activities – this permitted general situation only applies to the Defence Force (see APP 3.4(b), 6.2(c) and 8.2(d))

C.3 These permitted general situations are discussed generally below. Specific examples relevant to each APP are also given in the chapter relating to that APP.

Lessening or preventing a serious threat to life, health or safety

C.4 This permitted general situation applies when an APP entity is collecting, using or disclosing personal information or a government related identifier, and:

• it is unreasonable or impracticable to obtain the individual’s consent to the collection, use or disclosure, and
• the entity reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety (s 16A, Item 1).

Unreasonable or impracticable to obtain consent

C.5 Consent is defined as ‘express consent or implied consent’ (s 6(1)) and is discussed in Chapter B (Key concepts). The main criteria for establishing consent are:

• the individual is adequately informed before giving consent
• the individual gives consent voluntarily
• the consent is current and specific, and
• the individual has the capacity to understand and communicate their consent.

C.6 An APP entity should be able to point to one or more clear reasons that make it unreasonable or impracticable to obtain an individual’s consent. Relevant considerations may include:

• the nature of, and potential consequences associated with, the serious threat. For example, the urgency of a situation and level of threatened harm may require collection, use or disclosure before it is possible to seek consent

• the possible adverse consequences for an individual if their consent is not obtained before the collection, use or disclosure. It may be more difficult for an entity to establish that it was unreasonable or impracticable to obtain the individual’s consent as the risk of adversity increases

• the source of the threat. For example, it may be unreasonable to seek consent from the individual posing the threat where that individual could reasonably be anticipated to withhold consent, or where the act of seeking that individual’s consent could increase the threat

• the ability to contact the individual to obtain consent. For example, it may be impracticable to obtain consent if the individual’s location is unknown after reasonable enquiries have been made, or if they cannot be contacted for another reason

• the capacity of the individual to give consent. For example, it may be unreasonable or impracticable to obtain consent where an individual is incapable of communicating consent because of their physical or psychological state or their age (capacity is discussed as part of ‘consent’ in Chapter B (Key concepts))

• the number of individuals whose personal information is to be collected, used or disclosed. For example, it may be impracticable to obtain consent from a very large number of individuals (though see below as to the relevance of inconvenience, time and costs)

• the inconvenience, time and cost involved in obtaining consent. However, an entity is not excused from obtaining consent by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it impracticable to obtain consent will depend on whether the burden is excessive in all the circumstances.

Reasonably believes collection, use or disclosure is necessary

C.7 Where it is unreasonable or impracticable to obtain consent, an APP entity must reasonably believe the collection, use or disclosure is necessary to lessen or prevent a serious threat. The terms ‘reasonably believes’ and ‘necessary’ are discussed in Chapter B (Key concepts).

C.8 In summary, there must be a reasonable basis for the belief, and not merely a genuine or subjective belief. It is the responsibility of an APP entity to be able to justify its
reasonable belief. A collection, use or disclosure would not be considered necessary where it is merely helpful, desirable or convenient.

**Lessen or prevent a serious threat**

C.9 This permitted general situation applies to a serious threat to the life, health or safety of any individual, or to public health or safety. The permitted general situation would not apply after the threat has passed. A ‘serious’ threat is one that poses a significant danger to an individual or individuals. The likelihood of a threat occurring as well as the consequences if the threat materialises are both relevant. A threat that may have dire consequences but is highly unlikely to occur would not normally constitute a serious threat. On the other hand, a potentially harmful threat that is likely to occur, but at an uncertain time, may be a serious threat, such as a threatened outbreak of infectious disease. This allows an APP entity to take preventative action to stop a serious threat from escalating before it materialises.

C.10 The permitted general situation applies to a threat to life, health or safety. This can include a threat to a person’s physical or mental health and safety. It could include a potentially life threatening situation or one that might reasonably result in other serious injury or illness. The permitted general situation would not ordinarily extend to a threat to an individual’s finances or reputation.

C.11 The threat may be to an individual the APP entity is dealing with or to another person. It may also be a threat of serious harm to an unspecified individual, such as a threat to inflict harm randomly.

C.12 A ‘serious threat to public health or safety’ relates to broader safety concerns affecting a number of people. Examples include:

- the potential spread of a communicable disease
- harm, or threatened harm, to a group of people due to a terrorist incident
- harm caused by an environmental disaster.

C.13 If time permits, attempts could be made to seek the consent from the relevant individuals for the collection, use or disclosure, before relying on this permitted general situation.

**Taking appropriate action in relation to suspected unlawful activity or serious misconduct**

C.14 This permitted general situation applies when an APP entity is collecting, using or disclosing personal information or a government related identifier, and the entity:

- has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity’s functions or activities has been, is being, or may be engaged in, and
- reasonably believes that the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter (s 16A, Item 2).
C.15 This permitted general situation is intended to apply to an APP entity’s internal investigations about activities within or related to the entity. It applies when the entity has reason to suspect unlawful activity, as well as misconduct of a serious nature that does not necessarily amount to unlawful activity.

C.16 ‘Unlawful activity’ is not defined in the Privacy Act. The core meaning is activity that is criminal, illegal or prohibited or proscribed by law, and can include unlawful discrimination or harassment, but does not include breach of a contract. Examples of unlawful activity include criminal offences, unlawful discrimination, and trespass. The unlawful activity must relate to the APP entity’s functions or activities. For example, harassment or discrimination within an entity would be an unlawful activity.

C.17 ‘Misconduct’ is defined in s 6(1) to include ‘fraud, negligence, default, breach of trust, breach of duty, breach of discipline or any other misconduct in the course of duty’. ‘Serious’ misconduct does not cover minor breaches and transgressions. The serious misconduct must relate to the APP entity’s functions or activities. For example, a serious breach by a staff member of the Australian Public Service Code of Conduct, or fraudulent conduct by a professional adviser or a client in relation to the entity’s functions or activities.

C.18 An APP entity must have ‘reason to suspect’ that unlawful activity or serious misconduct is being, or may be engaged in. Though only a reasonable suspicion is required, it is the responsibility of the entity to be able to justify the suspicion.

C.19 An APP entity must ‘reasonably believe’ that the collection, use or disclosure of personal information is ‘necessary’ for the entity to take ‘appropriate action’. ‘Reasonably believes’ and ‘necessary’ are discussed further in Chapter B (Key concepts). In summary, there must be a reasonable basis for the belief that the collection, use or disclosure is necessary, and not merely a genuine or subjective belief. A collection, use or disclosure would not be considered necessary where it is merely helpful, desirable or convenient. It is the responsibility of an entity to be able to justify its reasonable belief.

C.20 Whether action is ‘appropriate’ will depend on the nature of the suspected unlawful activity or misconduct and the nature of the action that the APP entity proposes to take. Appropriate action may include investigating an unlawful activity or serious misconduct and reporting these matters to the police or another relevant person or authority. For example, if an entity reasonably believes that it cannot effectively investigate serious misconduct without collecting, using or disclosing personal information, this permitted general situation may apply.

### Locating a person reported as missing

C.21 This permitted general situation applies when an APP entity reasonably believes that the collection, use or disclosure of personal information is reasonably necessary to

---

1 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 67.
2 Where an APP entity seeks to disclose personal information to an ‘enforcement body’, such as the Australian Federal Policy or the police force or service of a State or Territory, it may be able to rely on the exception at APP 6.2(e). APP 6.2(e) permits the use or disclosure of personal information where an APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body (see Chapter 6).
assist any APP entity, body or person to locate a person who has been reported as missing. The collection, use or disclosure must comply with the rules made by the Information Commissioner under s 16A(2) (s 16A, Item 3).

C.22 The terms ‘reasonably believes’ and ‘reasonably necessary’ are discussed further in Chapter B (Key concepts). In summary, the APP entity must have a reasonable basis for the belief that the collection, use or disclosure is reasonably necessary, and not merely a genuine or subjective belief. ‘Reasonably necessary’ has regard to whether a reasonable person who is properly informed would agree that the collection, use or disclosure is necessary. It is the responsibility of an entity to be able to justify that the entity reasonably believes that the collection, use or disclosure is reasonably necessary.

C.23 The rules made by the Commissioner under s 16A(2) are a legislative instrument that are available on the Comlaw website.³

### Reasonably necessary for establishing, exercising or defending a legal or equitable claim

C.24 This permitted general situation applies if an APP entity collects, uses or discloses personal information that is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim (s 16A, Item 4).

C.25 The term ‘reasonably necessary’ is discussed further in Chapter B (Key concepts). In summary, it is an objective test that has regard to whether a reasonable person, who is properly informed, would agree that the collection, use or disclosure is necessary. A collection, use or disclosure would not be considered necessary where it is merely helpful, desirable or convenient. It is the responsibility of the APP entity to be able to justify that the particular collection, use or disclosure is reasonably necessary.

C.26 This permitted general situation applies to the collection, use or disclosure of personal information in relation to existing or anticipated legal proceedings in a court or tribunal. Where legal proceedings have not yet commenced, this situation will usually only apply to a collection, use or disclosure involving a real possibility of legal proceedings, for example where professional legal advice is sought about commencing legal proceedings. By contrast, this permitted general situation does not compel an APP entity to disclose personal information in response to a request from a third party, and it may be difficult for an entity to be satisfied that it is reasonably necessary to do so solely on the basis that a third party has requested the information in connection with existing or anticipated legal proceedings.

C.27 An APP should not rely on this permitted general situation to disclose personal information if doing so would be contrary to an Australian law (for example, a statutory secrecy provision) or a legal order or principle (for example, if disclosure would be a breach of legal professional privilege).

Reasonably necessary for a confidential alternative dispute resolution process

C.28 This permitted general situation applies if an APP entity collects, uses or discloses personal information that is reasonably necessary for the purposes of a confidential alternative dispute resolution process (s 16A, Item 5).

C.29 The term ‘reasonably necessary’ is discussed further in Chapter B (Key concepts). In summary, it is an objective test that has regard to whether a reasonable person, who is properly informed, would agree that the collection, use or disclosure is necessary. A collection, use or disclosure would not be considered necessary where it is merely helpful, desirable or convenient. It is the responsibility of the APP entity to be able to justify that the particular collection, use or disclosure is reasonably necessary.

C.30 The phrase ‘alternative dispute resolution process’ (or ADR) is not defined in the Privacy Act. ADR covers processes, other than judicial determinations, in which an impartial person assists those in a dispute to resolve the issues between them. That person may, but is not required to, have any particular form of accreditation. Examples of ADR processes include mediation, conciliation, facilitation, expert assessment, determination, or neutral evaluation.4

C.31 For the exception to apply, the parties to the dispute and the ADR provider must be bound by confidentiality obligations such that any personal information collected, used or disclosed for the purpose of that ADR process will not be used or disclosed for any purpose outside the ADR process, including use or disclosure in subsequent proceedings. The confidentiality obligations may be imposed through contractual agreements or legislative provisions.

C.32 This permitted general situation extends to a disclosure of personal information by an APP entity to an ADR provider, a collection, use or disclosure by an entity for the purpose of participating in the ADR, and the collection, use or disclosure by an entity in relation to a complaint of professional misconduct against an ADR practitioner.

Necessary for a diplomatic or consular function or activity

C.33 This permitted general situation applies when an agency reasonably believes that the collection, use or disclosure of personal information is necessary for the agency’s diplomatic or consular functions or activities (s 16A, Item 6). This permitted general situation applies only to agencies, and not to organisations. The terms ‘reasonably believes’ and ‘necessary’ are discussed further in Chapter B (Key concepts).

C.34 The terms ‘diplomatic’ and ‘consular’ are not defined in the Privacy Act. An agency can rely on this permitted general situation only if it has diplomatic or consular functions or powers, conferred either by legislation or an executive instrument (such as the

---

Administrative Arrangements Order). The following are given as examples of when this permitted general situation might apply:

- **Diplomatic functions or activities**: where an agency collects, uses or discloses personal information to grant a diplomatic visa to a foreign national accredited as a member of the diplomatic staff of a mission to Australia.

- **Consular functions or activities**: where an agency collects, uses or discloses personal information to:
  - assist Australian citizens who are in distress overseas, including where an Australian individual is detained or is the victim of crime, or where assistance is required with repatriation in the case of death or serious illness, or to provide assistance in response to a crisis or emergency overseas.
  - provide information to the next of kin of an Australian individual who is overseas where, for example, the individual is seriously injured or is suffering serious physical or mental illness, and the agency considers that there are likely to be significant, serious or undesirable consequences for the individual or their next of kin if it does not disclose the personal information.

### Necessary for certain Defence Force activities outside Australia

C.35 This permitted general situation applies to the collection, use or disclosure of personal information by the Defence Force, where it reasonably believes that the collection, use or disclosure is necessary for any of the following occurring outside Australia and the external Territories:

- war or warlike operations
- peacekeeping or peace enforcement
- civil aid, humanitarian assistance, medical or civil emergency or disaster relief (s 16A, Item 7).

C.36 For a discussion of ‘reasonably believes’ and ‘necessary’, see Chapter B (Key concepts).

C.37 The following are given as examples of when this permitted general situation might apply:

- War or warlike operations/peacekeeping or peace enforcement: where the Defence Force collects sensitive information, such as biometric information, about an enemy or other hostile adversary and uses and discloses this and other personal information in order to support Defence Force military operations.

- Civil aid, humanitarian assistance, medical or civil emergency or disaster relief: where the Defence Force collects sensitive information about an individual in the immediate aftermath of a natural or man-made disaster outside Australia and the
external Territories, and uses or discloses this and other personal information in order to trace the individual or relatives of the individual, or assist in the provision of proper medical care.
Chapter D: Permitted health situations

Version 1.0, February 2014

What are permitted health situations? ................................................................................ 2
Collection — providing a health service ........................................................................... 2
Collection — conducting research; compiling or analysing statistics; management, funding
or monitoring of a health service ......................................................................................... 3
Public health or public safety ............................................................................................. 3
Management, funding or monitoring of a health service .................................................. 4
De-identified information .................................................................................................. 4
Impracticable to obtain consent ........................................................................................ 4
Guidelines approved under s 95A ...................................................................................... 5
Disclosure of personal information collected under this permitted health situation ....... 5
Use or disclosure — conducting research; compiling or analysing statistics ....................... 5
Use or disclosure — necessary to prevent a serious threat to the life, health or safety of a
genetic relative ..................................................................................................................... 6
Disclosure — responsible person for an individual .............................................................. 7
Incapacity to give consent................................................................................................... 7
Cannot communicate consent ............................................................................................ 8
Carer ................................................................................................................................... 8
Wishes of the individual........................................................................................................ 8
What are permitted health situations?

D.1 The information handling requirements imposed by APP 3 and APP 6 do not apply to an organisation if a ‘permitted health situation’ exists. This exception applies to the collection, use or disclosure of health information or genetic information by an organisation. The exception applies only to organisations, and not to agencies. It is open to an organisation to comply with the APP requirements even though an exception applies.

D.2 There are five permitted health situations listed in s 16B:

- the collection of health information to provide a health service (s 16B(1)) (see APP 3.4(c))
- the collection of health information for certain research and other purposes (s 16B(2)) (see APP 3.4(c))
- the use or disclosure of health information for certain research and other purposes (s 16B(3)) (see APP 6.2(d))
- the use or disclosure of genetic information (s 16B(4)) (see APP 6.2(d))
- the disclosure of health information for a secondary purpose to a responsible person for an individual (s 16B(5)) (see APP 6.2(d)).

D.3 ‘Health information’ is defined in s 6(1). It is a type of sensitive information and is discussed in more detail in Chapter B (Key concepts). Genetic information is not defined in the Privacy Act, and is discussed in paragraphs D.26–D.27 below.

D.4 The permitted health situations are discussed generally below. For specific examples that are relevant to APPs 3 and 6, see Chapters 3 and 6.

Collection — providing a health service

D.5 This permitted health situation applies when an organisation is collecting health information about an individual, if the information is necessary to provide a health service to the individual, and either:

- the collection is required or authorised by or under an Australian law (other than the Privacy Act), or
- the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation (s 16B(1)).

D.6 The terms ‘necessary’, ‘health service’ and ‘required or authorised by or under Australian law’ are discussed in Chapter B (Key concepts).

D.7 This permitted health situation overlaps with another exception stated in APP 3.4(a), namely the collection of sensitive information (which includes health information) as required or authorised by or under law or a court/tribunal order.
D.8 In deciding whether the collection of health information is ‘necessary’ to provide a health service, an organisation should consider if there are reasonable alternatives available. Further, an organisation should collect only the minimum amount of health information needed to provide a health service.

D.9 The Privacy Act does not specify which bodies qualify as ‘competent health or medical bodies’. Common examples include medical boards and other rule-making bodies recognised in an applicable Australian law. An important requirement is that the organisation collecting the information does so in accordance with rules established by such a body, is bound by those rules, and those rules impose obligations of professional confidentiality. Generally, a binding rule is one that will attract a sanction or adverse consequence if breached.

**Collection — conducting research; compiling or analysing statistics; management, funding or monitoring of a health service**

D.10 This permitted health situation applies when an organisation is collecting health information about an individual, if the collection is necessary for research relevant to public health or public safety, the compilation or analysis of statistics relevant to public health or public safety, or the management, funding or monitoring of a health service, and:

- the particular purpose cannot be served by collecting de-identified information
- it is impracticable to obtain the individual’s consent, and
- the collection is either:
  - required by or under an Australian law (other than the Privacy Act)
  - in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation, or
  - in accordance with guidelines approved under s 95A (s 16B(2)).

D.11 The terms ‘necessary’, ‘de-identified’, ‘consent’ and ‘required by or under an Australian law’ are discussed in Chapter B (Key concepts). Collection in accordance with rules of a competent health or medical body is discussed in paragraph D.9 of this chapter.

D.12 This permitted health situation overlaps with another exception stated in APP 3.4(a), namely the collection of sensitive information (which includes health information) as required or authorised by or under law or a court/tribunal order.

**Public health or public safety**

D.13 The phrase ‘relevant to public health or public safety’ is not defined in the Privacy Act. Illustrative examples include research or the compilation or analysis of statistics.
relating to communicable diseases, cancer, heart disease, mental health, injury control and prevention, diabetes and the prevention of childhood diseases.

**Management, funding or monitoring of a health service**

D.14 Examples of where health information about an individual may be collected for the ‘management, funding or monitoring of a health service’ include collection by:

- a quality assurance body, of data about the quality of a health service provided by a nursing home or hostel
- an oversight body, of information from a private hospital about an incident occurring in an individual’s health treatment
- a health insurer, of information relevant to possible fraud or an incorrect payment.

**De-identified information**

D.15 An organisation should consider whether the purposes listed in s 16B(2)(a) can be achieved by collecting de-identified information, rather than personal information. If they can, this permitted health situation will not apply.

**Impracticable to obtain consent**

D.16 The following are given as examples of where it may be impracticable for an organisation to obtain an individual’s consent to the collection of health information for one of the purposes listed in this permitted health situation:

- the integrity or validity of health research could be impaired, for example, because the organisation is conducting a participant observation study and obtaining the consent of participants may alter their behaviour and the research results. Consideration could be given to consulting a human research ethics committee as to whether obtaining consent would have this effect
- where obtaining the individual’s consent would adversely impact an investigation or monitoring activity
- there are no current contact details for the individual and the organisation has insufficient information to obtain up-to-date contact details.

D.17 It is the responsibility of an organisation relying on this permitted health situation to be able to justify why it would be impracticable to obtain an individual’s consent. Incurring some expense or doing extra work to obtain consent would not by itself make it impracticable to obtain consent.
Guidelines approved under s 95A

D.18 The ‘guidelines approved under s 95A’ are issued by the National Health and Medical Research Council (NHMRC) or a ‘prescribed authority’, and approved by the Information Commissioner.1

Disclosure of personal information collected under this permitted health situation

D.19 An organisation that collects personal information under this permitted health situation, must take reasonable steps to ensure that the information is de-identified before it is disclosed (APP 6.4 (Chapter 6)).

Use or disclosure — conducting research; compiling or analysing statistics

D.20 This permitted health situation applies when an organisation is using or disclosing health information about an individual, if the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety, and:

- it is impracticable to obtain the individual’s consent to the use or disclosure
- the use or disclosure is conducted in accordance with guidelines approved under s 95A, and
- in the case of disclosure — the organisation reasonably believes that the recipient of the information will not disclose the information, or personal information derived from that information (s 16B(3)).

D.21 The terms ‘necessary’ and ‘reasonably believes’ are discussed in Chapter B (Key concepts); ‘relevant to public health or public safety’ is discussed in paragraph D.13; ‘impracticable to obtain an individual’s consent’ is discussed in paragraph D.16–D.17; and ‘guidelines approved under s 95A’ is discussed in paragraph D.18.

D.22 When considering whether a use or disclosure is ‘necessary’ under this permitted health situation, an organisation should consider whether the research or statistical compilation or analysis could be undertaken using or disclosing de-identified information. If so, the use or disclosure of personal information would not be considered necessary. De-identification is discussed in Chapter B (Key concepts).

D.23 An organisation cannot rely on this permitted health situation to disclose health information unless it reasonably believes that the recipient will not disclose the information or personal information derived from that information. It is the responsibility of the organisation to be able to justify its reasonable belief.

1 See National Health and Medical Research Council (NHMRC), Guidelines approved under Section 95A of the Privacy Act 1988, NHMRC website <www.nhmrc.gov.au>.
Use or disclosure — necessary to prevent a serious threat to the life, health or safety of a genetic relative

D.24 This permitted health situation applies when an organisation is using or disclosing genetic information about an individual, if:

- the organisation has obtained the information in the course of providing a health service to the individual
- the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another individual who is a genetic relative of the individual
- the use or disclosure is conducted in accordance with guidelines approved under s 95AA, and
- in the case of disclosure — the recipient of the information is a genetic relative of the individual (s 16B(4)).

D.25 The terms ‘health service’, ‘necessary’ and ‘reasonably believes’ are discussed in Chapter B (Key concepts). The phrase ‘serious threat to life, health or safety’ is discussed in Chapter C (Permitted general situations).

D.26 ‘Genetic information’ is not defined in the Privacy Act. Genetic information about an individual is, however, included in the definition of ‘sensitive information’ (s 6(1)). Genetic information that is ‘about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual’ is also covered by the definition of ‘health information’ (s 6(1)).’ This permitted health situation applies to genetic information whether it is sensitive information or health information.

D.27 This permitted health situation applies to genetic information about an individual that an organisation has obtained from any source in the course of providing a health service to the individual. For example, the genetic information may include the results of a parentage test, or information from other sources that confirms a condition that is clinically apparent or that may predict the likelihood of an individual developing a condition.

D.28 A ‘genetic relative’ is defined in s 6(1) to mean an individual who is related by blood, including but not limited to a sibling, a parent or a descendant.

D.29 A serious threat to the life, health or safety of a genetic relative could include a threat to their physical or mental health. Whether a threat is serious can include consideration of both the likelihood of a threat occurring as well as the consequences if the threat materialises.
D.30 The ‘guidelines approved under s 95AA’ are issued by the NHMRC and approved by the Information Commissioner.2

Disclosure — responsible person for an individual

D.31 This permitted health situation applies when an organisation discloses health information about an individual, and:

- the organisation provides a health service to the individual
- the recipient of the information is a responsible person for the individual
- the individual is either physically or legally incapable of giving consent to the disclosure, or physically cannot communicate consent to the disclosure
- another individual providing the health service for the organisation (the ‘carer’) is satisfied that either the disclosure is necessary to provide appropriate care or treatment of the individual, or the disclosure is made for compassionate reasons
- the disclosure is not contrary to any wish expressed by the individual before the individual became unable to give or communicate consent of which the carer is aware or of which the carer could reasonably be expected to be aware, and
- the disclosure is limited to the extent reasonable and necessary to provide appropriate care or treatment of the individual or to fulfil the purpose of making a disclosure for compassionate reasons (s 16B(5)).

D.32 The terms ‘health service’, ‘consent’ (including capacity), ‘reasonable’ and ‘necessary’ are discussed in Chapter B (Key concepts). A ‘responsible person’ is defined in s 6AA and includes for example, a parent, adult child, spouse, partner, relative, guardian or nominee of an individual.

Incapacity to give consent

D.33 An individual may be ‘physically or legally incapable of giving consent’ if they cannot understand the nature of a consent decision, including the effect of giving or withholding consent, forming a view based on reasoned judgement and how to communicate a consent decision. Issues that may affect an individual’s capacity to give consent include:

- age
- physical or mental disability
- temporary or incremental incapacity, for example, during a psychotic episode, a temporary psychiatric illness, or because the person is unconscious, in severe distress, or suffering dementia
- limited understanding of English.

2 See National Health and Medical Research Council (NHMRC), Use and disclosure of genetic information to a patient’s genetic relatives under Section 95AA of the Privacy Act 1988: Guidelines for health practitioners in the private sector, NHMRC website <www.nhmrc.gov.au>.
D.34  An organisation should consider whether any such issue could be addressed by providing the individual with appropriate support to enable them to have capacity.

**Cannot communicate consent**

D.35  Where an individual physically cannot communicate consent to the disclosure, an organisation may disclose the individual’s personal information to a responsible person, without having to form a view as to the individual’s capacity (provided the other criteria in this permitted health situation are satisfied).

**Carer**

D.36  For the purposes of this permitted health situation, a ‘carer’ is an individual who is providing the health service for the organisation, such as a doctor, nurse, pharmacist, locum, visiting medical officer or qualified employee of the organisation. This is different to the use of the term ‘carer’ in other situations, as referring for example to a family member, close friend or other person who cares for the individual but does not provide a health service.

D.37  The carer must be satisfied that it is necessary to disclose the individual’s health information to a responsible person for the individual in order to provide appropriate care or treatment or for compassionate reasons. This requires a practical judgement by the carer. For example, the carer may be satisfied that ongoing care cannot be guaranteed without the disclosure occurring.

D.38  A compassionate reason for disclosure may include an update about the condition or progress of an unconscious patient to family members or an emergency contact.

**Wishes of the individual**

D.39  The disclosure must not be contrary to any wish expressed by the individual before they were unable to give or communicate consent. An individual’s wish or preference need not have been communicated in writing but may have been earlier communicated in anticipation of the individual no longer being able to make decisions about their health information, for example, where an individual has a degenerative condition which will lead to a lack of capacity.

D.40  An example of where a carer could be reasonably aware of an individual’s wishes is where they are noted on the individual’s medical record. An individual’s wishes may also have been expressed verbally during clinician-patient consultations, prior to the individual losing capacity to consent.

D.41  An individual’s wishes would be unlikely to override a guardianship order or other relevant legal authority, unless that guardianship order or other legal authority is limited or makes reference to the patient’s wishes. In these circumstances, an organisation should consider whether it can disclose the information under APP 6.2(b).
Chapter 1: Australian Privacy Principle 1 — Open and transparent management of personal information

Version 1.0, February 2014

Key points........................................................................................................................................2
What does APP 1 say? .................................................................................................................. 2
Implementing practices, procedures and systems to ensure APP compliance.......................... 2
Developing an APP Privacy Policy .......................................................................................... 4
Information that must be included in an APP Privacy Policy .................................................. 5
  Kinds of personal information collected and held................................................................. 6
  How personal information is collected and held................................................................. 6
  Purposes for which the entity collects, holds, uses and discloses personal information ......... 6
  Accessing and seeking correction of personal information .............................................. 7
  Complaints about a breach of the APPs or a binding registered APP code ..................... 7
  Likely overseas disclosures ......................................................................................... 8
Other matters for inclusion in an APP Privacy Policy .......................................................... 9
Making an APP Privacy Policy publicly available ................................................................. 9
Making an APP Privacy Policy available free of charge and in an appropriate form .......... 9
Making an APP Privacy Policy available in a requested form ............................................. 10
Key points

- APP 1 outlines the requirements for an APP entity to manage personal information in an open and transparent way.
- An APP entity must take reasonable steps to implement practices, procedures and systems that will ensure it complies with the APPs and any binding registered APP code, and is able to deal with related inquiries and complaints.
- An APP entity must have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information.
- An APP entity must take reasonable steps to make its APP Privacy Policy available free of charge and in an appropriate form (usually on its website).
- An APP entity must, upon request, take reasonable steps to provide a person or body with a copy of its APP Privacy Policy in the particular form requested.

What does APP 1 say?

1.1 The declared object of APP 1 is ‘to ensure that APP entities manage personal information in an open and transparent way’ (APP 1.1). This enhances the accountability of APP entities for their personal information handling practices and can build community trust and confidence in those practices.

1.2 APP 1 imposes three separate obligations upon an APP entity to:

- take reasonable steps to implement practices, procedures and systems that will ensure the entity complies with the APPs and any binding registered APP code, and is able to deal with related inquiries and complaints (APP 1.2)
- have a clearly expressed and up-to-date APP Privacy Policy about how the entity manages personal information (APP 1.3 and 1.4)
- take reasonable steps to make its APP Privacy Policy available free of charge in an appropriate form (APP 1.5) and, upon request, in a particular form (APP 1.6).

1.3 APP 1 lays down the first step in the information lifecycle – planning and explaining how personal information will be handled before it is collected. APP entities will be better placed to meet their privacy obligations under the Privacy Act if they embed privacy protections in the design of their information handling practices.

Implementing practices, procedures and systems to ensure APP compliance

1.4 APP 1.2 requires an APP entity to take reasonable steps to implement practices, procedures and systems relating to the entity’s functions or activities that will:

- ensure the entity complies with the APPs and any binding registered APP code (see Part III B), and
• enable the entity to deal with inquiries or complaints from individuals about the entity’s compliance with the APPs or such a code.

1.5 APP 1.2 imposes a distinct and separate obligation upon an APP entity, in addition to being a general statement of its obligation to comply with other APPs. The purpose of APP 1.2 is to require an entity to take proactive steps to establish and maintain internal practices, procedures and systems that ensure compliance with the APPs. The obligation is a constant one. An entity could consider keeping a record of the steps taken to comply with APP 1.2, to demonstrate that personal information is managed in an open and transparent way.

1.6 The requirement to implement practices, procedures and systems is qualified by a ‘reasonable steps’ test. The reasonable steps that an APP entity should take will depend upon circumstances that include:

• the nature of the personal information held. More rigorous steps may be required as the amount and sensitivity of personal information handled by an APP entity increases

• the possible adverse consequences for an individual if their personal information is not handled as required by the APPs. More rigorous steps may be required as the risk of adversity increases

• the nature of the APP entity. Relevant considerations include an entity’s size, resources and its business model. For example, the reasonable steps expected of an entity that operates through franchises or dealerships, or gives database and network access to contractors, may differ from the reasonable steps required of a centralised entity

• the practicability, including time and cost involved. A ‘reasonable steps’ test recognises that privacy protection must be viewed in the context of the practical options available to an APP entity. However, an entity is not excused from implementing particular practices, procedures or systems by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances.

1.7 The following are given as examples of practices, procedures and systems that an APP entity should consider implementing:

• procedures for identifying and managing privacy risks at each stage of the information lifecycle, including collection, use, disclosure, storage, destruction or de-identification

• security systems for protecting personal information from misuse, interference and loss and from unauthorised access, modification or disclosure (such as IT systems, internal access controls and audit trails) (see also Chapter 11 (APP 11))

• a commitment to conducting a Privacy Impact Assessment (PIA) for new projects in which personal information will be handled, or when a change is proposed to information handling practices. Whether a PIA is appropriate will depend on a
project’s size, complexity and scope, and the extent to which personal information will be collected, used or disclosed\(^1\)

- procedures for identifying and responding to privacy breaches, handling access and correction requests and receiving and responding to complaints and inquiries\(^2\)
- procedures that give individuals the option of not identifying themselves, or using a pseudonym, when dealing with the entity in particular circumstances (see also Chapter 2 (APP 2))
- governance mechanisms to ensure compliance with the APPs (such as designated privacy officers and regular reporting to the entity’s governance body)
- regular staff training and information bulletins on how the APPs apply to the entity, and its practices, procedures and systems developed under APP 1.2
- appropriate supervision of staff regularly handling personal information, and reinforcement of the entity’s APP 1.2 practices, procedures and systems
- mechanisms to ensure that agents and contractors in the service of, or acting on behalf of, the entity comply with the APPs
- a program of proactive review and audit of the adequacy and currency of the entity’s APP Privacy Policy and of the practices, procedures and systems implemented under APP 1.2.

### Developing an APP Privacy Policy

1.8 APP 1.3 requires an APP entity to have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information. At a minimum, a clearly expressed policy should be easy to understand (avoiding jargon, legalistic and in-house terms), easy to navigate, and only include information that is relevant to the management of personal information by the entity. As the policy will usually be available on the entity’s website (see paragraph 1.36), it should be written in a style and length that makes it suitable for web publication.\(^3\)

1.9 An APP entity should regularly review and update its APP Privacy Policy to ensure that it reflects the entity’s information handling practices. This review could, at a minimum, be undertaken as part of an entity’s annual planning processes. An entity could also:

- include a notation on the policy indicating when it was last updated
- invite comment on the policy to evaluate its effectiveness, and explain how any comments will be dealt with.


\(^3\) The OAIC has developed a guide to help mobile device application (app) developers embed better privacy practices in their products and services, see OAIC, *Mobile Privacy: A Better Practice Guide for Mobile APP Developers*, OAIC website <www.oaic.gov.au>.
1.10 An APP Privacy Policy should explain how the APP entity manages the personal information it collects, and the information flows associated with that personal information. This reflects the central object of APP 1, which is to ensure that entities manage personal information in an open and transparent manner. The policy is not expected to contain detail about all the practices, procedures and systems adopted to ensure APP compliance. The policy also differs from a collection notice provided to an individual under APP 5.1, which will provide specific information relevant to a particular collection of personal information (see Chapter 5 (APP 5)).

1.11 It is open to an APP entity to choose the style and format for its APP Privacy Policy, so long as the policy is clearly expressed, up-to-date and otherwise complies with the requirements of APP 1.

1.12 Where an APP Privacy Policy is made available online, using a layered approach to the provision of the information may assist an individual’s understanding of the information in the policy. A layered approach means providing a condensed version of the full policy to outline key information, with direct links to the more detailed information in the full policy.4

1.13 An APP Privacy Policy should be tailored to the specific information handling practices of an entity. For example, for a large APP entity where distinct business units handle personal information differently, it may be appropriate for the entity to have a set of policies to cover the different types of personal information handled or different information handling practices.

1.14 The APP Privacy Policy should be directed to the different audiences who may consult it. Primarily this will be individuals whose personal information is, or is likely to be, collected or held by the APP entity. If personal information relevant to particular classes of people or segments of the community is handled differently within the entity, this could be explained and signposted by headings. For example, different practices may be adopted in the entity for handling personal information relating to young people or people with a disability.

**Information that must be included in an APP Privacy Policy**

1.15 APP 1.4 contains a non-exhaustive list of information that an APP entity must include in its APP Privacy Policy:

- the kinds of personal information collected and held by the entity (APP 1.4(a))
- how personal information is collected and held (APP 1.4(b))
- the purposes for which personal information is collected, held, used and disclosed (APP 1.4(c))
- how an individual may access their personal information and seek its correction (APP 1.4(d))
- how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled (APP 1.4(e))

4 For an example of a layered approach, see OAIC, *Summary of the OAIC’s APP Privacy Policy*, OAIC website <www.oaic.gov.au>.
• whether the entity is likely to disclose personal information to overseas recipients (APP 1.4(f)), and if so, the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy (APP 1.4(g)).

1.16 Further guidance on each of these items is set out below.

Kinds of personal information collected and held

1.17 An APP Privacy Policy must describe in general terms the kinds of personal information an APP entity usually collects and holds (APP 1.4(a)). The terms ‘collects’ and ‘holds’ are discussed in Chapter B (Key concepts). For example, the policy may list personal information holdings as ‘contact details’, ‘employment history’, ‘educational qualifications’ and ‘complaint details’.

1.18 ‘Sensitive information’ collected or held by the entity could be separately listed (‘sensitive information’ is defined in s 6(1) and discussed in Chapter B (Key concepts)). For example, a policy may list sensitive information relating to ‘health information about an individual’, ‘racial or ethnic origin’, ‘criminal records’, ‘religious affiliation’ and ‘political opinions.’

How personal information is collected and held

1.19 An APP Privacy Policy must explain an APP entity’s usual approach to collecting personal information (APP 1.4(b)). For example, the policy may explain whether personal information is collected directly from individuals or from list purchases, competitions, or referrals from individuals or other entities.

1.20 The policy must describe an APP entity’s usual approach to holding personal information. This should include how the entity stores and secures personal information. For example, the policy may explain that personal information is stored by a third party data storage provider, or is combined or linked to other information held about an individual. The description of security measures should not provide details that jeopardise the effectiveness of those measures.

Purposes for which the entity collects, holds, uses and discloses personal information

1.21 An APP Privacy Policy must describe the purposes for which personal information is usually collected, held, used and disclosed (APP 1.4(c)). An APP entity is not expected to publish details of purposes that form part of normal internal business practices, such as auditing, business planning, billing, and de-identifying personal information. The description of purposes could indicate the range of people or entities to which personal information is usually disclosed, and details about an entity’s functions or activities that involve personal information that are contracted out. An organisation could also indicate if personal information is shared with a related body corporate.\(^5\) Discussion of the terms ‘purpose’, ‘collects’, ‘holds’, ‘uses’ and ‘discloses’ is in Chapter B (Key concepts).

\(^5\) Section 13B of the Privacy Act permits ‘related bodies corporate’ to share personal information in some circumstances. Related bodies corporate are discussed in Chapter B (Key concepts). The sharing of information between related bodies corporate is discussed in Chapter 3 (APP 3) and Chapter 6 (APP 6).
Accessing and seeking correction of personal information

1.22 An APP Privacy Policy must explain the procedure an individual can follow to gain access to or seek correction of personal information the APP entity holds (APP 1.4(d)). At a minimum, the policy should state:

- that individuals have a right to request access to their personal information and to request its correction (APPs 12 and 13), and
- the position title, telephone number, postal address and email address of a contact person for requests to access and correct personal information. An APP entity could establish a generic telephone number and email address that will not change with staff movements (for example privacy@agency.gov.au).  

1.23 If an APP entity wishes an individual to follow a particular procedure in requesting access to or correction of their personal information, the entity could publish that procedure and draw attention to it, for example, by providing a link in the entity’s APP Privacy Policy. However, an APP entity cannot require the individual to follow a particular procedure to make the access or correction request (see Chapter 12 (APP 12) and Chapter 13 (APP 13)).

1.24 An agency’s APP Privacy Policy could also refer to the Freedom of Information Act 1982 (FOI Act) and explain that the access and correction requirements in the Privacy Act operate alongside and do not replace other informal or legal procedures by which an individual can be provided with access to, or correction of, their personal information, including the FOI Act (this is discussed in more detail in Chapter 12 (APP 12) and Chapter 13 (APP 13)).

Complaints about a breach of the APPs or a binding registered APP code

1.25 An APP Privacy Policy must explain how an individual can complain about an APP entity’s breach of the APPs or a binding registered APP code (APP 1.4(e)). It is implicit in this requirement that an entity which is bound by a binding, registered APP code should clearly state that fact and name the code.

1.26 Details that should also be included in the APP Privacy Policy are the procedure and contact details for complaining directly to the APP entity (see for example, the generic contact details in paragraph 1.22) and, where applicable, the procedure for complaining to an external complaint body (such as an external dispute resolution scheme of which the entity is a member and that is recognised by the Information Commissioner). The policy could inform individuals of the different stages in complaint handling: that a complaint should first be made in writing to the entity, as required by s 40(1A), and that the entity should be given a reasonable time (usually 30 days) to respond; the complaint may then be taken to a recognised external dispute resolution scheme of which the entity is a member; and lastly that the complaint may be taken to the OAIC.

---

6 The OAIC has published guidance for agencies about developing their access to information webpages. This includes recommendations about adopting a new 'Access to information' icon. This guidance may assist agencies in developing online access and correction processes, which could then be explained in the APP Privacy Policy under APP 1.4(d). See OAIC, Guidance for agency websites: ‘Access to information’ web page, OAIC website <www.oaic.gov.au>.

7 Further information about external dispute resolution schemes recognised by the Information Commissioner is available in OAIC, Guidelines for recognising External Dispute Resolution Schemes, OAIC website <www.oaic.gov.au>.

1.27 The policy could refer to other complaint avenues that operate alongside the Privacy Act. For example, banks are required to provide information to customers about complaint handling and dispute resolution in relation to the bank’s obligations under the *Corporations Act 2001*, the Code of Banking Practice, and the Electronic Funds Transfer Code of Conduct. In these circumstances, the APP Privacy Policy could note the different procedures for privacy and non-privacy complaints (or link to other explanatory material the APP entity has published).

**Likely overseas disclosures**

1.28 An APP Privacy Policy must set out whether personal information is likely to be disclosed to overseas recipients and the countries in which such recipients are likely to be located ‘if it is practicable to specify those countries in the policy’ (APP 1.4(f) and 1.4(g)). This includes a likely disclosure to a related body corporate located overseas, and the country in which that body is located. An APP entity can be regarded as likely to disclose personal information to an overseas recipient if it is the entity’s current practice or it has established plans to do so.

1.29 An APP entity is required to set out in the policy only likely disclosures of personal information to overseas recipients, and not likely uses of personal information by the entity. For example, routing personal information, in transit, through a server located outside Australia would usually be considered a ‘use’.\(^8\) Similarly, it would also be a use and not a disclosure for an entity to make personal information accessible to an overseas office of the entity, such as a consular office.\(^9\) For further discussion of the requirements applying to a cross-border disclosure of personal information, and what is considered a disclosure, see Chapter 8 (APP 8).

1.30 An example of when it may be impracticable to specify the countries in which overseas recipients of personal information are likely to be located is where personal information is likely to be disclosed to numerous overseas recipients and the burden of determining where those recipients are likely to be located is excessively time-consuming, costly or inconvenient in all the circumstances. However, an APP entity is not excused from specifying the countries by reason only that it would be inconvenient, time-consuming or impose some cost to do so. As in other examples, it is the responsibility of the entity to be able to justify that this is impracticable.

1.31 If personal information is disclosed to numerous overseas locations, one practical option may be to list those countries in an appendix to the APP Privacy Policy rather than in the body of the policy. Another option in these circumstances may be to include a link in the APP Privacy Policy to a regularly updated list of those countries, accessible from the APP entity’s website. Where it is not practicable to specify the countries, the entity could instead identify general regions (such as European Union countries).

1.32 This requirement to describe overseas disclosure practices in an APP Privacy Policy complements the obligation on an APP entity under APP 5.2(j) and (i) to notify an individual when personal information is being collected if the personal information is likely to be disclosed to overseas recipients and the location of those recipients (see Chapter 5 (APP 5)).

---

\(^8\) Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.

\(^9\) Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.
Other matters for inclusion in an APP Privacy Policy

1.33 The list of matters that must be included in an APP Privacy Policy, as discussed above, is not exhaustive. The policy should contain sufficient information to describe how the APP entity manages personal information.

1.34 The following are examples of other information that could be included:

- any exemptions under the Privacy Act that apply to personal information held by the entity or to any of its acts or practices
- whether the APP entity retains a record of personal information about all individuals (or categories of persons) with whom it deals
- who, other than the individual, can access personal information, and the conditions for access
- the entity’s process or schedule for updating its APP Privacy Policy, and how changes will be publicised
- if the entity interacts with and collects personal information about a vulnerable segment of the community (such as children), the criteria that will be applied and the procedure that will be followed in collecting and holding that personal information
- the situations in which a person can deal with the entity by not identifying themselves or by using a pseudonym (see APP 2, Chapter 2)
- information retention or destruction practices or obligations that are specific to the entity.

Making an APP Privacy Policy publicly available

Making an APP Privacy Policy available free of charge and in an appropriate form

1.35 APP 1.5 requires an APP entity to take reasonable steps to make its APP Privacy Policy available free of charge, and in an appropriate form. This furthers the objective of APP 1 of ensuring that personal information is managed in an open and transparent way.

1.36 An APP entity is generally expected to make its policy available by publishing it on its website (see Note to APP 1.5). The information in the policy may be provided using a layered approach (see paragraph 1.12 above). The policy should be prominently displayed, accessible and easy to download. For example, a prominent link or privacy icon, displayed on each page of the entity’s website, could provide a direct link to the APP Privacy Policy. If it is foreseeable that the policy may be accessed by individuals with special needs (such as individuals with a vision impairment, or individuals from a non-English speaking background), appropriate accessibility measures should be put in place. Agencies are also required to comply with any applicable government accessibility requirements.10

---

1.37 Online publication may not be appropriate in some circumstances, for example, where the APP entity does not have an online presence or, where individuals who regularly interact with the entity may not have internet access. In these circumstances, options that an entity should consider include:

- displaying the policy on a stand at the entity’s premises, so that it can be seen by members of the public
- distributing a printout of the policy on request
- including details about how to access the policy at the bottom of all correspondence to individuals
- where the entity interacts with individuals by telephone, informing them during the telephone call of how the policy may be accessed in a particular form.

**Making an APP Privacy Policy available in a requested form**

1.38 APP 1.6 requires an APP entity, upon request, to take reasonable steps to provide a person or body with a copy of its APP Privacy Policy in the form requested. This should be done as soon as reasonably practicable after the request is received.

1.39 The reference to a ‘body’ requesting a copy of a policy makes it clear that a request may be made other than by an individual or entity that is subject to the Privacy Act.

1.40 An APP entity can decline to provide a copy of its APP Privacy Policy in a particular form if it would not be reasonable in the circumstances to meet the request. The steps that are reasonable will depend upon:

- other steps taken by the entity to make its policy publicly available and accessible
- the practicability, including time and cost involved. However, an entity is not excused from providing a copy in a particular form by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances
- the sensitivity of the personal information held. More rigorous steps may be required where the entity holds ‘sensitive information’ (defined in s 6(1) and discussed in Chapter B (Key concepts)) or information of a sensitive nature
- whether the entity has unique or unusual information handling practices
- any reasons given by the body or person for requesting the policy in a particular form
- any special needs of the body or person requesting the policy. For example, it may be reasonable to provide the policy in a form that can be accessed via assistive technology where this meets the requester’s special needs.

1.41 Inherent in the obligation to take ‘reasonable steps’ is an expectation that an APP Privacy Policy will usually be made available free of charge. The cost of doing so should be treated as part of an APP entity’s normal operating costs. If a charge is imposed in special circumstances, the reason for the charge and the basis of calculation should be clearly communicated and explained before the policy is made available in the requested form, and the charge should be calculated at the lowest reasonable cost.
1.42 If a request for access in a particular form is declined, the APP entity should explain this decision to the person or body making the request. The entity should be prepared to undertake reasonable consultation with the requester about the request.
Chapter 2: Australian Privacy Principle
2 — Anonymity and pseudonymity

Version 1.0, February 2014

Key points............................................................................................................................................................................. 2
What does APP 2 say?............................................................................................................................................................. 2
The difference between anonymity and pseudonymity ................................................................................................. 2
  Anonymity............................................................................................................................................................................. 2
  Pseudonymity....................................................................................................................................................................... 3
Why anonymity and pseudonymity are important ......................................................................................................... 3
Providing anonymous and pseudonymous options ....................................................................................................... 4
Requiring identification – required or authorised by law ................................................................................................. 5
Requiring identification – impracticability....................................................................................................................... 6
Key points

- APP 2 provides that individuals must have the option of dealing anonymously or by pseudonym with an APP entity.

- An APP entity is not required to provide those options where:
  - the entity is required or authorised by law or a court or tribunal order to deal with identified individuals, or
  - it is impracticable for the entity to deal with individuals who have not identified themselves.

- Anonymity means that an individual dealing with an APP entity cannot be identified and the entity does not collect personal information or identifiers.

- A pseudonym is a name, term or descriptor that is different to an individual’s actual name. Where applicable, an APP entity must ensure that individuals are made aware of their opportunity to deal anonymously or by pseudonym with the entity.

What does APP 2 say?

2.1 APP 2 provides that individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

2.2 That principle does not apply in relation to a particular matter if:

- the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves (APP 2.2(a)), or
- it is impracticable for the APP entity to deal with individuals who have not identified themselves or used a pseudonym (APP 2.2(b)).

2.3 ‘Anonymity’ and ‘pseudonymity’ are different concepts. APP 2 requires that both options be made available to individuals dealing with an APP entity unless one of the two exceptions applies. Both options must also be made available each time an individual interacts with the entity, that is, when a person is ‘dealing with an APP entity in relation to a particular matter’ (APP 2.1). Similarly, the exceptions (‘required or authorised by law’ and ‘impracticability’) apply to the particular dealing between an individual and the entity.

The difference between anonymity and pseudonymity

Anonymity

2.4 Anonymity requires that an individual may deal with an APP entity without providing any personal information or identifiers. The entity should not be able to identify the individual at the time of the dealing or subsequently.
2.5 Examples of anonymous dealings include an unidentified individual telephoning an APP entity to inquire generally about its goods or services, and an individual completing a retail transaction and paying for goods in cash.

Pseudonymity

2.6 Pseudonymity requires that an individual may deal with an APP entity by using a name, term or descriptor that is different to the person’s actual name. Examples include an email address that does not contain the person’s actual name, a user name that a person uses when participating in an online forum, or an artist who uses a ‘pen-name’ or ‘screen-name’.

2.7 The use of a pseudonym does not necessarily mean that an individual cannot be identified. The individual may choose to divulge their identity, or to volunteer personal information necessary to implement a particular transaction, such as credit information or an address at which goods can be delivered. Similarly, an APP entity may have in place a registration system that enables a person to participate by pseudonym in a moderated online discussion forum, on condition that the person is identifiable to the forum moderator or the entity.

2.8 An APP entity should bear in mind that the object of APP 2 is to provide individuals with the opportunity to deal with the entity without revealing their identity. Personal information should only be linked to a pseudonym if this is required or authorised by law, it is impracticable for the entity to act differently, or the individual has consented to providing or linking the additional personal information. An entity could also restrict access to personal information that is linked to a pseudonym to authorised personnel (for a discussion of the security requirements for personal information, see Chapter 11 (APP 11)).

Why anonymity and pseudonymity are important

2.9 Anonymity and pseudonymity are important privacy concepts. They enable individuals to exercise greater control over their personal information and decide how much personal information will be shared or revealed to others.

2.10 An individual may prefer to deal anonymously or pseudonymously with an APP entity for various reasons, including:

- a preference not to be identified or to be ‘left alone’
- to avoid subsequent contact such as direct marketing from that entity or other entities
- to keep their whereabouts secret from a former partner or family member
- to access services (such as counselling or health services) without this becoming known to others
- to express views in the public arena without being personally identified.

2.11 There can be wider benefits too:
• individuals may be more likely to inquire about products and services that an APP entity provides if able to do so without being identified, meaning the community is better informed
• freedom of expression is enhanced if individuals can express controversial or minority opinions without fear of reprisal
• the risk of identity fraud is minimised when less personal information is collected, linked and stored by entities
• an APP entity can lessen its compliance burden under the APPs by reducing the quantity of personal information it collects
• client feedback may be more forthcoming and robust if individuals have the option of making an unattributed compliment or complaint to an entity.

Providing anonymous and pseudonymous options

2.12 It is implicit in APP 2 that an APP entity should ensure that, if applicable, individuals are made aware of their opportunity to deal anonymously or by pseudonym with the entity. If anonymity or pseudonymity is the default setting, this does not apply.

2.13 The steps an APP entity should take to draw both options to the attention of individuals will depend on the nature of the dealing between the entity and an individual. For example, an entity’s APP Privacy Policy could explain the circumstances in which an individual may deal anonymously or by pseudonym with the entity, and the procedures for doing so (see Chapter 1 (APP 1)). The policy could go further and explain how the entity manages pseudonyms and any linked personal information, and if there will be any consequences for an individual if they deal with the entity anonymously or through a pseudonym (for example, where only a limited service can be provided).

2.14 Other measures that could be adopted by an APP entity to facilitate anonymous and pseudonymous dealings include:

• if the entity provides a facility on its website for online communication, stating prominently that an individual may use that facility without providing personal information
• if telephone calls to the entity are routed through an automated message, informing callers in that message that they are not required to provide personal information
• if individuals can contact the entity by using an online or printed form, stating on the form that personal identification boxes (such as name and address) are not mandatory fields
• if the entity solicits public submissions or comments from individuals, allowing participants to use a pseudonym that will be published, even if the individual’s name is supplied confidentially to the entity
• in other dealings between the entity and individuals, informing individuals at the beginning of a dealing that they may interact anonymously or by pseudonym.
2.15 APP 2.2(a) provides that an individual may not have the option of dealing anonymously or by pseudonym with an APP entity if the entity ‘is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves’. The meaning of ‘required or authorised by or under an Australian law or court/tribunal order’ is discussed in Chapter B (Key concepts).

2.16 If an APP entity is ‘required’ by a law or order to deal only with an identified individual it will be necessary for the individual to provide adequate identification. If an entity is ‘authorised’ by a law or order to deal with an identified individual, the entity can require the individual to identify themselves, but equally will have discretion to allow the individual to deal with the entity anonymously or pseudonymously. The nature of any discretion, and whether it is appropriate to rely upon it, will depend on the terms of the law or order and the nature of the dealing.

2.17 The following are given as examples of where a law or order may require or authorise an APP entity to deal only with an identified individual:

- processing an individual’s application for an identity document (such as a passport, licence or security pass)
- issuing a tax file number to an individual
- paying a social security or healthcare benefit to an eligible individual
- providing assistance to an individual who has been diagnosed with a disease that must be recorded and notified under a public health law
- providing assistance to a suspected victim of child abuse, whose injury is covered by a mandatory reporting requirement
- opening a bank account for an individual, or providing other financial services where legislation requires the individual to be identified
- supplying a pre-paid mobile phone to an individual where legislation requires identification
- discussing the individual’s personal information with them, such as the individual’s account information
- giving access to the individual’s personal information under the Privacy Act or Freedom of Information Act 1982.\(^1\)

2.18 An APP entity that relies on APP 2.2(a) to collect personal information should ensure that the collection does not go beyond the requirements of the law or court or tribunal order. For example, the legal requirement may be satisfied by sighting, but not collecting, the personal information, or by collecting an individual’s name but not their address, gender or date of birth. APP 3 imposes a complementary requirement, that

---

\(^1\) It may be practicable to deal with a pseudonymous request for personal information under the Privacy Act or the Freedom of Information Act 1982 if the individual has previously transacted under that pseudonym and can establish their identity as that individual (see APP 12, Chapter 12).
generally an entity can only collect personal information that is reasonably necessary for one or more of its functions or activities.

**Requiring identification – impracticability**

2.19 APP 2.2(b) provides that an individual may not have the option of dealing anonymously or by pseudonym with an APP entity if ‘it is impracticable for the APP entity to deal with individuals who have not identified themselves’.

2.20 The following are given as examples of where it may be impracticable to deal with an individual who is not identified:

- in dispute resolution, it may be impracticable to investigate and resolve an individual’s particular complaint about how their case was handled or how the staff of an APP entity behaved unless the complainant provides their name or similar information
- where an entity is delivering purchased goods to an individual, it may not be able to do so without knowing that individual’s address, or their name (for example, where the individual needs to sign for delivery of the goods).

2.21 In special circumstances it may be open to an APP entity to rely on the ‘impracticability’ exception where the burden of the inconvenience, time and cost of dealing with an unidentified or pseudonymous individual, or of changing an existing system or practice to include the option of anonymous or pseudonymous dealings, would be excessive in all the circumstances. However, this is more likely to be a transitional rather than an ongoing justification. Unless an entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves (see paragraphs 2.15–2.18 above), entities are expected to design and maintain information collection systems that incorporate anonymous and pseudonymous options.

2.22 An APP entity that is relying on APP 2.2(b) should not collect more personal information than is required to facilitate the dealing with an individual (see paragraph 2.18 above).
Chapter 3: Australian Privacy Principle
3 — Collection of solicited personal information

Version 1.0, February 2014

Key points........................................................................................................................................ 3
What does APP 3 say?.................................................................................................................... 3
‘Solicit’ and ‘collect’ ...................................................................................................................... 4
Collecting for an APP entity’s ‘functions or activities’ .................................................................. 5
  Identifying the functions or activities of an agency................................................................. 5
  Identifying the functions or activities of an organisation....................................................... 6
Collecting personal information that is ‘directly related’ to an agency’s functions or activities ................................................................................................................................. 6
Collecting personal information that is ‘reasonably necessary’ for an APP entity’s functions or activities ........................................................................................................................................ 6
Collecting sensitive information .................................................................................................. 8
  Collecting sensitive information as required or authorised by law......................................... 8
  Collecting sensitive information where a permitted general situation exists........................... 8
    Locating a person reported as missing.................................................................................. 9
    Reasonably necessary for establishing, exercising or defending a legal or equitable claim .............................................................................................................................................. 9
    Reasonably necessary for a confidential alternative dispute resolution process ................. 10
    Necessary for a diplomatic or consular function or activity............................................... 10
Collecting sensitive information where a permitted health situation exists............................. 10
  Providing a health service........................................................................................................... 11
  Conducting research; compiling or analysing statistics; management, funding or monitoring of a health service .................................................................................................................. 11
Collecting sensitive information for an enforcement related activity........................................ 12
Collection of sensitive information by a non-profit organisation.............................................. 13
Collecting by lawful and fair means............................................................................................ 13
Collecting by lawful means ........................................................................................................ 14
Collecting by fair means ............................................................................................................ 14
Collecting directly from the individual...................................................................................... 15
Unreasonable or impracticable to collect directly from the individual...................................... 15
Consent by the individual — for agencies only.............................................................. 16
Required or authorised by law or a court or tribunal order — for agencies only ........ 16
Collecting personal information from a related body corporate .................................... 16
Key points

- APP 3 outlines when an APP entity may collect solicited personal information.
- An APP entity solicits personal information if it explicitly requests another entity to provide personal information, or it takes active steps to collect personal information.
- APP 3 deals with when an APP entity can collect personal information, and how an APP entity must collect personal information.
- For personal information (other than sensitive information), an APP entity that is:
  - an agency, may only collect this information where it is reasonably necessary for, or directly related to, the agency’s functions or activities
  - an organisation, may only collect this information where it is reasonably necessary for the organisation’s functions or activities.
- APP 3 contains different requirements for the collection of sensitive information compared to other types of personal information. Unless an exception applies, an APP entity may only collect sensitive information where the above conditions are met and the individual concerned consents to the collection.
- Personal information must only be collected by lawful and fair means.
- Personal information must be collected from the individual concerned, unless this is unreasonable or impracticable (additional exceptions apply to agencies).

What does APP 3 say?

3.1 The APPs distinguish between an APP entity collecting solicited personal information (APP 3) and receiving unsolicited personal information (APP 4).

3.2 APP 3 deals with two aspects of collecting solicited personal information:
- when an APP entity can collect personal information — the requirements vary according to whether the personal information is or is not sensitive information, and whether the APP entity is an agency or an organisation
- how an APP entity must collect personal information — the same requirements apply to all APP entities and to all kinds of personal information.

3.3 In summary, the principles that apply are:
- an agency may only solicit and collect personal information that is reasonably necessary for, or directly related to, one or more of its functions or activities (APP 3.1)
- an organisation may only solicit and collect personal information that is reasonably necessary for one or more of its functions or activities (APP 3.2)
- in addition to the above requirements, an APP entity may only solicit and collect sensitive information if the individual consents to the sensitive information being collected, unless an exception applies (APP 3.3)
• an APP entity must solicit and collect personal information:
  o only by lawful and fair means (APP 3.5), and
  o directly from the individual, unless an exception applies (APP 3.6).

‘Solicit’ and ‘collect’

3.4 APP 3 applies when an APP entity ‘solicits’ and ‘collects’ personal information, while APP 4 applies when an APP entity receives personal information that it ‘did not solicit’. Examples of solicited personal information collected by an entity are given in paragraph 3.7 below; examples of unsolicited personal information received by an entity are given in Chapter 4 (APP 4).

3.5 An APP entity ‘collects’ personal information ‘only if the entity collects the personal information for inclusion in a record or generally available publication’ (s 6(1)). This concept applies broadly, and includes gathering, acquiring or obtaining personal information from any source and by any means. In practice, all personal information that is held by an entity will generally be treated as information that was collected by the entity. ‘Collect’ is discussed in more detail in Chapter B (Key concepts).

3.6 An APP entity ‘solicits’ personal information ‘if the entity requests another entity to provide the personal information, or to provide a kind of information in which that personal information is included’ (s 6(1)). The request may be made to an agency, organisation, individual or a small business operator. A ‘request’ is an active step taken by an entity to collect personal information, and may not involve direct communication between the entity and an individual.

3.7 Examples of solicited personal information collected by an APP entity include the following, where they are collected for inclusion in a record or generally available publication:

• personal information provided by an individual in response to a request, direction or order
• personal information about an individual provided by another entity in response to a request, direction, order or arrangement for sharing or transferring information between both entities
• personal information provided at a business meeting, where it relates to the subject matter of the meeting, including business cards exchanged at the meeting
• a completed form or application submitted by an individual
• a complaint letter sent in response to a general invitation on an APP entity’s website to individuals to complain to the entity
• an employment application sent in response to either a job advertisement published by an entity or an expression of interest register maintained by the entity
• a form completed to enter a competition being conducted by an entity

1 An ‘entity’ is defined in s 6(1) to mean an agency, organisation or small business operator. ‘Organisation’ is defined in s 6C to include an individual.
• personal information provided to a ‘fraud hotline’ that is designed to capture ‘tip-offs’ from the public
• an entry in an APP entity’s visitors book
• a record of a credit card payment
• CCTV footage that identifies individuals.

Collecting for an APP entity’s ‘functions or activities’

3.8 An APP entity must only collect personal information which is reasonably necessary for one or more of the entity's functions or activities (APPs 3.1 and 3.2). Agencies may, in addition, collect personal information that is directly related to one or more of the agency's functions or activities.

3.9 Determining whether a particular collection of personal information is permitted involves a two-step process:

• identifying an APP entity’s functions or activities - different criteria apply for ascertaining the functions and activities of agencies and organisations
• determining whether the particular collection of personal information is reasonably necessary for (or, for agencies, directly related to) one of those functions or activities.

Identifying the functions or activities of an agency

3.10 An agency’s functions will be conferred either by legislation (including a subordinate legislative instrument) or an executive scheme or arrangement established by government. Identifying an agency’s functions involves examining the legal instruments that confer or describe the agency’s functions. These include:

• Acts and subordinate legislative instruments
• the Administrative Arrangements Order made by the Governor-General
• government decisions or ministerial statements that announce a new government function.

3.11 The activities of an agency will be related to its functions. The activities of an agency include incidental and support activities, such as human resource, corporate administration, property management and public relations activities.

3.12 One resource that describes an agency’s functions is that agency’s Information Publication Scheme (IPS) entry. Agencies to which the Freedom of Information Act 1982

---

2 See Chapter 9 (APP 9) for a discussion of particular issues relating to the lawful collection of government related identifiers by organisations.


4 An agency’s incidental functions (described in paragraph 3.11) are not required to be published in its IPS entry: see OAIC, Guidelines issued by the Australian Information Commissioner under s 93A of the Freedom of Information Act 1982 at [13.47]–[13.49], OAIC website <www.oaic.gov.au>.
(FOI Act) applies are required to publish on a website ‘details of the functions of the agency’. This forms part of the IPS established by the FOI Act (FOI Act, ss 8(2)(c), 8D(3)). The IPS entries of most agencies are readily accessible through a link on the homepage of the agency’s website. Another resource that describes agency functions and activities is the annual report of an agency, usually accessible from the agency’s website.

### Identifying the functions or activities of an organisation

3.13 An organisation’s functions or activities include:

- current functions or activities of the organisation
- proposed functions or activities the organisation has decided to carry out and for which it has established plans
- activities the organisation carries out in support of its other functions and activities, such as human resource, corporate administration, property management and public relations activities.

3.14 The functions and activities of an organisation will commonly be described (though not necessarily exhaustively) on a website, in an annual report, and in corporate brochures, advertising, product disclosure statements and client and customer letters and emails.

3.15 The functions and activities of an organisation (for which it may collect personal information under APP 3) are limited to those in which it may lawfully engage.

### Collecting personal information that is ‘directly related’ to an agency’s functions or activities

3.16 An agency may collect personal information that is ‘directly related to’ one or more of the agency’s functions or activities (APP 3.1). To be ‘directly related to’, a clear and direct connection must exist between the personal information being collected and an agency function or activity.

### Collecting personal information that is ‘reasonably necessary’ for an APP entity’s functions or activities

3.17 An APP entity may collect personal information that is ‘reasonably necessary for’ a function or activity of the entity (APP 3.1 and APP 3.2). An APP entity may also collect the personal information of an individual (other than sensitive information) from a related body corporate (s 13B(1)(a)).

3.18 The ‘reasonably necessary’ test is an objective test: whether a reasonable person who is properly informed would agree that the collection is necessary. It is the responsibility of an APP entity to be able to justify that the particular collection is reasonably necessary. ‘Reasonably necessary’ is also discussed in Chapter B (Key concepts).

3.19 Factors relevant to determining whether a collection of personal information is reasonably necessary for a function or activity include:

---

5 An APP entity may also collect the personal information of an individual (other than sensitive information) from a related body corporate (s 13B(1)(a)).
3.20 The following are instances in which the OAIC has previously ruled that a collection of personal information was not reasonably necessary for an entity’s function or activity:

- a job applicant being asked to advise if they had suffered a work-related injury or illness, when this was not relevant to the position being advertised\(^6\)
- a person applying to open a bank account being asked to complete a standard form application that included a question about marital status, when this had no bearing on the applicant’s eligibility to open an account\(^7\)
- a medical practitioner photographing a patient for the patient’s medical file, when this was not necessary to provide a health service.\(^8\)

3.21 Other examples of personal information collection that may not be reasonably necessary for an entity’s functions or activities include:

- collecting personal information about a group of individuals, when information is only required for some of those individuals
- collecting more personal information than is required for a function or activity. For example, collecting all information entered on an individual’s driver licence when the purpose is to establish if the individual is aged 18 years or over
- collecting personal information that is not required for a function or activity but is being entered in a database in case it might be needed in the future (this is to be distinguished from the situation where personal information is required for a function or activity, but is not being used immediately)
- an organisation collecting personal information for or on behalf of a related body corporate where the collection of that personal information is not reasonably necessary for the organisation’s own functions or activities.


\(^7\) *D v Banking Institution* [2006] PrivCmrA 4, Australasian Legal Information Institute website <www.austlii.edu.au>.

Collecting sensitive information

3.22  APP 3.3 imposes an additional requirement for collecting sensitive information about an individual. Unless an exception applies, an APP entity must:

- satisfy the criteria above, i.e. the collection of the sensitive information must be reasonably necessary for (or, for agencies, directly related to) one or more of the entity’s functions or activities, and
- the individual about whom the sensitive information relates must consent to the collection (APP 3.3(a)).

3.23  ‘Sensitive information’ is defined in s 6(1), and is discussed in more detail in Chapter B (Key concepts). ‘Consent’ is defined in s 6(1) as ‘express consent or implied consent’, and is discussed in more detail in Chapter B (Key concepts). The four key elements of consent are:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent.

3.24  APP 3.4 lists five exceptions to the requirements of APP 3.3(a). These are considered below.

Collecting sensitive information as required or authorised by law

3.25  An APP entity may collect sensitive information if the collection ‘is required or authorised by or under an Australian law or a court/tribunal order’ (APP 3.4(a)). The meaning of ‘required or authorised by or under an Australian law or a court/tribunal order’ is discussed in more detail in Chapter B (Key concepts).

3.26  An example of where a law or order may require or authorise collection of sensitive information is the collection by an authorised officer under the Migration Act 1958 of personal identifiers (that may include biometric information) from a non-citizen who is in immigration detention.9

Collecting sensitive information where a permitted general situation exists

3.27  An APP entity may collect sensitive information if a ‘permitted general situation’ exists in relation to the collection (APP 3.4(b)).

3.28  Section 16A lists seven permitted general situations (two of which apply only to agencies). The seven situations are set out below, and are discussed in Chapter C (Permitted general situations), including the meaning of relevant terms.

Lessening or preventing a serious threat to life, health or safety

3.29  An APP entity may collect sensitive information if:

---

9 See Migration Act 1958, ss 5A, 261AA.
• it is unreasonable or impracticable to obtain the individual’s consent to the collection, and
• the entity reasonably believes the collection is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety (s 16A(1), Item 1).

3.30 Examples of where this permitted general situation might apply are:
• collecting health information about an individual who is seriously injured, requires treatment and, due to their injuries, cannot give informed consent, on the basis that it is impracticable to obtain the individual’s consent
• collecting sensitive information about a parent that is required to provide assistance to a child who may be at risk of physical or sexual abuse by the parent, on the basis that it would be unreasonable to obtain the parent’s consent.

Taking appropriate action in relation to suspected unlawful activity or serious misconduct

3.31 An APP entity may collect sensitive information if the entity:
• has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity’s functions or activities has been, is being, or may be engaged in, and
• reasonably believes that the collection is necessary in order for the entity to take appropriate action in relation to the matter (s 16A(1), Item 2).

3.32 Examples of where this permitted general situation might apply are the collection of sensitive information by:
• an APP entity that is investigating fraudulent conduct by a professional adviser or a client in relation to the entity’s functions or activities
• an agency that is investigating a suspected serious breach by a staff member of the Australian Public Service Code of Conduct.

Locating a person reported as missing

3.33 An APP entity may collect sensitive information if:
• the entity reasonably believes that the collection is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing, and
• the collection complies with rules made by the Information Commissioner under s 16A(2) (s 16A(1), Item 3).

Reasonably necessary for establishing, exercising or defending a legal or equitable claim

3.34 An APP entity may collect sensitive information if the collection is reasonably necessary to establish, exercise or defend a legal or equitable claim (s 16A(1), Item 4).

3.35 An example of where this permitted general situation might apply is an insurer collecting health information about an individual who has made an insurance
compensation claim but is suspected of misrepresenting their claim or the extent of their injuries.\textsuperscript{10}

\textit{Reasonably necessary for a confidential alternative dispute resolution process}

3.36 An APP entity may collect sensitive information if the collection is reasonably necessary for the purposes of a confidential alternative dispute resolution (ADR) process (s 16A(1), Item 5).

3.37 An example of where this permitted general situation might apply is an alternative dispute resolution practitioner making a record of a party recounting their version of events, where that account includes the disclosure of sensitive information about an individual who is directly or indirectly involved in the dispute. This permitted general situation will only apply where the parties to the dispute and the ADR provider are bound by confidentiality obligations.

\textit{Necessary for a diplomatic or consular function or activity}

3.38 An agency may collect sensitive information if the agency reasonably believes the collection is necessary for the agency’s diplomatic or consular functions or activities (s 16A(1), Item 6). This permitted general situation applies only to agencies, and not to organisations.

3.39 An example of where this permitted general situation might apply is where an agency with diplomatic or consular functions collects sensitive information about an individual who is overseas and in need of consular assistance because the individual has been hospitalised, is suffering a psychiatric illness, has been arrested or is missing.

\textit{Necessary for certain Defence Force activities outside Australia}

3.40 The Defence Force (as defined in s 6(1)) may collect sensitive information if it reasonably believes the collection to be necessary for a warlike operation, peacekeeping, civil aid, humanitarian assistance, a medical emergency, a civil emergency or disaster relief occurring outside Australia and the external Territories (s 16A(1), Item 7).

\textit{Collecting sensitive information where a permitted health situation exists}

3.41 An organisation may collect sensitive information if a ‘permitted health situation’ exists in relation to the collection (APP 3.4(c)). This exception applies only to organisations, and not to agencies.

3.42 Section 16B lists two permitted health situations that relate to the collection of health information by an organisation. The two situations are set out below, and are discussed in Chapter D (Permitted health situations), including the meaning of relevant terms.

Providing a health service

3.43 An organisation may collect health information about an individual if the health information is necessary to provide a health service to the individual, and either:

- the collection is required or authorised by or under an Australian law (other than the Privacy Act), or
- the health information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation (s 16B(1)).

3.44 An example of where this permitted health situation might apply is where a participant in the personally controlled electronic health record (e-health record) system collects health information included in a consumer’s e-health record as authorised by the Personally Controlled Electronic Health Records Act 2012.11

3.45 ‘Health information’ is defined in s 6(1) and discussed in more detail in Chapter B (Key concepts).

Conducting research; compiling or analysing statistics; management, funding or monitoring of a health service

3.46 An organisation may collect health information about an individual if the collection is necessary for research relevant to public health or public safety, the compilation or analysis of statistics relevant to public health or public safety, or the management, funding or monitoring of a health service, and:

- the particular purpose cannot be served by collecting de-identified information
- it is impracticable to obtain the individual’s consent, and
- the collection is either:
  - required by or under an Australian law (other than the Privacy Act)
  - in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation, or
  - in accordance with guidelines approved under s 95A (s 16B(2)).12

3.47 An example of where this permitted health situation might apply is an organisation conducting longitudinal research into heart disease and requiring health information about a large number of individuals from different data sources for research linkage. In this case, the collection must be required by an Australian law or carried out in accordance with the rules or guidelines referred to in s 16B(2).

3.48 ‘Health information’ is defined in s 6(1) and discussed in more detail in Chapter B (Key concepts).

---

11 See Personally Controlled Electronic Health Records Act 2012, ss 63, 64, 65, 66 and 68.
12 See National Health and Medical Research Council (NHMRC), Guidelines approved under Section 95A of the Privacy Act 1988, NHMRC website <www.nhmrc.gov.au>.
Collecting sensitive information for an enforcement related activity

3.49 An enforcement body may collect sensitive information where:

- if the body is the Immigration Department\(^{13}\), the Department reasonably believes that collecting the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the Department (APP 3.4(d)(i))

- for other enforcement bodies, the body reasonably believes that collecting the information is reasonably necessary for, or directly related to, one or more of the body’s functions or activities (APP 3.4(d)(ii)).

3.50 ‘Enforcement body’ is defined in s 6(1) as a list of specific bodies and is discussed in Chapter B (Key concepts). The list includes Commonwealth, State and Territory bodies that are responsible for policing, criminal investigations, and administering laws to protect the public revenue or to impose penalties or sanctions. Examples of Commonwealth enforcement bodies are the Australian Federal Police, Australian Crime Commission, Customs, the Integrity Commissioner,\(^{14}\) the Immigration Department, Australian Prudential Regulation Authority, Australian Securities and Investments Commission and AUSTRAC.

3.51 For an enforcement body to collect sensitive information using this exception, it must:

- for the Immigration Department, identify the ‘enforcement related activities’ it conducts or that are conducted on its behalf, and for other enforcement bodies, identify their ‘functions or activities’, and

- ‘reasonably believe’ that the collection is either ‘reasonably necessary for’ or ‘directly related to’ one or more of those functions or activities.

3.52 ‘Reasonably believes’ is discussed in more detail in Chapter B (Key concepts). Identifying the ‘functions or activities’ of an agency is discussed above at paragraphs 3.10–3.12, while ‘reasonable necessary for’ and ‘directly related to’ are discussed above at paragraphs 3.16–3.21.

3.53 ‘Enforcement related activities’ are defined in s 6(1) and discussed in Chapter B (Key concepts). Where applied to the Immigration Department, the activities could include assessing and enforcing compliance with visa and citizenship requirements, and detecting, preventing, investigating and prosecuting breaches of visa, immigration and citizenship laws. Non-enforcement related activities of the Department do not fall within this exception.\(^{15}\)

3.54 An example of where the Immigration Department may collect sensitive information from an individual using this exception is where it reasonably believes that

---

\(^{13}\) ‘Immigration Department’ is defined in s 6(1) as the Department administered by the Minister administering the Migration Act 1958 and is discussed in Chapter B (Key concepts).

\(^{14}\) ‘Integrity Commissioner’ is defined in s 6(1) as having the same meaning as in the Law Enforcement Integrity Commissioner Act 2006.

\(^{15}\) Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 76.
the sensitive information directly relates to the function of investigating whether a person has breached an immigration law.

Collection of sensitive information by a non-profit organisation

3.55 A non-profit organisation may collect sensitive information if:

- the information relates to the activities of the organisation, and
- the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities (APP 3.4(e)).

3.56 ‘Non-profit organisation’ is defined in s 6(1) as an organisation ‘that is a non-profit organisation; and that engages in activities for cultural, recreational, political, religious, philosophical, professional, trade or trade union purposes’. The term ‘cultural purposes’ includes both racial and ethnic purposes.

3.57 There are three criteria a non-profit organisation must meet to rely on this exception to collect sensitive information:

- firstly, the non-profit organisation can rely on this exception only when collecting sensitive information for an activity that is undertaken for one of the specified purposes in the definition of ‘non-profit organisation’ (s 6(1)). An organisation conducting activities for some other purpose cannot rely on this exception to collect sensitive information for that purpose
- secondly, the sensitive information that is collected must ‘relate’ to the activity that is being conducted for a specified purpose. A clear relationship, assessed objectively, must exist between the information collected and that activity. For example, the information may relate to a fundraising activity undertaken by a non-profit organisation to support its cultural, recreational, political, religious, philosophical, professional, trade or trade union purpose
- thirdly, the sensitive information must relate solely to a member of the organisation, or an individual who has regular contact with the organisation in connection with its activities. Collection of sensitive information about a relative of a member of the organisation would not be covered unless the relative was also a member or person in regular contact with the non-profit organisation.

3.58 An example of where a non-profit organisation may be permitted to collect sensitive information is where a religious organisation collects information about the views of its members on religious or moral issues.

Collecting by lawful and fair means

3.59 An APP entity must collect personal information ‘only by lawful and fair means’ (APP 3.5). This requirement applies to all APP entities.
Collecting by lawful means

3.60 The term ‘lawful’ is not defined in the Privacy Act. It is lawful for an organisation to destroy or de-identify unsolicited personal information if it is not unlawful to do so. That is, if the destruction or de-identification is not criminal, illegal or prohibited or proscribed by law. Unlawful activity does not include breach of a contract.

3.61 Examples of collection that would not be lawful include:

- collecting in breach of legislation, for example:
  - collecting via computer hacking\(^{16}\)
  - collecting using telephone interception or a listening device except under the authority of a warrant\(^{17}\)
  - requesting or requiring information in connection with, or for the purpose of, an act of discrimination\(^{18}\)
- collecting by a means that would constitute a civil wrong, for example, by trespassing on private property or threatening damage to a person unless information is provided
- collecting information contrary to a court or tribunal order, for example, contrary to an injunction issued against the collector.

Collecting by fair means

3.62 A ‘fair means’ of collecting information is one that does not involve intimidation or deception, and is not unreasonably intrusive.\(^{19}\) Whether a collection uses unfair means will depend on the circumstances. For example, it would usually be unfair to collect personal information covertly without the individual’s knowledge. However, this may be a fair means of collection if undertaken in connection with a fraud investigation.

3.63 The following are given as examples of where a collection of personal information may be unfair (some may also be unlawful):

- collecting from a file dumped by accident on a street, or from an electronic device which is lost or left unattended
- collecting from an individual who is traumatised, in a state of shock or intoxicated
- collecting in a way that disrespects cultural differences
- misrepresenting the purpose or effect of collection, or the consequences for the individual of not providing the requested information
- collecting by telephoning an individual in the middle of the night

\(^{16}\) For example, Criminal Code Act 1995, Part 10.7.

\(^{17}\) For example, Telecommunications (Interception) Act 1979 (Cth) s 7; Surveillance Devices Act 2004 (Cth) s 14.

\(^{18}\) See for example, the Disability Discrimination Act 1992, s 30 and the Sex Discrimination Act 1984, s 27.

\(^{19}\) Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 77.
• collecting by deception, for example, wrongly claiming to be a police officer, doctor or trusted organisation.

Collecting directly from the individual

3.64 APP 3.6 provides that an APP entity ‘must collect personal information about an individual only from the individual’, unless one of the following exceptions apply:

• for all APP entities, it is unreasonable or impracticable for the entity to collect personal information only from the individual

• for agencies, the individual consents to the personal information being collected from someone other than the individual

• for agencies, the agency is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual.

Unreasonable or impracticable to collect directly from the individual

3.65 Whether it is ‘unreasonable or impracticable’ to collect personal information only from the individual concerned will depend on the circumstances of the particular case. Considerations that may be relevant include:

• whether the individual would reasonably expect personal information about them to be collected directly from them or from another source

• the sensitivity of the personal information being collected

• whether direct collection would jeopardise the purpose of collection or the integrity of the personal information collected

• any privacy risk if the information is collected from another source

• the time and cost involved of collecting directly from the individual. However, an APP entity is not excused from collecting from the individual rather than another source by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable or impracticable will depend on whether the burden is excessive in all the circumstances.

3.66 The following are given as examples of when it may be unreasonable or impracticable to collect personal information only from the individual concerned:

• collection by a law enforcement agency of personal information about an individual who is under investigation, where the collection may jeopardise the investigation if the personal information is collected only from that individual

• if a legal or official document that is mailed to an individual is returned to the sender, the individual’s current contact details may need to be obtained from another source.

---

20 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 77.
Consent by the individual — for agencies only

3.67 The term ‘consent’ is discussed at paragraph 3.23 above and in Chapter B (Key concepts). As noted in those sections, consent can be express or implied, and must be voluntary, informed, current and specific, and the individual must have capacity to consent.

3.68 An example of where an agency might collect personal information from someone other than the individual is where an individual consents to one agency disclosing their personal information (such as contact details) to the other agency.

Required or authorised by law or a court or tribunal order — for agencies only

3.69 The meaning of ‘required or authorised by or under an Australian law or a court/tribunal order’ is discussed in Chapter B (Key concepts). It is a common feature of legislation that an agency, for the purpose of performing a function or exercising a power, is authorised to require a person or body to provide personal information.

3.70 An example of where collection by an agency from someone other than the individual concerned might be required or authorised by law is s 44 of the Privacy Act, which provides that the Information Commissioner may issue a notice to a person requiring them to provide specified information for the purpose of an investigation under the Act (and that information may include personal information).

Collecting personal information from a related body corporate

3.71 Section 13B(1)(a) provides that the collection of personal information about an individual (other than sensitive information) by a body corporate from a related body corporate is generally not ‘an interference with the privacy of an individual’ (interferences with privacy are discussed in Chapter A (Introductory matters)). This provision applies to collection of information from related bodies corporate and not to other corporate relationships such as a franchise or joint-venture relationship.21

3.72 The effect of s 13B(1)(a) is that an APP entity may collect personal information (other than sensitive information) from a related body corporate without satisfying the requirements of APP 3.1 or 3.2 (see paragraphs 3.8–3.21 above). However, s 13B(1A) sets out some exceptions to this, including where the related body corporate is not an organisation.

---

21 Section 6(8) states ‘for the purposes of this Act, the question of whether bodies corporate are related to each other is determined in the manner in which that question is determined under the Corporations Act 2001’.
Chapter 4: Australian Privacy Principle
4 — Dealing with unsolicited personal information

Version 1.0, February 2014

Key points.......................................................................................................................................................... 2
What does APP 4 say?........................................................................................................................................ 2
‘Unsolicited’ personal information ......................................................................................................................... 3
Determining whether unsolicited personal information could have been collected under APP 3 ........................................................................................................................................................................ 4
Dealing with unsolicited personal information that could not have been collected under APP 3 ........................................................................................................................................................................ 4
  Unsolicited personal information received by an agency ........................................................................ 5
  Unsolicited personal information received by an organisation ................................................................. 5
    Destruction or de-identification that is ‘lawful’ ...................................................................................... 6
    Destruction or de-identification that is ‘reasonable’ .............................................................................. 6
Dealing with unsolicited personal information that could have been collected under APP 3, or is not destroyed or de-identified .............................................................................................................. 7
Key points

- APP 4 outlines the steps an APP entity must take if it receives unsolicited personal information.
- Unsolicited personal information is personal information received by an APP entity where the entity has taken no active steps to collect the information.
- If an APP entity receives unsolicited personal information, it must decide whether it could have collected the information under APP 3 (collection of solicited personal information).
- If the entity determines it could not have collected the personal information under APP 3, different rules apply according to whether or not the information is contained in a ‘Commonwealth record’.
- If the unsolicited personal information is contained in a Commonwealth record, APP 4 does not require it to be destroyed or de-identified.
- Other unsolicited personal information that could not have been collected under APP 3, must be destroyed or de-identified as soon as practicable if it is lawful and reasonable to do so.
- If an APP entity is not required to destroy or de-identify the unsolicited personal information under APP 4, the entity may retain the personal information but must deal with it in accordance with APPs 5–13.

What does APP 4 say?

4.1 APP 4 outlines the steps an APP entity must take if it receives unsolicited personal information. Unsolicited personal information is personal information received by an entity that has not been requested by that entity.

4.2 An APP entity that receives unsolicited personal information must decide whether or not it could have collected the information under APP 3, and:

- if the entity could not have collected the personal information and the information is not contained in a Commonwealth record — the entity must destroy or de-identify the information as soon as practicable, if it is lawful and reasonable to do so (APP 4.3), or
- if the entity could have collected the personal information under APP 3, or the information is contained in a Commonwealth record, or the entity is not required to destroy or de-identify the information under APP 4.3 because it would be unlawful or unreasonable to do so — the entity may keep the information but must deal with it in accordance with APPs 5–13. See Chapter B (Key concepts) for more information about Commonwealth records.

4.3 In effect, APP 4 requires an APP entity to consider the following issues:

- has the entity received unsolicited personal information?
• could the entity have collected that personal information under APP 3?
• if the entity is an agency or a ‘contracted service provider’, is the personal information contained in a Commonwealth record?
• should unsolicited personal information held by the entity be destroyed or de-identified, or should it be retained and dealt with in accordance with APP 5–13?

4.4 The objective of APP 4 is to ensure that personal information that is received by an APP entity is afforded appropriate privacy protection, even where the entity has not solicited the personal information.

‘Unsolicited’ personal information

4.5 All personal information received by an APP entity is either solicited or unsolicited personal information. Section 6(1) defines ‘solicit’ but does not define ‘unsolicited’. Therefore, personal information received by an entity that does not fall within the definition of ‘solicited’ is unsolicited personal information.

4.6 The term ‘solicit’ is discussed in Chapter 3 (APP 3), including examples of solicited personal information collected by APP entities. An APP entity solicits personal information if it requests another agency, organisation, individual or small business operator to provide the personal information, or to provide a kind of information in which that personal information is included. A ‘request’ is an active step taken by an entity to collect information, and may not involve direct communication between the entity and an individual.

4.7 Applying that definition of ‘solicit’, unsolicited personal information is personal information that an APP entity receives but has taken no active steps to collect. Examples include:

• redirected mail received by an entity
• correspondence to Ministers and Government departments from members of the community, or other unsolicited correspondence to an entity
• a petition sent to an entity that contains names and addresses
• an employment application sent to an entity on an individual’s own initiative and not in response to an advertised vacancy
• a promotional flyer containing personal information, sent to an entity by an individual promoting the individual’s business or services.

4.8 As a general rule, personal information provided to an APP entity that is additional to the information that has been requested by the entity should be treated as unsolicited personal information. For example, if an individual completes an application form provided by an entity but attaches financial records that have not been requested by the entity, these should be treated as unsolicited personal information. The entity must determine whether it could have collected the personal information under APP 3 (APP 4.1), and deal with the unsolicited personal information as required by either APP 4.3 or 4.4 (see below).
4.9 In some instances, an APP entity may have difficulty deciding whether personal information it receives falls within the terms of the entity’s request and is therefore solicited personal information. In such circumstances, an entity should focus on the nature of the additional personal information and the connection it has with the entity’s request. Where it is unclear whether the information is solicited or unsolicited personal information, the entity should err on the side of caution and treat the personal information as unsolicited personal information.

Determining whether unsolicited personal information could have been collected under APP 3

4.10 An APP entity that receives unsolicited personal information must, ‘within a reasonable period after receiving the information’, decide whether the personal information could have been collected by the entity under APP 3 (APP 4.1).

4.11 The tests for deciding whether personal information can be collected by an APP entity are set out in APP 3 (see Chapter 3):

- an agency may only collect personal information that is reasonably necessary for, or directly related to, one or more of its functions or activities (APP 3.1)
- an organisation may only collect personal information that is reasonably necessary for one or more of its functions or activities (APP 3.2)
- and, in addition to the above requirements, an APP entity may only collect sensitive information if the individual consents to the sensitive information being collected, unless an exception applies (APP 3.3).

4.12 What is a ‘reasonable period’ for deciding whether unsolicited personal information could have been collected under APP 3 will depend on the circumstances of the particular case. The APP entity may undertake internal processes before making this decision, but should do so promptly.

4.13 APP 4.2 permits an APP entity to use or disclose the unsolicited personal information (for example, in internal discussions) for the purpose of determining whether the personal information could have been collected under APP 3.

Dealing with unsolicited personal information that could not have been collected under APP 3

4.14 If an APP entity receives unsolicited personal information that it determines it could not have collected under APP 3, it has an obligation to destroy or de-identify the personal information as soon as practicable, unless it is contained in a ‘Commonwealth record’ or it is unlawful or unreasonable to do so (APP 4.3). In practice, this means that different rules apply to agencies and organisations when handling unsolicited personal information.
Unsolicited personal information received by an agency

4.15 The term ‘Commonwealth record’ in s 6(1) has the same meaning as in s 3 of the Archives Act 1983 (the Archives Act) and is discussed in more detail in Chapter B (Key concepts). The term is likely to include all or most personal information received by agencies. It may also include personal information received by contracted service providers.

4.16 If the unsolicited personal information is contained in a Commonwealth record, the agency is not required to destroy or de-identify the personal information under APP 4.3, even if it determines that it could not have collected the information under APP 3. The agency will instead be required to comply with the provisions of the Archives Act in relation to the Commonwealth record.

4.17 A Commonwealth record can, as a general rule, only be destroyed or altered in accordance with s 24 of the Archives Act. The grounds on which this may be done include with the permission of the National Archives of Australia (as set out in a records disposal authority) or in accordance with ‘normal administrative practice’. See Chapter B (Key concepts) for more information about Commonwealth records.

4.18 Unsolicited personal information held by an agency in a Commonwealth record must be dealt with in accordance with APPs 5–13 (APP 4.4) (see paragraphs 4.28 to 4.30 below).

Unsolicited personal information received by an organisation

4.19 Unsolicited personal information received by an organisation, that could not have been collected under APP 3 must, as soon as practicable, be destroyed or de-identified if it is lawful and reasonable to do so (APP 4.3).

4.20 After an organisation has decided that the destruction or de-identification is lawful and reasonable, it should destroy or de-identify the personal information as promptly as practicable. In adopting a timetable that is ‘practicable’ an organisation can take technical and resource considerations into account. However, it is the responsibility of the organisation to be able to justify any delay in destroying or de-identifying the personal information.

---

1 Archives Act 1983, s 3: Commonwealth record means:
   (a) a record that is the property of the Commonwealth or of a Commonwealth institution; or
   (b) a record that is to be deemed to be a Commonwealth record by virtue of a regulation under subsection (6) or by virtue of section 22;
   but does not include a record that is exempt material or is a register or guide maintained in accordance with Part VIII.
Destruction or de-identification that is ‘lawful’

4.21 The term ‘lawful’ is not defined in the Privacy Act. It is lawful for an organisation to destroy or de-identify unsolicited personal information if it is not unlawful to do so. That is, if the destruction or de-identification is not criminal, illegal or prohibited or proscribed by law. Unlawful activity does not include breach of a contract.

4.22 Examples of where destruction may not be lawful include:

- a legislative provision in an Act or subordinate instrument requires an organisation to retain the personal information for a specified purpose — for example, for auditing, inspection or reporting purposes
- a court, tribunal or body with legal power to issue binding orders, has made an order requiring the personal information to be retained for a specified purpose or period.

4.23 As those examples illustrate, it is important that each organisation is aware of the legal rules or orders that may prevent it from destroying or de-identifying unsolicited personal information.

Destruction or de-identification that is ‘reasonable’

4.24 Whether destruction or de-identification is reasonable is a question of fact in each individual case. It is an objective standard that has regard to how a reasonable person, who is properly informed, would be expected to act in the circumstances. It is the responsibility of the organisation to be able to justify that its conduct was reasonable.

4.25 Relevant considerations may include:

- the amount and sensitivity of the personal information
- whether the personal information is commingled with solicited personal information, and it would be impractical for the organisation to separate the personal information (see paragraph 4.26 below for an example of where it may be practicable to separate solicited and unsolicited personal information)
- whether a law enforcement authority has requested that the personal information be retained pending the completion of an investigation
- whether the organisation has considered a range of options for destroying or de-identifying the personal information
- whether the individual that the personal information is about has expressly requested the organisation to return the information to the individual, rather than destroying or de-identifying the information, and the organisation does not retain another copy of the personal information
- where destruction or de-identification is unreasonable within a short timeframe, whether the destruction or de-identification task could be undertaken using a staged approach
- the practicability, including time and cost involved. However, an organisation is not excused from destroying or de-identifying the personal information by reason only
that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to destroy or de-identify the personal information will depend on whether the burden is excessive in all the circumstances.

4.26 Those and other relevant considerations should be applied cautiously. Before deciding that it is reasonable to retain unsolicited personal information, an organisation should examine viable options for destroying or de-identifying it. For example, it may be practicable to transcribe or convert, and produce a new record of, solicited personal information that is commingled with unsolicited personal information. The original record containing the unsolicited personal information could then be destroyed or de-identified.

4.27 For further discussion of destroying and de-identifying personal information, see Chapter B (Key concepts) and Chapter 11 (APP 11).

Dealing with unsolicited personal information that could have been collected under APP 3, or is not destroyed or de-identified

4.28 An APP entity may retain unsolicited personal information if the entity has determined that it could have collected the personal information under APP 3, or the personal information is contained in a Commonwealth record, or the entity is not required to destroy or de-identify the personal information under APP 4.3 because it would be unlawful or unreasonable to do so. The personal information must then be dealt with in accordance with APPs 5–13 (APP 4.4). This means, for example, that a notice of collection may be required (see Chapter 5 (APP 5)), the personal information may only be used or disclosed for the primary purpose for which it was collected unless an exception applies (see paragraph 4.29 below and Chapter 6 (APP 6)), the security of the personal information must be protected (see Chapter 11 (APP 11)), an individual can request access to the personal information (see Chapter 12 (APP 12)) and an individual can request the entity to correct the personal information (see Chapter 13 (APP 13)).

4.29 Two other matters should be borne in mind by an APP entity that retains personal information for one of the reasons listed in paragraph 4.28. The first is that the personal information, though retained by the APP entity, may not be information that could have been collected for a particular purpose under APP 3.1 (for example, where the personal information is retained because it is contained in a Commonwealth record, or because it is not lawful or reasonable for the entity to destroy or de-identify it). Consequently, if the entity has not collected the personal information for a particular primary purpose, the entity may only use or disclose it if an exception in APP 6 applies (see Chapter 6).

4.30 Secondly, APP 11.2 requires an APP entity to destroy or de-identify personal information it holds but which it no longer needs for any purpose permitted by the APPs, unless the personal information is contained in a Commonwealth record or the entity is required by or under an Australian law, or a court/tribunal order, to retain the information. Consequently, personal information that is retained under APP 4.4 may
nevertheless need to be destroyed or de-identified in accordance with APP 11.2 (see Chapter 11 (APP 11)).
Chapter 5: Australian Privacy Principle 5 — Notification of the collection of personal information

Version 1.1, March 2018

Key points............................................................................................................................................ 2
What does APP 5 say?.................................................................................................................................. 2
Taking reasonable steps to notify or ensure awareness ........................................................................ 2
   When not taking any steps might be reasonable ............................................................................ 4
Matters about which an individual must be notified or made aware ................................................... 5
   The APP entity’s identity and contact details ................................................................................. 5
   The facts and circumstances of collection ..................................................................................... 5
   If the collection is required or authorised by law ............................................................................ 6
   The purposes of collection ............................................................................................................... 6
   The consequences for the individual if personal information is not collected ............................. 7
   Other APP entities, bodies or persons to which the personal information is usually disclosed ............................................................................................................................... 7
   Information about access and correction in the APP entity’s APP Privacy Policy ...................... 8
   Likely cross-border disclosures of the personal information .......................................................... 8
   When notification is to occur .......................................................................................................... 9
Key points

- An APP entity that collects personal information about an individual must take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters.

- The matters include:
  - the APP entity’s identity and contact details
  - the fact and circumstances of collection
  - whether the collection is required or authorised by law
  - the purposes of collection
  - the consequences if personal information is not collected
  - the entity’s usual disclosures of personal information of the kind collected by the entity
  - information about the entity’s APP Privacy Policy
  - whether the entity is likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located.

- An APP entity must take reasonable steps, before, or at the time it collects personal information. If this is not practicable, reasonable steps must be taken as soon as practicable after collection.

What does APP 5 say?

5.1 APP 5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters (generally referred to in this chapter as ‘APP 5 matters’). The term ‘collects’ is discussed in Chapter B (Key concepts). Reasonable steps must be taken at or before the time of collection, or as soon as practicable afterwards.

5.2 The requirement to notify or ensure awareness of the APP 5 matters applies to all personal information ‘collected’ about an individual, either directly from the individual or from a third party. It applies to solicited personal information (APP 3) and also unsolicited personal information that is not destroyed or de-identified by the APP entity (APP 4) (see Chapter 3 (APP 3), Chapter 4 (APP 4) and Chapter B (Key concepts)).

Taking reasonable steps to notify or ensure awareness

5.3 An APP entity must take reasonable steps either to notify an individual of the APP 5 matters or to ensure the individual is aware of those matters (APP 5.1).

5.4 The reasonable steps for an APP entity will depend upon circumstances that include:
• the sensitivity of the personal information collected. More rigorous steps may be required when collecting ‘sensitive information’ (defined in s 6(1) and discussed in Chapter B (Key concepts)) or information of a sensitive nature

• the possible adverse consequences for an individual as a result of the collection. More rigorous steps may be required as the risk of adversity increases

• any special needs of the individual. More rigorous steps may be required if personal information is collected from an individual from a non-English speaking background who may not readily understand the APP 5 matters

• the practicability, including time and cost involved. However, an entity is not excused from taking particular steps by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances.

5.5 An individual may be notified or made aware of APP 5 matters through a variety of formats, provided the matters are expressed clearly. A notice may be prepared in advance (paper, online, telephone script) and staff should be trained to understand their obligation to take reasonable steps to notify or ensure awareness under APP 5. A notice may also be provided in layers, from a full explanation to a brief refresher as individuals become more familiar with how the APP entity operates and how personal information is handled. Brief privacy notices on forms or signs may be supplemented by longer notices made available online or in brochures.

5.6 Examples of reasonable steps that an APP entity could consider taking to notify or ensure awareness of the APP 5 matters include:

• if the entity collects personal information directly from an individual who completes a form or uses an online facility, clearly and prominently displaying the APP 5 matters in the form, or providing a readily accessible and prominent link to an APP 5 notice

• if personal information is collected by telephone, explaining the APP 5 matters to the individual at the commencement of the call (perhaps following a template script or using an automated message). Where this is not practicable, an entity should give the individual information about the APP 5 matters as soon as possible afterwards, such as in any subsequent electronic or paper-based communication, or directing the individual to the relevant notice on the entity’s website

• if the entity collects personal information from another entity, ensuring that the other entity has notified or made the individual aware of the relevant APP 5 matters on its behalf (such as through an enforceable contractual arrangement)

• where it is not reasonable to notify or ensure awareness of the full range of APP 5 matters, an entity could alert the individual to specific sections of its APP Privacy Policy (see Chapter 1 (APP 1)), such as parts of the Policy about likely overseas disclosures (APP 5.2(i)), or other general documents containing relevant
information.\textsuperscript{1} However, before doing so the entity should consider whether information in the APP Privacy Policy sufficiently covers the APP 5 matters as they relate to the particular collection, as the APP Privacy Policy may describe only the general information handling practices of the entity.

When not taking any steps might be reasonable

5.7 APP 5.1 acknowledges that it may be reasonable for an APP entity to not take any steps to provide a notice or ensure awareness of all or some of the APP 5 matters. It is the responsibility of the entity to be able to justify not taking any steps. The following are given as examples of when this may be reasonable:

- the individual is aware that personal information is being collected, the purpose of collection and other APP 5 matters relating to the collection, for example, a doctor has informed a patient that a specialist to whom the patient is referred for treatment will obtain the patient’s health information from the doctor
- an entity collects personal information from an individual on a recurring basis in relation to the same matter. However, if a long period of time has elapsed since the notice was provided and the individual may no longer be aware of the APP 5 matters, the entity may need to take steps to notify or ensure awareness. Similarly, if a change in circumstances as to how personal information is collected affects any of the APP 5 matters, the entity should take reasonable steps to ensure an individual is aware of those matters.
- notification may pose a serious threat to the life, health or safety of an individual or pose a threat to public health or safety, for example, a law enforcement agency obtaining personal information from a confidential source for the purpose of an investigation
- notification may jeopardise the purpose of collection or the integrity of the personal information collected and there is a clear public interest in the purpose of collection, for example, a law enforcement agency undertaking lawful covert surveillance of an individual in connection with a criminal investigation
- notification would be inconsistent with another legal obligation, for example, by breaching a statutory secrecy provision, a client’s legal professional privilege, or a legal obligation of confidence
- an entity collects personal information about a person who poses (or is alleged to pose) a risk of committing family violence and this collection is permitted by a legislated family violence information sharing scheme, such as that established by the Family Violence Protection Act 2008 (Vic)

\textsuperscript{1} See Tenants’ Union of Queensland Inc, Tenants’ Union of NSW Co-op Ltd v TICA Default Tenancy Control Pty Ltd [2004] PrivCmrACD 4 (16 April 2004) [80], [82], which states ‘if an organisation provides the information required to meet its obligations on different forms or in different locations it would generally need to alert individuals to the fact the other information was available…it should [also] seek to ensure that there are appropriate references to that information in the primary form’.
• the impracticability of notification, including the time and cost, outweighs the privacy benefit of notification. For example:
  o where an entity collects personal information about the individual’s next of kin for emergency contact purposes, it would generally be reasonable for the entity to take no steps to notify the next of kin of the collection of their personal information
  o where an individual provides unsolicited personal information to an entity about a third party for the purposes of a confidential alternative dispute resolution process, and the entity is not required to destroy or de-identify the information under APP 4 (see Chapter 4), it would generally be reasonable for the entity to take no steps to notify the third party. This is especially so where the entity will not rely on the personal information in investigating or resolving the matter, or does not have the contact details of the third party.

Matters about which an individual must be notified or made aware

5.8 APP 5.2 lists the matters (discussed separately below) that must be notified to an individual or of which they must be made aware. For each matter, an APP entity must consider whether notifying the individual is reasonable in the circumstances. This means that it may be reasonable for an entity to notify some but not all of the APP 5 matters. For example, it may be reasonable not to notify an individual of the collecting entity’s identity where this is obvious from the circumstances.

The APP entity’s identity and contact details

5.9 The matter set out in APP 5.2(a) is the identity and contact details of the APP entity. This could include the position title, telephone number and email address of a contact who handles enquiries and requests relating to the Privacy Act. Consideration could also be given to establishing a generic telephone number and email address (for example, privacy@agency.gov.au) that will not change with staff movements. This ensures awareness of a contact if an individual chooses to exercise any available rights such as to request access to, or correction of, personal information later (see Chapter 12 (APP 12) and Chapter 13 (APP 13)).

The facts and circumstances of collection

5.10 The matter set out in APP 5.2(b) is the fact and circumstances of collection. This may include how, when and from where the personal information was collected. This requirement applies where either the personal information has been collected from a third party or the individual may not be aware that the entity has collected their personal information.

5.11 The following examples illustrate matters that can be notified:
• where the individual’s personal information was or will be collected from another entity, the individual should be made aware of the name of the entity. If this is not practicable because, for instance, the APP entity collects information from a wide variety of entities and it would not be practicable to give a separate notice in relation to each entity, the APP entity should instead indicate the kinds of entities from which it collects that information.

• where the individual’s personal information was or will be collected from an individual, the name of that individual should be provided, unless doing so would be an interference with the privacy of that individual (for example, the use or disclosure breaches APP 6 because that individual would not reasonably expect their personal information to be disclosed in an APP 5 notice and no other exception in APP 6 applies) (see Chapter 6 (APP 6)).

• where the individual may not be aware of their personal information being collected, the individual should be made aware of the method of collection, for example, that personal information is collected through use of a hidden radio-frequency identification tag (RFID tags), software (such as cookies), or biometric technology (such as voice or facial recognition).

If the collection is required or authorised by law

5.12 The matter set out in APP 5.2(c) is the fact (if applicable) that a collection is required or authorised by or under an Australian law or a court/tribunal order. The phrase ‘required or authorised by or under an Australian law or court/tribunal order’ is discussed in Chapter B (Key concepts).

5.13 The name of the Australian law (or, if applicable, the regulation or other instrument), or details of the particular court or tribunal order, that requires or authorises the collection, must also be included. If practicable, the notice could include the provision of the law, regulation or other instrument relied upon for collection.

5.14 If it is not reasonable to name the particular law relied upon (for example, multiple Australian laws authorise or require the collection) the more practical option may be to include a generic description of the laws under which personal information is collected (for example, ‘taxation laws’).

The purposes of collection

5.15 The matter set out in APP 5.2(d) is the purposes for which the APP entity collects the personal information. This includes the primary purpose of collection, that is, the specific function or activity for which particular personal information is collected.

5.16 If the APP entity may use or disclose personal information for purposes other than the primary purpose (known as a ‘secondary purpose’), these could also be included. This may create a reasonable expectation that the personal information will be used or disclosed for a secondary purpose, of relevance to the exception in APP 6.2(a) (this exception is discussed in Chapter 6 (APP 6)). The entity does not need to include in its description internal purposes that form part of normal business practices, such as auditing, business planning, billing or de-identifying personal information.
5.17 The term ‘purpose’, including ‘primary purpose’, ‘secondary purpose’ and how a purpose should be described, are discussed in Chapter B (Key concepts) and Chapter 6 (APP 6)).

The consequences for the individual if personal information is not collected

5.18 The matter set out in APP 5.2(e) is the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity.

5.19 An APP entity is not required to list all possible or remote consequences or those that would be obvious to a reasonable person. Instead, it should describe significant consequences that could be expected to result. If the individual can avoid or lessen those consequences by providing some but not other personal information, this should be explained.

5.20 The following are given as examples of consequences that may result if personal information is not collected:

- an application for a licence, benefit, allowance or concession cannot be processed
- an APP entity cannot properly investigate or resolve an individual’s complaint
- a different level of service will be provided to the individual. For example, the individual may not be eligible to purchase a discounted flight without providing personal information about a medical emergency in the individual’s family.

Other APP entities, bodies or persons to which the personal information is usually disclosed

5.21 The matter set out in APP 5.2(f) is any other APP entity, body or person, or the types of other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity.

5.22 An APP entity is not required to include that a particular disclosure has occurred or will occur. Rather, APP 5.2(f) requires an entity to notify or ensure awareness of the ‘usual’ practices of the entity in disclosing personal information of that ‘kind’ to other APP entities, bodies or persons or ‘types’ of APP entities, bodies or persons.

5.23 A ‘usual’ disclosure is one that occurs regularly, under an agreed arrangement, or that can reasonably be predicted or anticipated. It does not include a disclosure that may occur in exceptional or special circumstances (such as a disclosure under a lawful warrant to a law enforcement agency).

5.24 The ‘kind’ of personal information that is usually disclosed may be described, for example, as ‘contact details’, ‘employment history’, ‘educational qualifications’ or ‘complaint details’.

5.25 If the personal information is usually disclosed to a particular APP entity (including a related body corporate), body or person, it should be named, unless it would be impracticable to include a long list of APP entities, bodies or persons. In that case, the ‘type’ of APP entity, body or person should be described, for example, as ‘health insurers’ or ‘State Government motor vehicle licensing authorities’ or ‘related bodies corporate’.

An APP entity is not required to describe the disclosure practices of the APP entity, body
or person to which the information is disclosed. However, if it is known that that APP
text, body or person usually discloses the personal information to other entities, this
could be noted.

**Information about access and correction in the APP entity’s APP Privacy Policy**

5.26 The matters set out in APP 5.2(g) and (h) are that the APP entity’s APP Privacy Policy contains information about how the individual may:

- access and seek correction of their personal information held by the entity (APP 5.2(g))
- complain to the entity about a breach of the APPs, or any registered APP code that
  binds the entity, and how the entity will deal with such a complaint (APP 5.2(h)).

5.27 Where practicable, an APP 5 notice could include a prominent and accessible link
to the APP Privacy Policy on the entity’s website or explain how it may be accessed. The
APP Privacy Policy requirements are discussed in Chapter 1 (APP 1).

**Likely cross-border disclosures of the personal information**

5.28 The matters set out in APP 5.2(i) and (j) are:

- whether the APP entity is likely to disclose the personal information to overseas
  recipients (APP 5.2(i)), and
- if so, the countries in which such recipients are likely to be located if it is practicable
  to specify those counties in the notice or to otherwise make the individual aware of
  them (APP 5.2(j)).

5.29 This requirement only applies to a likely disclosure of personal information to an
overseas recipient. It does not apply to a use of personal information by an APP entity
that does not constitute a disclosure. For example, routing personal information, in
transit, through servers located outside Australia would usually be considered a ‘use’ and
not a ‘disclosure’.² Similarly, if an entity makes personal information accessible to an
overseas office of the entity (for example, a consular office), this is a use and not a
disclosure.³ For further discussion of the requirements applying to a cross-border
disclosure of personal information, and what is considered a disclosure, see Chapter 8
(APP 8).

5.30 An example of when it may be impracticable to specify the countries in which
overseas recipients of personal information are likely to be located is where personal
information is likely to be disclosed to numerous overseas recipients and the burden of
determining where those recipients are located is excessively time-consuming, costly or
inconvenient in all the circumstances. However, an APP entity is not excused from
specifying the countries by reason only that it would be inconvenient, time-consuming or
impose some cost to do so. Whether these factors make it impracticable to specify the
countries will depend on whether the burden is excessive in all the circumstances. In this,

---

² Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.
³ Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.
as in other examples, it is the responsibility of the entity to be able to justify that this is impracticable.

5.31 The requirement to notify an individual or ensure awareness if information being collected is likely to be disclosed to overseas recipients, and the location of those recipients, complements the obligation on APP entities under APP 1.4(f) and (g) to describe overseas disclosure practices in an APP Privacy Policy (see Chapter 1 (APP 1)).

5.32 If the personal information is disclosed to numerous overseas locations, one practical option may be to list those countries in an appendix to the notice rather than in the body of the notice. Where it is not practicable to specify the countries, the entity could instead identify general regions (such as European Union countries).

5.33 An APP entity that regularly discloses personal information overseas could consider including additional information in an APP 5 notice about these disclosures, to ensure transparent handling of personal information. For example, the APP 5 notice could explain:

- how the overseas recipient might use, disclose and protect the personal information, including whether the overseas recipient may be required to disclose the personal information under a foreign law (see discussion of s 6A(4) in Chapter 8 (APP 8))
- how the individual can request further information about laws or binding schemes that protect privacy in the country of receipt (this information may be particularly relevant if an entity intends to rely on the exception in APP 8.2(a) (see Chapter 8 (APP 8))
- how the individual can access personal information held by the overseas recipient.

When notification is to occur

5.34 An APP entity must take any reasonable steps to comply with APP 5:

- at or before the time an APP entity collects an individual’s personal information, or
- if that is not practicable, as soon as practicable after the collection occurs.

5.35 This requirement recognises that it is preferable that an individual can make an informed choice about whether to provide personal information to an APP entity.

5.36 Examples of when it may not be practicable to take reasonable steps at or before the time of collection include where:

- urgent collection of the personal information is required and giving a notice or ensuring awareness would unreasonably delay the collection, for example, where there is a serious threat to an individual’s life or health or to public safety
- the medium through which personal information is collected makes it impracticable to provide a detailed APP 5 notice or ensure awareness at or before the time of collection. For example, where personal information is collected by telephone, it
may be impracticable to notify or ensure the individual is aware of all of the APP 5 matters at the time of collection (see paragraph 5.5).4

5.37 The test of practicability is an objective test. It is the responsibility of the APP entity to be able to justify that it is not practicable to give notification or ensure awareness before or at the time of collection. Options for providing early notification or ensuring awareness should, so far as practicable, be built into information collection processes and systems – for example, by including relevant information in standard forms and online collection mechanisms (see APP 1.2, Chapter 1).

5.38 If notification does not occur before or at the time of collection, the APP entity must take reasonable steps to provide notification, or ensure the individual is aware, as soon as practicable after the collection. In adopting a timetable that is ‘practicable’, an entity can take technical and resource considerations into account. However, it is the responsibility of the entity to be able to justify any delay in notification.

---

Chapter 6: Australian Privacy Principle
6 — Use or disclosure of personal information

Version 1.0, February 2014

Key points .................................................................................................................................... 3
What does APP 6 say? .................................................................................................................. 3
‘Holds’, ‘use’, ‘disclose’ and ‘purpose’ ...................................................................................... 4
‘Holds’ .......................................................................................................................................... 4
‘Use’ ............................................................................................................................................... 4
‘Disclose’ ....................................................................................................................................... 5
‘Purpose’ of collection .................................................................................................................. 6
Using or disclosing personal information for a secondary purpose ........................................... 6
Using or disclosing personal information with the individual’s consent ..................................... 6
Using or disclosing personal information where reasonably expected by the individual and related to the primary purpose of collection ................................................................. 7
Reasonably expect .................................................................................................................... 7
Relationship between the primary and secondary purpose ....................................................... 7
Using or disclosing personal information as required or authorised by law ................................ 8
Using or disclosing personal information where a permitted general situation exists ................ 9
Taking appropriate action in relation to suspected unlawful activity or serious misconduct ......... 11
Locating a person reported as missing ...................................................................................... 11
Reasonably necessary for a confidential alternative dispute resolution processes ................... 11
Necessary for a diplomatic or consular function or activity ....................................................... 12
Necessary for certain Defence Force activities outside Australia ............................................... 12
Using or disclosing personal information where a permitted health situation exists ............... 12
Conducting research; compiling or analysing statistics; management, funding or monitoring of a health service .................................................................................................................. 12
Necessary to prevent a serious threat to the life, health or safety of a genetic relative .................. 13
Disclosure to a responsible person for the individual .................................................................. 14
Using or disclosing personal information for an enforcement related activity .......................... 14
Reasonable belief .......................................................................................................................... 15
Reasonably necessary ................................................................. 15
Making a written note of use or disclosure for this secondary purpose .......... 16
Disclosing biometric information to an enforcement body ............................... 16
De-identifying certain health information before disclosure ............................ 16
Related bodies corporate ................................................................................. 17
Disclosing personal information to a related body corporate ......................... 17
Using or disclosing personal information collected from a related body corporate .... 18
Key points

- APP 6 outlines when an APP entity may use or disclose personal information.
- An APP entity can only use or disclose personal information for a purpose for which it was collected (known as the ‘primary purpose’), or for a secondary purpose if an exception applies.
- The exceptions include where:
  - the individual has consented to a secondary use or disclosure
  - the individual would reasonably expect the APP entity to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose
  - the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order
  - a permitted general situation exists in relation to the secondary use or disclosure
  - the APP entity is an organisation and a permitted health situation exists in relation to the secondary use or disclosure
  - the APP entity reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body, or
  - the APP entity is an agency (other than an enforcement body) and discloses biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner for the purposes of APP 6.3.

What does APP 6 say?

6.1 APP 6 outlines when an APP entity may use or disclose personal information. The intent is that an entity will generally use and disclose an individual’s personal information only in ways the individual would expect or where one of the exceptions applies.

6.2 An APP entity that holds personal information about an individual can only use or disclose the information for a particular purpose for which it was collected (known as the ‘primary purpose’ of collection), unless an exception applies. Where an exception applies the entity may use or disclose personal information for another purpose (known as the ‘secondary purpose’). Exceptions include:
- the individual consented to a secondary use or disclosure (APP 6.1(a))
- the individual would reasonably expect the secondary use or disclosure, and that is related to the primary purpose of collection or, in the case of sensitive information, directly related to the primary purpose (APP 6.2(a))
Chapter 6: APP6 — Use or disclosure of personal information   Version 1.0, February 2014

Office of the Australian Information Commissioner — APP guidelines 4

- the secondary use or disclosure of the personal information is required or authorised by or under an Australian law or a court/tribunal order (APP 6.2(b))
- a permitted general situation exists in relation to the secondary use or disclosure of the personal information by the APP entity (APP 6.2(c))
- the APP entity is an organisation and a permitted health situation exists in relation to the secondary use or disclosure of the personal information by the organisation (APP 6.2(d))
- the APP entity reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body (APP 6.2(e))
- the APP entity is an agency (other than an enforcement body) and discloses personal information that is biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner for the purposes of APP 6.3 (APP 6.3).

6.3 An APP entity may disclose personal information, other than sensitive information, to a related body corporate (s 13B(1)(b)).

6.4 APP 6 does not apply to the use or disclosure by an organisation of:
- personal information for the purpose of direct marketing (this is covered by APP 7), or
- government related identifiers (this is covered by APP 9) (APP 6.7).

‘Holds’, ‘use’, ‘disclose’ and ‘purpose’

6.5 Each of the terms ‘holds’, ‘use’, ‘disclose’ and ‘purpose’ which are used in APP 6 and other APPs, are discussed in more detail in Chapter B (Key concepts). The following is a brief analysis of the meaning of these terms in the context of APP 6.

‘Holds’

6.6 APP 6 only applies to personal information that an APP entity ‘holds’. An APP entity ‘holds’ personal information ‘if the entity has possession or control of a record that contains the personal information’ (s 6(1)).

6.7 The term ‘holds’ extends beyond physical possession of a record to include a record that an entity has the right or power to deal with. For example, an APP entity that outsources the storage of personal information to a third party, but retains the right to deal with that information, including to access and amend it, holds that personal information. The term ‘holds’ is discussed further in Chapter B (Key concepts).

‘Use’

6.8 The term ‘use’ is not defined in the Privacy Act. An APP entity ‘uses’ information where it handles or undertakes an activity with the information, within the entity’s effective control. For further discussion of use, see Chapter B (Key concepts). Examples include:
• the entity accessing and reading the personal information
• the entity searching records for the personal information
• the entity making a decision based on the personal information
• the entity passing the personal information from one part of the entity to another
• unauthorised access by an employee of the entity.¹

‘Disclose’

6.9 The term ‘disclose’ is not defined in the Privacy Act. An APP entity ‘discloses’ personal information where it makes it accessible to others outside the entity and releases the subsequent handling of the information from its effective control. This focuses on the act done by the disclosing party. The state of mind or intentions of the recipient does not affect the act of disclosure. Further, there will be a disclosure in these circumstances even where the information is already known to the recipient. For further discussion of disclosure, see Chapter B (Key concepts).

6.10 The release may be a proactive release or publication, a release in response to a specific request, an accidental release or an unauthorised release by an employee.² Examples include where an APP entity:

• shares the personal information with another entity or individual
• discloses personal information to themselves, but in their capacity as a different entity
• publishes the personal information on the internet, whether intentionally or not,³ and it is accessible by another entity or individual
• accidentally provides personal information to an unintended recipient⁴
• reveals the personal information in the course of a conversation with a person outside the entity
• displays a computer screen so that the personal information can be read by another entity or individual, for example, at a reception counter or in an office.

6.11 ‘Disclosure’ is a separate concept from:

• ‘unauthorised access’ which is addressed in APP 11. An APP entity is not taken to have disclosed personal information where a third party intentionally exploits the entity’s security measures and gains unauthorised access to the information.⁵

¹ An APP entity is taken to have ‘used’ personal information where an employee gains unauthorised access ‘in the performance of the duties of the person’s employment’ (see s 8(1)).
² An APP entity is taken to have ‘disclosed’ personal information where an employee carries out an unauthorised disclosure ‘in the performance of the duties of the person’s employment’ (s 8(1)).
⁴ The APP entity may also breach APP 11 if it did not take reasonable steps to protect the information from this unauthorised disclosure (see APP 11, Chapter 11).
⁵ The actions of an employee will be attributed to the APP entity where it was carried out ‘in the performance of the duties of the person’s employment’ (s 8(1)).
Examples include unauthorised access following a cyber-attack or a theft, including where the third party then makes that personal information available to others outside the entity. However, where a third party gains unauthorised access, the APP entity may breach APP 11 if it did not take reasonable steps to protect the information from unauthorised access (see Chapter 11 (APP 11)).

- ‘use’, which is discussed in paragraph 6.8 above. APP 6 generally imposes the same obligations on an APP entity for uses and disclosures of personal information. Therefore, this distinction is not relevant in interpreting this principle (except in relation to APP 6.3). However, the distinction is relevant to APP 8, which applies to the disclosure of personal information to an overseas recipient (see Chapter 8 (APP 8)).

‘Purpose’ of collection

6.12 The purpose for which an APP entity collects personal information is known as the ‘primary purpose’ of collection. This is the specific function or activity for which the entity collects the personal information. ‘Purpose’, including how to identify and describe the primary purpose, is discussed in more detail in Chapter B (Key concepts).

6.13 The notification requirements in APP 5 complement the limitations on use and disclosure under APP 6. APP 5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. This includes the primary purpose of collection and could also include other purposes for which the entity collects the information (known as secondary purposes) (see APP 5.2(d)). The notification requirements are discussed in Chapter 5 (APP 5).

Using or disclosing personal information for a secondary purpose

6.14 A ‘secondary purpose’ is any purpose other than the primary purpose for which the APP entity collected the personal information.

6.15 The grounds on which an APP entity may use or disclose personal information for a secondary purpose are outlined below. It is nevertheless open to an entity not to rely on any such ground and to decide not to use or disclose personal information, unless the use or disclosure is required by law (see paragraphs 6.29–6.31 below).

Using or disclosing personal information with the individual’s consent

6.16 APP 6.1(a) permits an APP entity to use or disclose personal information for a secondary purpose where the individual has consented to the use or disclosure.

6.17 Consent is defined in s 6(1) as ‘express consent or implied consent’ and is discussed in Chapter B (Key concepts). The four key elements of consent are:

---

• the individual is adequately informed before giving consent
• the individual gives consent voluntarily
• the consent is current and specific, and
• the individual has the capacity to understand and communicate their consent.

Using or disclosing personal information where reasonably expected by the individual and related to the primary purpose of collection

6.18 APP 6.2(a) permits an APP entity to use or disclose personal information for a secondary purpose if the individual would reasonably expect the entity to use or disclose the information for that secondary purpose, and:

• if the information is sensitive information, the secondary purpose is directly related to the primary purpose of collection, or
• if the information is not sensitive information, the secondary purpose is related to the primary purpose of collection.

6.19 This exception creates a two-limb test which focuses both on the reasonable expectations of the individual, and the relationship between the primary and secondary purposes.

Reasonably expect

6.20 The ‘reasonably expects’ test is an objective one that has regard to what a reasonable person, who is properly informed, would expect in the circumstances. This is a question of fact in each individual case. It is the responsibility of the APP entity to be able to justify its conduct.

6.21 An APP entity should consider whether an individual would reasonably expect it to use or disclose for a secondary purpose only some of the personal information it holds about the individual, rather than all of the personal information it holds. The entity should only use or disclose the minimum amount of personal information sufficient for the secondary purpose. For example, an individual may not reasonably expect an entity that is investigating their complaint against a contractor to disclose the individual’s residential address and home contact details to the contractor as part of its investigation. The individual would reasonably expect the entity to give the contractor only the minimum amount of personal information necessary to enable them to respond to the complaint.7

6.22 Examples of where an individual may reasonably expect their personal information to be used or disclosed for a secondary purpose include where:

• the individual makes adverse comments in the media about the way an APP entity has treated them. In these circumstances, it may be reasonable to expect that the

---

7 For another example of where an individual would not reasonably expect disclosure, see W v Telecommunications Company [2007] PrivCmrA 25, Australasian Legal Information Institute website <www.austlii.edu.au>.
entity may respond publicly to these comments in a way that reveals personal information specifically relevant to the issues that the individual has raised8

- an agency discloses to another agency a query, view or representation that an individual has made to the first-mentioned agency9

- the entity has notified the individual of the particular secondary purpose under APP 5.1 (see Chapter 5 (APP 5))

- the secondary purpose is a normal internal business practice, such as as auditing, business planning, billing or de-identifying the personal information.

**Relationship between the primary and secondary purpose**

6.23 This exception is limited to using or disclosing personal information for a secondary purpose that is ‘related’, or for sensitive information ‘directly related’, to the primary purpose of collection.

**Related secondary purpose**

6.24 A related secondary purpose is one which is connected to or associated with the primary purpose. There must be more than a tenuous link.10

6.25 Examples of where a secondary purpose is related to the primary purpose of collection include:

- an organisation collects personal information about an individual for the primary purpose of collecting a debt. A law firm, acting on behalf of that organisation in relation to the debt collection, contacts the individual’s neighbour and seeks information from the neighbour about the individual’s whereabouts (but does not disclose any specific information about the debt). This disclosure to the neighbour, for the secondary purpose of locating the individual, is related to the primary purpose of debt collection and would be within the individual’s reasonable expectations11

- an agency collects personal information to include in an employee’s personnel file for the primary purpose of administering that individual’s employment.12 It then uses this personal information as part of an investigation into complaints by the individual about working conditions. In these circumstances, the use for the secondary purpose of investigating a complaint in the workplace is related to the

---


9 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 78.


11 This example is adapted from M and Law Firm [2011] AlCmrCN 7 (available at Australasian Legal Information Institute website <www.austlii.edu.au>), where the Commissioner also referred the complaint to the Australian Competition and Consumer Commission to consider whether the debt collection practices were consistent with its debt collection guidelines.

12 The exemption relating to employee records in s 7B(3) only applies to organisations.
primary purpose of collection, and would be within the individual’s reasonable expectations.\textsuperscript{13}

- an APP entity uses personal information for the purpose of de-identifying the information.

\textbf{Directly related secondary purpose}

6.26 For the use or disclosure of sensitive information, the secondary purpose must be ‘directly related’ to the primary purpose of collection. A directly related secondary purpose is one which is closely associated with the primary purpose, even if it is not strictly necessary to achieve that primary purpose. This requirement for a direct relationship recognises that the use and disclosure of sensitive information can have serious ramifications for the individual or their associates, including humiliation, embarrassment or loss of dignity.

6.27 An example of where a secondary purpose is directly related to the primary purpose of collection is:

- a health service provider collects health information about an individual for the purpose of providing treatment, and then decides, for ethical and therapeutic reasons, that they cannot treat the individual. The health service provider then advises another provider at the medical clinic of the individual’s need for treatment and of the provider’s inability to provide that treatment. This disclosure to the other provider is directly related to the purpose for which the information was collected, and would be within the individual’s reasonable expectations.\textsuperscript{14}

6.28 The use of sensitive information for the purpose of de-identifying the information will also be directly related to the primary purpose of collection.

\textbf{Using or disclosing personal information as required or authorised by law}

6.29 An APP entity may use or disclose personal information for a secondary purpose if the use or disclosure is required or authorised by or under an Australian law or a court/tribunal order (APP 6.2(b)).

6.30 The meaning of ‘required or authorised by or under an Australian law or a court/tribunal order’ is discussed in Chapter B (Key concepts).

6.31 Examples of where an APP entity may be required or authorised by law to use or disclose personal information include where:

- a warrant, order or notice issued by a court requires the entity to provide information, or produce records or documents that are held by the entity

- the entity is subject to a statutory requirement to report certain matters to an agency or enforcement body, for example, specific financial transactions, notifiable diseases and suspected cases of child abuse

\textsuperscript{13} \textit{N v Commonwealth Agency} [2009] PrivCmrA 17, Australasian Legal Information Institute website \texttt{<www.austlii.edu.au>},

\textsuperscript{14} \textit{F v Medical Specialist} [2009] PrivCmrA 8, Australasian Legal Information Institute website \texttt{<www.austlii.edu.au>}. 
• a law applying to the entity clearly and specifically authorises it to use or disclose the personal information, for example:
  o to give a record to the Private Health Insurance Ombudsman,\textsuperscript{15} or to disclose matters to a trustee conducting a bankruptcy investigation\textsuperscript{16}
  o a specified use or disclosure of personal information by an Agency Head, the Merit Protection Commissioner or the Australian Public Service Commissioner\textsuperscript{17}
  o a specified use or disclosure of personal information under the Privacy Act, for example, to de-identify personal information as required by APP 11.

Using or disclosing personal information where a permitted general situation exists

6.32 An APP entity may use or disclose personal information for a secondary purpose if a ‘permitted general situation’ exists in relation to the use or disclosure of the information by the entity (APP 6.2(e)).

6.33 Section 16A lists seven permitted general situations (two of which only apply to agencies). The seven situations are set out below, and are discussed in Chapter C (Permitted general situations), including the meaning of relevant terms.

**Lessening or preventing a serious threat to life, health or safety**

6.34 An APP entity may use or disclose personal information for a secondary purpose where:

• it is unreasonable or impracticable to obtain the individual’s consent to the use or disclosure, and

• the entity reasonably believes the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety (s 16A(1), Item 1).

6.35 Examples of where this permitted general situation might apply include:

• where an individual is seriously injured while interstate and, due to their injuries, cannot give informed consent, the individual’s usual health service provider may be able to disclose personal information about the individual to another health service provider who is treating the individual’s serious injuries on the basis that it is impracticable to obtain the individual’s consent

• where an APP entity that provides child protection services has evidence that a child is at risk of physical or sexual abuse by their parent, the entity may be able to disclose the personal information of the parent to another child protection service on the basis that it would be unreasonable to obtain the parent’s consent.

\textsuperscript{15} *Private Health Insurance Act 2007*, s 250.10.

\textsuperscript{16} *Bankruptcy Act 1966*, s 77A.

\textsuperscript{17} *Public Service Act 1999*, s 72E and Public Service Regulations 1999, regulation 9.2.
Chapter 6: APP6 — Use or disclosure of personal information

Taking appropriate action in relation to suspected unlawful activity or serious misconduct

6.36 An APP entity may use or disclose personal information for a secondary purpose where the entity:

- has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity’s functions or activities has been, is being or may be engaged in, and
- reasonably believes that the collection use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter (s 16A(1), Item 2).

6.37 Examples of where this permitted general situation might apply are the use of personal information by:

- an APP entity that is investigating fraudulent conduct by a professional adviser or a client in relation to the entity’s functions or activities
- an agency that is investigating a suspected serious breach by a staff member of the Australian Public Service Code of Conduct.

Locating a person reported as missing

6.38 An APP entity may use or disclose personal information for a secondary purpose where the entity:

- reasonably believes that the use or disclosure is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing, and
- the use or disclosure complies with rules made by the Commissioner under s 16A(2) (s 16A(1), Item 3).

Reasonably necessary for establishing, exercising or defending a legal or equitable claim

6.39 An APP entity may use or disclose personal information for a secondary purpose where the use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim (s 16A(1) Item 4).

6.40 An example of where this permitted general situation might apply is where an individual has made a claim under their life insurance policy and the insurer is preparing to dispute the claim. The insurer may use or disclose personal information about the individual to establish its defence of the claim.

Reasonably necessary for a confidential alternative dispute resolution processes

6.41 An APP entity may use or disclose personal information for a secondary purpose where the use or disclosure is reasonably necessary for the purposes of a confidential alternative dispute resolution (ADR) process (s 16A(1), Item 5).

6.42 An example of where this permitted general situation might apply is where an APP entity discloses their version of events during a confidential ADR process, where that account includes the disclosure of personal information about an individual who is
directly or indirectly involved in the dispute. This permitted general situation will only apply where the parties to the dispute and the ADR provider are bound by confidentiality obligations.

**Necessary for a diplomatic or consular function or activity**

6.43 An agency may use or disclose personal information for a secondary purpose where the agency reasonably believes that the use or disclosure is necessary for the agency’s diplomatic or consular functions or activities (s 16A(1), Item 6). This permitted general situation applies only to agencies, and not to organisations.

6.44 An example of where this permitted general situation might apply is where an agency with diplomatic or consular functions uses or discloses personal information to grant a diplomatic visa to a foreign national accredited as a member of the diplomatic staff of a mission to Australia.

**Necessary for certain Defence Force activities outside Australia**

6.45 The Defence Force (as defined in s 6(1)) may use or disclose personal information for a secondary purpose where it reasonably believes that the use or disclosure is necessary for a warlike operation, peacekeeping, civil aid, humanitarian assistance, a medical emergency, a civil emergency or disaster relief occurring outside Australia and the external Territories (s 16A(1), Item 7).

6.46 An example of where this permitted general situation might apply is where the Defence Force uses and discloses personal information about an enemy or other hostile adversary in order to support military operations.

**Using or disclosing personal information where a permitted health situation exists**

6.47 An organisation may use or disclose personal information if a ‘permitted health situation’ exists in relation to the use or disclosure (APP 6.2(d)). This exception applies only to organisations, and not to agencies.

6.48 Section 16B lists three permitted health situations that relate to the use or disclosure of health information or genetic information by an organisation. The three situations are set out below, and are discussed in Chapter D (Permitted health situations), including the meaning of relevant terms.

**Conducting research; compiling or analysing statistics; management, funding or monitoring of a health service**

6.49 An organisation may use or disclose health information about an individual for a secondary purpose if the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety, and:

- it is impracticable to obtain the individual’s consent to the use or disclosure
• the use or disclosure is conducted in accordance with guidelines approved under s 95A, and

• in the case of disclosure, the organisation reasonably believes that the recipient of the information will not disclose the information, or personal information derived from that information (s 16B(3)).

6.50 An example of where this permitted health situation might apply is where an organisation discloses health information to a researcher who is conducting public health research in circumstances where the age of the information makes it impracticable to obtain consent. The disclosing organisation should have a written agreement with the researcher which requires the researcher not to disclose the health information, or any personal information that is derived from that health information. The disclosure must be carried out in accordance with guidelines approved under s 95A.

Necessary to prevent a serious threat to the life, health or safety of a genetic relative

6.51 An organisation may use or disclose genetic information about an individual for a secondary purpose if:

• the organisation has obtained the information in the course of providing a health service to the individual

• the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another individual who is a genetic relative of the individual

• the use or disclosure is conducted in accordance with guidelines approved under s 95AA, and

• in the case of disclosure, the recipient of the information is a genetic relative of the individual (s 16B(4)).

6.52 An example of where this permitted health situation might apply is:

• in the course of providing a health service, an organisation obtains information that a patient has a pathogenic mutation in the Huntington disease gene, and

• the individual refuses to consent to the organisation disclosing any information to their genetic relatives, even after the individual has participated in discussions and counselling, and received information about the implications of the diagnosis for the individual’s genetic relatives

• despite this refusal, the organisation may disclose the genetic information to genetic relatives under this exception, providing any disclosure is in accordance with the guidelines approved under s95AA.

---

18 See National Health and Medical Research Council (NHMRC), Guidelines approved under Section 95A of the Privacy Act 1988, NHMRC website <www.nhmrc.gov.au>.

19 See National Health and Medical Research Council (NHMRC), Use and disclosure of genetic information to a patient’s genetic relatives under Section 95AA of the Privacy Act 1988: Guidelines for health practitioners in the private sector, NHMRC website <www.nhmrc.gov.au>.
Disclosure to a responsible person for the individual

6.53   An organisation may disclose health information about an individual for a secondary purpose if:

- the organisation provides a health service to the individual
- the recipient of the information is a ‘responsible person’ for the individual
- the individual is either physically or legally incapable of giving consent to the disclosure, or physically cannot communicate consent to the disclosure
- the individual providing the health service (the ‘carer’) is satisfied that either the disclosure is necessary to provide appropriate care or treatment of the individual, or the disclosure is made for compassionate reasons
- the disclosure is not contrary to any wish expressed by the individual before the individual became unable to give or communicate consent of which the carer is aware or of which the carer could reasonably be expected to be aware
- the disclosure is limited to the extent reasonable and necessary for providing appropriate care or fulfilling compassionate reasons (s 16B(5)).

6.54   An example of where this permitted health situation might apply is where an individual who cannot give consent is released from hospital into the care of family members. The health service provider (referred to in this exception as the ‘carer’) discloses health information to the family members to enable them to monitor the individual’s progress and administer medication. In these circumstances, the exception would apply where the carer is satisfied that the disclosure is necessary to provide appropriate care for the individual. The disclosure must be limited to the extent reasonable and necessary to provide appropriate care.

6.55   Another example is where a carer discloses health information to an unconscious patient’s family members about the patient’s condition. In these circumstances, the exception would apply where the carer is satisfied that the disclosure is necessary for compassionate reasons. The disclosure must be limited to the extent reasonable and necessary for the compassionate reasons.

Using or disclosing personal information for an enforcement related activity

6.56   An APP entity may use or disclose personal information for a secondary purpose where the entity reasonably believes that the use or disclosure of the personal information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body (APP 6.2(e)).

6.57   ‘Enforcement body’ is defined in s 6(1) as a list of specific bodies and is discussed in Chapter B (Key concepts). The list includes Commonwealth, State and Territory bodies that are responsible for policing, criminal investigations, and administering laws to protect the public revenue or to impose penalties or sanctions. Examples of Commonwealth enforcement bodies are the Australian Federal Police, Australian Crime
Commission, Customs, the Integrity Commissioner,20 the Immigration Department,21 Australian Prudential Regulation Authority, the Australian Securities and Investments Commission and AUSTRAC.

6.58 ‘Enforcement related activities’ is defined in s 6(1) and is discussed in Chapter B (Key concepts). Enforcement related activities include the prevention, detection, investigation and prosecution or punishment of criminal offences and intelligence gathering activities.

**Reasonable belief**

6.59 The phrase ‘reasonable belief’ is discussed in Chapter B (Key concepts). In summary, the APP entity must have a reasonable basis for the belief, and not merely a genuine or subjective belief. It is the responsibility of the entity to be able to justify its reasonable belief.

6.60 In some circumstances, the basis for an APP entity’s ‘reasonable belief’ will be clear, for example, if the entity discloses personal information in response to a written request by an enforcement body and the request is dated and signed by an authorised person. In other circumstances, the basis for this belief may be less clear, and the entity will need to reflect more carefully about whether its judgment is reasonable.

**Reasonably necessary**

6.61 The ‘reasonably necessary’ test is an objective test: whether a reasonable person who is properly informed would agree that the use or disclosure is reasonable in the circumstances. Again, it is the responsibility of an APP entity to be able to justify that the particular use or disclosure is reasonably necessary.

6.62 For example, investigators from an enforcement body suspect that a particular building is being used for drug trafficking activities. As part of the enforcement body’s intelligence gathering, the investigators request an APP entity to disclose the personal information of individuals associated with the building (although the investigators do not know the extent, if any, of the involvement of the individuals). This disclosure would be ‘reasonably necessary’ as it forms an important part of the enforcement body’s intelligence gathering about the suspected drug trafficking.

6.63 The use or disclosure does not need to relate to an existing enforcement related activity. The use or disclosure may be reasonably necessary for the initiation of an enforcement related activity. This recognises that a law enforcement body may not be in a position to prevent, detect or investigate offences or breaches of the law, unless and until certain information, including personal information, is brought to its attention.

6.64 An APP entity should ensure that it only uses or discloses the minimum amount of personal information reasonably necessary for a particular enforcement related activity. For example, an entity may hold a range of personal information about an individual, such as the person’s contact details, their photograph and information about their

---

20 ‘Integrity Commissioner is defined in s 6(1) as having the same meaning as in the Law Enforcement Integrity Commissioner Act 2006.

21 ‘Immigration Department’ is defined in s 6(1) as the Department administered by the Minister administering the Migration Act 1958.
political views and religious views. Before disclosing all of this personal information to the enforcement body, the entity should consider whether only some of it is reasonably necessary for the enforcement related activity. If so, it should disclose only that information.

**Making a written note of use or disclosure for this secondary purpose**

6.65 If an APP entity uses or discloses personal information in accordance with the ‘enforcement related activities’ exception in APP 6.2(e), the entity must make a written note of the use or disclosure (APP 6.5).

6.66 The APP entity could include the following details in that note:

- the date of the use or disclosure
- details of the personal information that was used or disclosed
- the enforcement body conducting the enforcement related activity
- if the entity used the personal information, how the personal information was used by the entity
- if the entity disclosed the personal information, who it disclosed the personal information to (this may be the enforcement body or another entity)
- the basis for the entity’s ‘reasonable belief’. This will help the entity assure itself that this exception applies, and it may be a useful reference if the entity later needs to justify its reasonable belief.

6.67 This requirement does not apply where a law prohibits the APP entity from making such a record.

**Disclosing biometric information to an enforcement body**

6.68 An agency may disclose biometric information or biometric templates for a secondary purpose if:

- the agency is not an enforcement body, and
- the recipient of the information is an enforcement body, and
- the disclosure is conducted in accordance with guidelines made by the Commissioner for the purposes of APP 6.3 (see APP 6.3, Chapter 6).

6.69 This exception does not apply to organisations.

6.70 ‘Biometric information’ and ‘biometric templates’ are types of ‘sensitive information’ (defined in s 6(1)). ‘Enforcement body’ is defined in s 6(1) and is discussed in more detail in Chapter B (Key concepts).

**De-identifying certain health information before disclosure**

6.71 APP 6.4 applies where an organisation collects health information under an exception to APP 3 in s 16B(2). Section 16B(2) outlines the permitted health situation that
allows an organisation to collect health information about an individual if the collection is necessary for research relevant to public health or safety, the compilation or analysis of statistics relevant to public health or public safety, or the management, funding or monitoring of a health service and certain other criteria are satisfied (see Chapter D (Permitted health situations)).

6.72 In these circumstances, APP 6.4 requires the organisation to take reasonable steps to ensure that the information is de-identified, before it discloses the information in accordance with APPs 6.1 or 6.2.

6.73 Personal information is de-identified ‘if the information is no longer about an identifiable individual or an individual who is reasonably identifiable’ (s 6(1)). De-identification is discussed in more detail in Chapter B (Key concepts).  

6.74 The reasonable steps that an organisation should take will depend upon circumstances that include:

- the possible adverse consequences for an individual if their health information is not de-identified before it is disclosed. More rigorous steps may be required as the risk of adversity increases
- the practicability, including time and cost involved. However, an organisation is not excused from taking particular steps to de-identify health information by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances.

Related bodies corporate

Disclosing personal information to a related body corporate

6.75 Section 13B(1)(b) provides that where a body corporate discloses personal information (other than sensitive information) to a related body corporate, this is generally not considered ‘an interference with the privacy of an individual’ under the Privacy Act (interferences with privacy are discussed in Chapter A (Introductory matters)). This provision applies to related bodies corporate and not to other corporate relationships, such as a franchise or joint-venture relationship.  

6.76 The effect of this provision is that an APP entity may disclose personal information (other than sensitive information) to a related body corporate without relying on an exception in APP 6.2.

---


23 Section 6(8) states ‘for the purposes of this Act, the question of whether bodies corporate are related to each other is determined in the manner in which that question is determined under the Corporations Act 2001’.
Using or disclosing personal information collected from a related body corporate

6.77 An APP entity that collects personal information from a related body corporate is taken to have the same primary purpose of collection as its related body corporate (APP 6.6). Under APP 6, the entity may only use or disclose the personal information for that primary purpose, unless an exception to that principle applies (see paragraph 6.2 above).

For example, an APP entity collects personal information about an applicant contractor for the purpose of assessing their suitability to perform work on its behalf. The parent company then collects that personal information from the entity. The primary purpose of this collection is taken to be the same as the original purpose of collection. The parent company may only disclose the personal information to a third party for another purpose, where an exception to APP 6 applies.
Chapter 7: Australian Privacy Principle 7 — Direct marketing

Version 1.0, February 2014

Key points

What does APP 7 say?

‘Direct marketing’

When are agencies covered by APP 7?

Using and disclosing personal information for the purpose of direct marketing where reasonably expected by the individual

Reasonably expect

Providing a simple means for ‘opting out’

Using and disclosing personal information for the purpose of direct marketing where no reasonable expectation of the individual, or information collected from a third party

Consent

Impracticable to obtain consent

Providing a prominent statement about simple means for ‘opting out’

Using and disclosing sensitive information for the purpose of direct marketing with the individual’s consent

Using and disclosing personal information for the purpose of direct marketing by contracted service providers

Requests by an individual to stop direct marketing communications

Requests by an individual to stop facilitating direct marketing

When does an organisation ‘facilitate’ direct marketing?

Requests by an individual to identify the source of the personal information

Interaction with other legislation
Key points

- APP 7 provides that an organisation must not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies. APP 7 may also apply to an agency in the circumstances set out in s 7A.

- Direct marketing involves the use or disclosure of personal information to communicate directly with an individual to promote goods and services.

- Where an organisation is permitted to use or disclose personal information for the purpose of direct marketing, it must always:
  - allow an individual to request not to receive direct marketing communications (also known as ‘opting out’), and
  - comply with that request.

- An organisation must, on request, provide its source for an individual’s personal information, unless it is impracticable or unreasonable to do so.

What does APP 7 say?

7.1 An organisation must not use or disclose the personal information that it holds about an individual for the purpose of direct marketing (APP 7.1). The term ‘holds’ is discussed in Chapter B (Key concepts).

7.2 There are a number of exceptions to this requirement. The exceptions in APP 7.2 and 7.3 apply to personal information other than sensitive information. They draw a distinction between the use or disclosure of personal information by an organisation where:

- the personal information has been collected directly from an individual, and the individual would reasonably expect their personal information to be used for the purpose of direct marketing (APP 7.2), and

- the personal information has been collected from a third party, or from the individual directly but the individual does not have a reasonable expectation that their personal information will be used for the purpose of direct marketing (APP 7.3). Sources of third party data include data list providers, third party mobile applications, third party lead generation and enhancement data.

7.3 Both of these exceptions require an organisation to provide a simple means by which an individual can request not to receive direct marketing communications (also known as ‘opting out’). However, in the circumstances where the organisation has not obtained personal information from the individual, or the individual would not reasonably expect their personal information to be used in this way, there are additional requirements to ensure that the individual is made aware of their right to opt out of receiving direct marketing communications from the organisation.

7.4 Exceptions to this principle also apply in relation to:
• sensitive information (APP 7.4), and
• an organisation that is a contracted service provider for a Commonwealth contract (APP 7.5).

7.5 APP 7 may apply to an agency in the circumstances set out in s 7A (see paragraph 7.13 below).

7.6 An individual may request an organisation not to use or disclose their personal information for the purpose of direct marketing, or for the purpose of facilitating direct marketing by other organisations (APP 7.6). The organisation must give effect to any such request by an individual within a reasonable period of time and for free (APP 7.7).

7.7 An organisation must, on request, notify an individual of its source of the individual’s personal information that it has used or disclosed for the purpose of direct marketing unless this is unreasonable or impracticable to do so (APP 7.6).

7.8 APP 7 does not apply to the extent that the Do Not Call Register Act 2006, the Spam Act 2003 or any other legislation prescribed by the regulations apply (APP 7.8). APP 7 will still apply to the acts or practices of an organisation that are exempt from these Acts.

‘Direct marketing’

7.9 Direct marketing involves the use and/or disclosure of personal information to communicate directly with an individual to promote goods and services. A direct marketer may communicate with an individual through a variety of channels, including telephone, SMS, mail, email and online advertising.

7.10 Organisations involved in direct marketing often collect personal information about an individual from a variety of sources, including:

• public records, such as telephone directories and land title registers
• membership lists of business, professional and trade organisations
• online, paper-based or phone surveys and competitions
• online accounts, for example, purchase history or the browsing habits of identified, or logged in, users
• mail order or online purchases.

7.11 Examples of direct marketing by an organisation include:

• sending an individual a catalogue in the mail addressed to them by name

---

1 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 81.
2 For more information about online behavioural advertising and personal information, see OAIC, Privacy Fact Sheet 4 — Online behavioural advertising: Know your choices, December 2011, OAIC website <www.oaic.gov.au>.
• displaying an advertisement on a social media site that an individual is logged into, using personal information, including data collected by cookies relating to websites the individual has viewed.

• sending an email to an individual about a store sale, or other advertising material relating to the store, using personal information provided by the customer in the course of signing up for a store loyalty card.

7.12 Marketing is not direct, and therefore APP 7.1 does not apply, if personal information is not used or disclosed to identify or target particular recipients, for example, where:

• an organisation sends catalogues by mail to all mailing addresses in a particular location, addressed ‘To the householder’ (that is, where recipients are not selected on the basis of personal information)

• an organisation hand delivers promotional flyers to the mailboxes of local residents

• an organisation displays advertisements on a website, but does not use personal information to select which advertisements are displayed.

When are agencies covered by APP 7?

7.13 An agency must comply with the direct marketing requirements of APP 7 in the circumstances set out in s 7A. These circumstances include where:

• the agency is listed in Part 1 of Schedule 2 to the Freedom of Information Act 1982 (the FOI Act) and is prescribed in regulations, or

• the act or practice relates to the commercial activity of an agency specified in Part 2 of Schedule 2 to the FOI Act.

Using and disclosing personal information for the purpose of direct marketing where reasonably expected by the individual

7.14 APP 7.2 provides that an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

• the organisation collected the personal information from the individual

---

3 For more information about cookies, see OAIC, Privacy Fact Sheet 4 — Online behavioural advertising: Know your choices, December 2011, OAIC website <www.oaic.gov.au>.


• the individual would reasonably expect the organisation to use or disclose the personal information for that purpose
• the organisation provides a simple way for the individual to request not to receive direct marketing communications from the organisation (also known as ‘opting out’), and
• the individual has not made such a request to the organisation.

Reasonably expect

7.15 The ‘reasonably expect’ test is an objective test that has regard to what a reasonable person, who is properly informed, would expect in the circumstances. This is a question of fact in each individual case. It is the responsibility of the organisation to be able to justify its conduct.

7.16 Factors that may be important in deciding whether an individual has a reasonable expectation that their personal information will be used or disclosed for the purpose of direct marketing include where:

• the individual has consented to the use or disclosure of their personal information for that purpose (see discussion in paragraph 7.23 below and Chapter B (Key concepts) for further information about the elements of consent)
• the organisation has notified the individual that one of the purposes for which it collects the personal information is for the purpose of direct marketing under APP 5.1 (see Chapter 5 (APP 5))
• the organisation made the individual aware that they could request not to receive direct marketing communications from the organisation, and the individual does not make such a request (see paragraph 7.21).

7.17 An organisation should not assume that an individual would reasonably expect their personal information to be used or disclosed for the purpose of direct marketing just because the organisation believes that the individual would welcome the direct marketing, for example, because of the individual’s profession, interest or hobby.

7.18 An individual is not likely to have a reasonable expectation that their personal information will be used or disclosed for the purpose of direct marketing where the organisation has notified the individual that their personal information will only be used for a particular purpose unrelated to direct marketing. For example, where an individual provides personal information to their bank when setting up internet banking, and the bank tells the individual that it will only use that personal information for enabling security for internet banking, the individual is not likely to have a reasonable expectation that their personal information will then be used or disclosed for the purpose of direct marketing.6

---

Providing a simple means for ‘opting out’

7.19 A simple means for opting out should include:

- a visible, clear and easily understood explanation of how to opt out, for example, instructions written in plain English and in a font size that is easy to read
- a process for opting out, which requires minimal time and effort
- an opt out process that uses a straightforward and accessible communication channel, or channels. For example, the same communication channel that the organisation used to deliver the direct marketing communication. However, in some circumstances, a straightforward and accessible communication channel may be a different channel to that used to deliver the direct marketing communication, such as telephone and email, where the original channel was post, and
- an opt out process that is free, or that does not involve more than a nominal cost for the individual, for example, the cost of a local phone call, text message or postage stamp.

7.20 The individual should be able to easily find out how to opt out. For example, an organisation could provide information about how to opt out in each direct marketing communication. An organisation should also consider whether the means for opting out is accessible to a person with a disability.

7.21 If the individual has ‘opted out’, the organisation must not use or disclose their personal information for the purpose of direct marketing, in accordance with the individual’s request (APP 7.2(d)). Further examples of a simple means to opt out are given in paragraphs 7.27–7.30 below.

Using and disclosing personal information for the purpose of direct marketing where no reasonable expectation of the individual, or information collected from a third party

7.22 APP 7.3 provides that an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

- the organisation collected the information from:
  - the individual, but the individual would not reasonably expect their information to be used or disclosed for that purpose, or
  - a third party, and
- the individual has consented to use or disclosure for that purpose, or it is impracticable to obtain that consent, and
- the organisation provides a simple way for the individual to opt out of receiving direct marketing communications from the organisation, and
• in each direct marketing communication with the individual, the organisation includes a prominent statement, or otherwise draws the individual’s attention to the fact that the individual may make such a request (referred to as an ‘opt out statement’), and

• the individual has not made such a request to the organisation.

**Consent**

7.23 Consent is defined in s 6(1) as ‘express consent or implied consent’ and is discussed generally in Chapter B (Key concepts). The four key elements of consent are:

• the individual is adequately informed before giving consent

• the individual gives consent voluntarily

• the consent is current and specific, and

• the individual has the capacity to understand and communicate their consent.

**Impracticable to obtain consent**

7.24 Whether it is ‘impracticable’ for an organisation to obtain consent will depend on a number of factors, including the time and cost involved in seeking consent. However, an organisation is not excused from obtaining consent by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it impracticable to obtain consent will depend on whether the burden is excessive in all the circumstances.

7.25 An organisation may obtain the consent from the individual in relation to a subsequent use or disclosure of the individual’s personal information for the purpose of direct marketing at the time it collects the personal information. In order to rely on this consent, the organisation must be satisfied that it is still current at the time of the use or disclosure. ‘Current’ consent is discussed in Chapter B (Key concepts).

7.26 Where an organisation did not obtain the individual’s consent at the time of collection, it must obtain the consent of the individual for the proposed use or disclosure, unless it is impracticable to do so. In that case, the organisation should assess whether it is impracticable to obtain consent at the time of the proposed use or disclosure.

**Providing a prominent statement about simple means for ‘opting out’**

7.27 APP 7.3 requires that an organisation provides a simple means for an individual to opt out of receiving direct marketing communications (see discussion at paragraphs 7.19–7.21 above).

7.28 In addition, APP 7.3 requires an organisation to provide a prominent statement that the individual may request to opt out in each direct marketing communication. This statement should meet the following criteria:

• it should be written in plain English, and not use legal or industry jargon
• it should be positioned prominently, and not hidden amongst other text. Headings may be necessary to draw attention to the statement, and
• it should be published in a font size and type which is easy to read, for example, in at least the same font size as the main body of text in the communication.

7.29 The following are given as examples of ways that an organisation may comply with the ‘opt out’ requirements of APP 7.3:

• clearly indicating in each direct marketing email that the individual can opt out of receiving future emails by replying with a single word instruction in the subject line (for example, ‘unsubscribe’). Alternatively, ensuring that a link is prominently located in the email, which takes the individual to a subscription control centre
• clearly indicating that the individual can opt out of future direct marketing by replying to a direct marketing text message with a single word instruction (for example, ‘STOP’)
• telling the recipient of a direct marketing phone call that they can verbally opt out from any future calls
• including instructions about how to opt out from future direct marketing in each mailed communication.

7.30 In each case, an organisation may use an opt out mechanism that provides the individual with the opportunity to indicate their direct marketing communication preferences, including the extent to which they wish to opt out. However, the organisation should always provide the individual with an option to opt out of all future direct marketing communications as one of these preferences.

Using and disclosing sensitive information for the purpose of direct marketing with the individual’s consent

7.31 APP 7.4 provides that an organisation may use or disclose sensitive information for the purpose of direct marketing if the individual has consented to the use or disclosure for that purpose.

7.32 The requirement to obtain consent applies even if the individual and the organisation have a pre-existing relationship.7 If consent is not obtained, the organisation cannot rely on this exception, even if obtaining consent is impracticable or impossible in the circumstances.

7.33 Consent is discussed in paragraph 7.23 below, and generally in Chapter B (Key concepts). ‘Sensitive information’ is defined in s 6(1) and discussed in Chapter B (Key concepts).

---

7 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 82.
Using and disclosing personal information for the purpose of direct marketing by contracted service providers

7.34 APP 7.5 provides that an organisation that is a contracted service provider for a Commonwealth contract may use or disclose personal information for the purpose of direct marketing if:

• it collects the information for the purpose of meeting (directly or indirectly) an obligation under the contract, and
• the use or disclosure is necessary to meet (directly or indirectly) such an obligation.

7.35 The terms ‘contracted service provider’ and ‘Commonwealth contract’ are defined in s 6(1) and discussed in Chapter A (Introductory matters).

Requests by an individual to stop direct marketing communications

7.36 If an organisation uses or discloses personal information about an individual for the purpose of direct marketing, the individual may request not to receive direct marketing communications from that organisation (APP 7.6(c)).

7.37 The organisation must not charge the individual for making or giving effect to the request (APP 7.7). It must also stop sending the direct marketing communications within a reasonable period after the request is made (APP 7.7(a)). A ‘reasonable period’ would generally be no more than 30 days. However, an organisation could give effect to an opt-out request in a shorter timeframe, particularly where digital communication channels are being utilised.

7.38 When the first organisation engages a second organisation to carry out, or assist in carrying out direct marketing on its behalf, it should ensure that the contractual arrangements with the second organisation reflect the first organisation’s obligations under APP 7. Where the second organisation is an APP entity, it must also comply with the APPs when handling personal information (see also paragraph 7.44 below).

7.39 In particular, where an individual makes a request to the second organisation to stop the direct marketing under APP 7.6, the contractual arrangements between the two organisations could require the second organisation to give effect to or pass on the opt out request to the first organisation.

Requests by an individual to stop facilitating direct marketing

7.40 An individual may request an organisation not to use or disclose personal information about the individual for the purpose of facilitating direct marketing by a second organisation (APP 7.6(d)).
7.41 The organisation must not charge the individual for making or giving effect to the request (APP 7.7). It must also stop using or disclosing the personal information for the purpose of facilitating direct marketing by a second organisation within a reasonable period after the request is made (APP 7.7(a)). A ‘reasonable period’ would be no more than 30 days. However, an organisation could give effect to an opt-out request in a shorter timeframe, particularly when digital communication channels are being utilised.

7.42 Where the second organisation is an APP entity, an individual can also make a separate request to not receive direct marketing communications from that organisation (APP 7.6(c)).

When does an organisation ‘facilitate’ direct marketing?

7.43 An organisation (the first organisation) facilitates direct marketing where it collects personal information for the purpose of providing that personal information to another organisation (the second organisation), so that the second organisation can undertake direct marketing of its own products or services. For example, an organisation facilitates direct marketing where it collects personal information and sells that personal information to the second organisation which uses or discloses the personal information to send out marketing material.

7.44 An organisation does not facilitate direct marketing where it engages a second organisation to carry out, or assist in carrying out, direct marketing on its own behalf. In these circumstances, the second organisation will usually be a contractor, or an agent of the first organisation (see paragraphs 7.38–7.39 above). The following are given as examples of where an organisation ‘carries out’ direct marketing through a contractor, rather than facilitates direct marketing by a second organisation:

- an organisation engages a mailing house to mail out its direct marketing communications
- an organisation engages a second organisation to conduct door-to-door marketing or telemarketing on its behalf.

Requests by an individual to identify the source of the personal information

7.45 An individual may ask an organisation to identify the source of the personal information that it uses or discloses for the purpose of direct marketing, or for the purpose of facilitating direct marketing by other organisations (APP 7.6(e)).

7.46 The organisation must then notify the individual of its source, unless this is impracticable or unreasonable (APP 7.7(b)). It is the responsibility of the organisation to be able to justify that it is impracticable or unreasonable to provide this notification. Relevant considerations may include:

---

8 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 82.
• the possible adverse consequences for the individual if they are not notified of the source
• the length of time that has elapsed since the personal information was collected by the organisation
• for personal information collected before commencement of APP 7, whether the source of the personal information was recorded
• the time and cost involved. However, an organisation is not excused from notifying an individual by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to do so will depend on whether the burden is excessive in all the circumstances.

7.47 Notification of the source of the personal information must be given within a reasonable period after the request is made (APP 7.7(b)). A ‘reasonable period’ would generally be 30 days unless special circumstances apply.

Interaction with other legislation

7.48 The Spam Act 2003 (Spam Act) and the Do Not Call Register Act 2006 (DNCR Act) contain specific provisions regarding direct marketing. Where the act or practice of an APP entity is subject to the Spam Act, DNCR Act, or other legislation prescribed under the regulations, APP 7 does not apply to the extent that this legislation applies (APP 7.8).

7.49 If an organisation that is an APP entity is exempt or partially exempt from the Spam Act or DNCR Act, APP 7 will still apply to the acts and practices of that organisation to the extent of that exemption.
Chapter 8: Australian Privacy Principle 8 — Cross-border disclosure of personal information

Version 1.1, March 2015

Key points

What does APP 8 say?

‘Overseas recipient’

When does an APP entity ‘disclose’ personal information about an individual to an overseas recipient?

Providing personal information to a contractor

Taking reasonable steps to ensure an overseas recipient does not breach the APPs

Disclosing personal information to an overseas recipient that is subject to a substantially similar law or binding scheme

Reasonable belief

Law or binding scheme

Substantially similar to

Mechanisms to enforce privacy protections

Disclosing personal information to an overseas recipient with the individual’s consent after the individual is expressly informed

Expressly inform

Consent

Disclosing personal information to an overseas recipient as required or authorised by law

Disclosing personal information to an overseas recipient where a permitted general situation exists

Lessening or preventing a serious threat to life, health or safety

Taking appropriate action in relation to suspected unlawful activity or serious misconduct

Locating a person reported as missing

Necessary for a diplomatic or consular function or activity

Necessary for certain Defence Force activities outside Australia

Disclosing personal information to an overseas recipient as required or authorised under an international agreement relating to information sharing

Disclosing personal information to an overseas recipient for an enforcement related activity
When is an APP entity accountable for personal information that it discloses to an overseas recipient?

Overseas acts or practices required by a foreign law
Key points

- Before an APP entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information (APP 8.1).

- An APP entity that discloses personal information to an overseas recipient is accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs (s 16C).

- There are exceptions to the requirement in APP 8.1 to take reasonable steps and to the accountability provision in s 16C.

What does APP 8 say?

8.1 APP 8 and s 16C create a framework for the cross-border disclosure of personal information. The framework generally requires an APP entity to ensure that an overseas recipient will handle an individual’s personal information in accordance with the APPs, and makes the APP entity accountable if the overseas recipient mishandles the information.1 This reflects a central object of the Privacy Act, of facilitating the free flow of information across national borders while ensuring that the privacy of individuals is respected (s 2A(f)).

8.2 APP 8.1 provides that before an APP entity discloses personal information about an individual to an overseas recipient, the entity must take reasonable steps to ensure that the recipient does not breach the APPs in relation to that information. Where an entity discloses personal information to an overseas recipient, it is accountable for an act or practice of the overseas recipient that would breach the APPs (s 16C).

8.3 There are exceptions to the requirement in APP 8.1 and to the accountability provision in s 16C (see paragraphs 8.19–8.55 below).

8.4 When an APP entity discloses personal information to an overseas recipient it will also need to comply with APP 6. That is, it must only disclose the personal information for the primary purpose for which it was collected unless an exception to that principle applies (see Chapter 6 (APP 6)). A note to APP 6.1 cross-references the requirements for the cross-border disclosure of personal information in APP 8. It is implicit in this note, that APP 8 only applies to personal information covered by APP 6. That is, it only applies to personal information ‘held’ by an APP entity. The term ‘holds’ is discussed in Chapter B (Key concepts).

---

‘Overseas recipient’

8.5  Under APP 8.1, an ‘overseas recipient’ is a person who receives personal information from an APP entity and is:

- not in Australia or an external Territory
- not the APP entity disclosing the personal information, and
- not the individual to whom the personal information relates.

8.6  This means that where an APP entity in Australia sends information to an overseas office of the entity, APP 8 will not apply as the recipient is the same entity.\(^2\) This is to be distinguished from the case where an APP entity in Australia sends personal information to a ‘related body corporate’ located outside of Australia.\(^3\) In that case, the related body corporate is a different entity to the APP entity in Australia. It will therefore be an ‘overseas recipient’ and APP 8 will apply.\(^4\)

When does an APP entity ‘disclose’ personal information about an individual to an overseas recipient?

8.7  The term ‘disclose’ is not defined in the Privacy Act.

8.8  An APP entity discloses personal information where it makes it accessible to others outside the entity and releases the subsequent handling of the information from its effective control. The release of the information may be a proactive release or publication, a release in response to a specific request, an accidental release or an unauthorised release by an employee.\(^5\) This focuses on the act done by the disclosing party. The state of mind or intentions of the recipient does not affect the act of disclosure. Further, there will be a disclosure in these circumstances even where the information is already known to the overseas recipient.

8.9  In the context of APP 8, an APP entity will disclose personal information to an overseas recipient where it, for example:

- shares the personal information with an overseas recipient
- reveals the personal information at an international conference or meeting overseas

\(^2\) Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.

\(^3\) Section 6(8) provides ‘for the purposes of this Act, the question whether bodies corporate are related to each other is determined in the manner in which that question is determined under the Corporations Act 2001.’

\(^4\) Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 states ‘APP 8 will apply where an organisation sends personal information to a ‘related body corporate’ located outside Australia’ (p 83). While s 13B(1) permits related bodies corporate to share personal information (unless an exception applies), it does not exempt an APP entity from complying with APP 8 before it discloses personal information to a related body corporate located overseas.

\(^5\) An APP entity is taken to have ‘disclosed’ personal information where an employee carries out an unauthorised disclosure ‘in the performance of the duties of the person’s employment’ (s 8(1)).
• sends a hard copy document or email containing an individual’s personal information to an overseas client

• publishes the personal information on the internet, whether intentionally or not, and it is accessible to an overseas recipient.

8.10 ‘Disclosure’ is a separate concept from:

• ‘unauthorised access’ which is addressed in APP 11. An APP entity is not taken to have disclosed personal information where a third party intentionally exploits the entity’s security measures and gains unauthorised access to the personal information. Examples include unauthorised access following a cyber-attack6 or a theft, including where the third party then makes that personal information available to others outside the entity.7 However, where a third party gains unauthorised access, the APP entity may breach APP 11 if it did not take reasonable steps to protect the personal information from unauthorised access (see Chapter 11 (APP 11))

• ‘use’. An APP entity uses personal information where it handles, or undertakes an activity with the personal information, within the entity’s effective control. For example, where an entity provides personal information to an overseas recipient, via a server in a different overseas location, there would not usually be a disclosure until the personal information reaches the overseas recipient. That is, routing personal information, in transit, through servers located outside Australia, would usually be considered a ‘use’.8 In limited circumstances, the provision of personal information to a contractor may also be a ‘use’ of that personal information (see paragraphs 8.12–8.15 below).

8.11 For further information about the concepts of ‘use’ and ‘disclosure’ of personal information, see Chapter B (Key concepts).

**Providing personal information to a contractor**

8.12 Where an APP entity engages a contractor located overseas to perform services on its behalf, in most circumstances, the provision of personal information to that contractor is a disclosure. This means that the entity will need to comply with APP 8 before making that disclosure. Where a subcontractor may be engaged, the entity should also take reasonable steps to ensure that the subcontractor does not breach the APPs in relation to the personal information.9

8.13 For example, the provision of personal information to a contractor is generally considered a ‘disclosure’ where:

---


7 The actions of an employee will be attributed to the APP entity where it was carried out ‘in the performance of the duties of the person’s employment’ (s 8(1)).

8 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.

9 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.
• an Australian based retailer outsources the processing of online purchases through its website to an overseas contractor and, in order to facilitate this, provides the overseas contractor with personal information about its customers

• an Australian entity, as part of a recruitment drive, provides the personal information of job applicants to an overseas services provider to perform reference checks on behalf of the Australian entity

• an Australian organisation relies on its overseas parent company to provide technical and billing support, and as part of this, provides the overseas parent company with access to its Australian customer database (which includes personal information).

8.14 However, in limited circumstances providing personal information to an overseas contractor to perform services on behalf of the APP entity may be a use, rather than a disclosure. This occurs where the entity does not release the subsequent handling of personal information from its effective control. In these circumstances, the entity would not need to comply with APP 8. For example, where an APP entity provides personal information to a cloud service provider located overseas for the limited purpose of performing the services of storing and ensuring the entity may access the personal information, this may be a ‘use’ by the entity in the following circumstances:

• a binding contract between the entity and the provider requires the provider only to handle the personal information for these limited purposes

• the contract requires any subcontractors to agree to the same obligations, and

• the contract gives the entity effective control of how the personal information is handled by the overseas recipient. Issues to consider include whether the entity retains the right or power to access, change or retrieve the personal information, who else will be able to access the personal information and for what purposes, what type of security measures will be used for the storage and management of the personal information (see also APP 11.1, Chapter 11) and whether the personal information can be retrieved or permanently deleted by the entity when no longer required or at the end of the contract.  

8.15 Where the provision of personal information to an overseas contractor is a use, an APP entity may breach the APPs if the information is mishandled while in the overseas contractor’s physical possession. This is because the APP entity is considered to still 'hold' the information (as it has effective control of the information), and a number of APPs apply to an entity that ‘holds’ personal information (‘holds’ is discussed in Chapter B(Key Concepts)).

---

Taking reasonable steps to ensure an overseas recipient does not breach the APPs

8.16 The requirement in APP 8.1 to ensure that an overseas recipient does not breach the APPs is qualified by a ‘reasonable steps’ test. It is generally expected that an APP entity will enter into an enforceable contractual arrangement with the overseas recipient that requires the recipient to handle the personal information in accordance with the APPs (other than APP 1).\(^\text{11}\) Contractual arrangements may include:

- the types of personal information to be disclosed and the purpose of disclosure
- a requirement that the overseas recipient complies with the APPs in relation to the collection, use, disclosure, storage and destruction or de-identification of personal information. This should also require the overseas recipient to enter a similar contractual arrangement with any third parties to whom it discloses the personal information (for example, a subcontractor)
- the complaint handling process for privacy complaints
- a requirement that the recipient implement a data breach response plan which includes a mechanism for notifying the APP entity where there are reasonable grounds to suspect a data breach and outlines appropriate remedial action (based on the type of personal information to be handled under the contract).\(^\text{12}\)

8.17 However, whether reasonable steps to ensure the overseas recipient does not breach the APPs requires a contract to be entered into, the terms of the contract, and the steps the APP entity takes to monitor compliance with any contract (such as auditing), will depend upon the circumstances that include:

- the sensitivity of the personal information. More rigorous steps may be required if the information is ‘sensitive information’ (defined in s 6(1) and discussed in Chapter B (Key concepts)) or other personal information of a sensitive nature
- the entity’s relationship with the overseas recipient. More rigorous steps may be required if an entity discloses information to an overseas recipient to which it has not previously disclosed personal information
- the possible adverse consequences for an individual if the information is mishandled by the overseas recipient. More rigorous steps may be required as the risk of adversity increases.
- existing technical and operational safeguards implemented by the overseas recipient which will protect the privacy of the personal information — more rigorous steps may be required where the recipient has limited safeguards in place
- the practicability, including time and cost involved. However, an entity is not excused from ensuring that an overseas recipient does not breach the APPs by

\(^\text{11}\) Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.

reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances.

8.18 Where an agency discloses personal information to a recipient that is engaged as a contracted service provider, the agency must also comply with s 95B. Section 95B(1) provides that an agency must take contractual measures to ensure that a contracted service provider does not do an act, or engage in a practice, that would breach an APP if done by that agency. The contract must contain provisions to ensure that such an act or practice is not authorised by a subcontract (s 95B(3)). Contractual measures taken under s 95B will generally satisfy the requirement in APP 8.1.

**Disclosing personal information to an overseas recipient that is subject to a substantially similar law or binding scheme**

8.19 An APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where the entity reasonably believes that:

- the overseas recipient is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way the APPs protect the information, and
- mechanisms can be accessed by the individual to enforce that protection of the law or binding scheme (APP 8.2(a)).

**Reasonable belief**

8.20 The term ‘reasonably believe’ is discussed in Chapter B (Key concepts). In summary, an APP entity must have a reasonable basis for its belief, and not merely a genuine or subjective belief. For example, this might be based on independent legal advice. It is the responsibility of an APP entity to be able to justify its reasonable belief.

**Law or binding scheme**

8.21 An overseas recipient may be subject to a law or binding scheme, where, for example, it is:

- bound by a privacy or data protection law that applies in the jurisdiction of the recipient
- required to comply with another law that imposes obligations in relation to the handling of personal information, for example some taxation law includes provisions that expressly authorise and prohibit specified uses and disclosures, permit the retention of some data, require destruction after a certain period of time and under particular circumstances, and include a right of access to an individual’s personal information
- subject to an industry scheme or privacy code that is enforceable once entered into, irrespective of whether the recipient was obliged or volunteered to participate or subscribe to the scheme or code
- subject to Binding Corporate Rules (BCRs). BCRs allow multinational corporations, international organisations and groups of companies to make intra-organisational
transfers of personal information across borders in compliance with EU Data Protection law. BCRs typically form a stringent, intra-corporate global privacy policy that satisfies EU standards. The Article 29 Working Party issued several guidance documents on BCR content, acceptance criteria and submission process.

8.22 However, an overseas recipient may not be subject to a law or binding scheme where, for example:

- the overseas recipient is exempt from complying, or is authorised not to comply, with part, or all of the privacy or data protection law in the jurisdiction
- the recipient can opt out of the binding scheme without notice and without returning or destroying the personal information.

**Substantially similar to**

8.23 A substantially similar law or binding scheme would provide a comparable, or a higher level of privacy protection to that provided by the APPs. Each provision of the law or scheme is not required to correspond directly to an equivalent APP. Rather, the overall effect of the law or scheme is of central importance.

8.24 Whether there is substantial similarity is a question of fact. Factors that may indicate that the overall effect is substantially similar, include:

- the law or scheme includes a comparable definition of personal information that would apply to the personal information disclosed to the recipient
- the law or scheme regulates the collection of personal information in a comparable way
- the law or scheme requires the recipient to notify individuals about the collection of their personal information
- the law or scheme requires the recipient to only use or disclose the personal information for authorised purposes
- the law or scheme includes comparable data quality and data security standards
- the law or scheme includes a right to access and seek correction of personal information.

**Mechanisms to enforce privacy protections**

8.25 An enforcement mechanism should meet two key requirements: it should be accessible to the individual and it should have effective powers to enforce the privacy or data protections in the law or binding scheme. A range of mechanisms may satisfy those requirements, ranging from a regulatory body similar to the Office of the Australian Information Commissioner (the OAIC), to an accredited dispute resolution scheme, an independent tribunal or a court with judicial functions and powers. Factors that may be

---


relevant in deciding whether there is an accessible and effective enforcement mechanism include whether the mechanism:

- is independent of the overseas recipient that is required by the law or binding scheme to comply with the privacy or data protections
- has authority to consider a breach of any of the privacy or data protections in the law or binding scheme
- is accessible to an individual, for example, the existence of the scheme is publicly known, and can be accessed by individuals directly and without payment of any unreasonable charge
- has the power to make a finding that the overseas recipient is in breach of the law or binding scheme and to provide a remedy to the individual
- is required to operate according to principles of procedural fairness.

8.26 The mechanism may be a single mechanism or a combination of mechanisms. It may be established by the law or binding scheme that contains the privacy or data protections, or by another law or binding scheme. Alternatively, the mechanism may take effect through the operation of cross-border enforcement arrangements between the OAIC and an appropriate regulatory authority in the foreign jurisdiction.15

**Disclosing personal information to an overseas recipient with the individual’s consent after the individual is expressly informed**

8.27 An APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where:

- the APP entity expressly informs the individual that if they consent to the disclosure, this principle will not apply, and
- the individual then consents to the disclosure (APP 8.2(b)).

**Expressly inform**

8.28 An APP entity should provide the individual with a clear written or oral statement explaining the potential consequences of providing consent. At a minimum, this statement should explain that if the individual consents to the disclosure and the overseas recipient handles the personal information in breach of the APPs:

- the entity will not be accountable under the Privacy Act
- the individual will not be able to seek redress under the Privacy Act.

8.29 The statement should also:

- be made at the time consent is sought
- not rely on assumed prior knowledge of the individual.

15 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.
8.30 The statement could also explain any other practical effects or risks associated with the disclosure that the APP entity is aware of, or would be reasonably expected to be aware of. These may include that:

- the overseas recipient may not be subject to any privacy obligations or to any principles similar to the APPs
- the individual may not be able to seek redress in the overseas jurisdiction
- the overseas recipient is subject to a foreign law that could compel the disclosure of personal information to a third party, such as an overseas authority.

**Consent**

8.31 Consent is defined in s 6(1) as ‘express consent or implied consent’, and is discussed in more detail in Chapter B (Key concepts). The four key elements of consent are:

- the individual is adequately informed before giving consent (in this case ‘expressly informed’)
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent.

8.32 An APP entity does not need to obtain consent before every proposed cross-border disclosure. It may obtain an individual’s consent to disclose a particular kind of personal information to the same overseas recipient for the same purpose on multiple occasions, providing it has expressly informed the individual of the potential consequences of providing that consent. In doing this, the entity should not seek a broader consent than is necessary for its purposes, for example, consent for undefined future uses, or consent to all legitimate uses or disclosures.

8.33 If an individual withdraws their consent, the APP entity must no longer rely on the original consent when dealing with the individual’s personal information.

**Disclosing personal information to an overseas recipient as required or authorised by law**

8.34 An APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where the disclosure is ‘required or authorised by or under an Australian law or a court/tribunal order’ (APP 8.2(c)). An APP entity cannot rely on a requirement or authorisation in an overseas jurisdiction (see paragraphs 8.60–8.64 below). The meaning of ‘required or authorised by or under an Australian law or a court/tribunal order’ is discussed in Chapter B (Key concepts).

8.35 The following are examples of where a law or order may require or authorise disclosure of personal information to an overseas recipient:

---

16 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 84.
• an APP entity disclosing personal information to the government of a foreign country under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)
• an agency disclosing personal information to an overseas recipient under the Australian Federal Police Act 1979 (Cth) or the Mutual Assistance in Criminal Matters Act 1987 (Cth)

8.36 An agency that intends to rely on this exception could consider establishing administrative arrangements, memorandums of understanding or protocols with the overseas recipient that set out mutually agreed standards for the handling of personal information that provide privacy protections comparable to the APPs (see discussion of contractual measures in paragraphs 8.16–8.18 above).

Disclosing personal information to an overseas recipient where a permitted general situation exists

8.37 The cross-border principle will not apply if a permitted general situation exists for that disclosure (APP 8.2(d)). Section 16A lists five permitted general situations that may exist for a cross border disclosure. These situations are set out below, and are discussed in more detail in Chapter C (Permitted general situations) (including the meaning of relevant terms).

Lessening or preventing a serious threat to life, health or safety

8.38 An APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where:
• it is unreasonable or impracticable to obtain the individual’s consent to the disclosure, and
• the entity reasonably believes the disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety (s 16A(1), Item 1).

8.39 For example, this permitted general situation might apply where an APP entity discloses the personal information of an individual to a foreign authority, based on a reasonable belief that this disclosure will lessen a serious threat to the health or safety of that individual’s children, but seeking the individual’s consent may increase the threat.

Taking appropriate action in relation to suspected unlawful activity or serious misconduct

8.40 An APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where the entity:
• has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity’s functions or activities has been, is being or may be engaged in, and
• reasonably believes that the cross-border disclosure is necessary for the entity to take appropriate action in relation to the matter (s 16A(1), Item 2).
8.41 For example, this permitted general situation may apply where an APP entity that is a global organisation has reason to suspect that an individual is engaging in transnational fraud affecting the entity’s activities, and the entity reasonably believes that disclosing personal information to an overseas authority is necessary to take appropriate action.

**Locating a person reported as missing**

8.42 An APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where:

- the entity reasonably believes that the disclosure is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing, and
- the disclosure complies with rules made by the Information Commissioner under s 16A(2) (s 16A(1), Item 3).

**Necessary for a diplomatic or consular function or activity**

8.43 An agency may disclose personal information to an overseas recipient without complying with APP 8.1 where the agency reasonably believes that the disclosure is necessary for the agency’s diplomatic or consular functions or activities (s 16A(1), Item 6). The permitted general situation applies only to agencies, and not to organisations.

8.44 For example, this permitted general situation may apply where an agency discloses personal information to an overseas recipient to assist an Australian citizen who is in distress overseas, such as where an Australian individual is detained or is the victim of crime, where assistance is required with repatriation in the case of death or serious illness, or to provide assistance in response to a crisis or emergency overseas.

**Necessary for certain Defence Force activities outside Australia**

8.45 The Defence Force (as defined in s 6(1)) may disclose personal information to an overseas recipient without complying with APP 8.1 where it reasonably believes that the disclosure is necessary for a warlike operation, peacekeeping, civil aid, humanitarian assistance, a medical emergency, a civil emergency or disaster relief occurring outside Australia and the external Territories (s 16A(1), Item 7).

8.46 For example, this permitted general situation might apply where, in the immediate aftermath of a natural or man-made disaster outside Australia, the Defence Force discloses an individual’s personal information to an overseas recipient in order to assist in the provision of proper medical care to that individual.

**Disclosing personal information to an overseas recipient as required or authorised under an international agreement relating to information sharing**

8.47 An agency may disclose personal information to an overseas recipient without complying with APP 8.1 where the disclosure is ‘required or authorised by or under an international agreement relating to information sharing to which Australia is a party’ (APP 8.2(e)). This exception does not apply to organisations.
8.48 The term ‘international agreement’ is not defined in the Privacy Act. This guideline clarifies that the term includes documents binding at international law (for example, treaties and conventions), as well as other formal written documents not binding at international law (for example, a memorandum of understanding or an official exchange of letters17) that provide for information sharing between an agency and an overseas recipient. This exception applies only to such documents where the parties are Australia and one or more foreign states, although the overseas recipient of shared information may be a non-state entity.

8.49 Information sharing may not be the only or the primary subject of the agreement, so long as the agreement makes provision for ‘information sharing’. Additionally, the disclosure of personal information to the overseas recipient must be ‘required or authorised’ by or under the agreement.

8.50 To meet those requirements, the agreement should make specific arrangements for disclosure of information to an overseas recipient, including identifying the agency and the overseas recipient, the categories of personal information that may be disclosed to the recipient under the agreement and the circumstances in which or the purposes for which the information will be disclosed. This exception is unlikely to apply to an agreement that contains only a general commitment by the parties to facilitate, or remove obstacles to, the disclosure or exchange of information (the terms ‘required’ and ‘authorised’ are discussed in more detail in Chapter B (Key concepts)).

8.51 The agreement could also include provisions dealing with the responsibility of the parties to ensure adequate protection of the personal information that is disclosed according to standards comparable to those in the APPs, and the procedure to be followed to ensure that obligations or undertakings imposed by the agreement are met. The discussion of contractual measures in paragraphs 8.16–8.18 above lists other matters that could be considered for inclusion the agreement.

Disclosing personal information to an overseas recipient for an enforcement related activity

8.52 An agency may disclose personal information to an overseas recipient without complying with APP 8.1 where both of the following apply:

- the agency reasonably believes that the disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body, and
- the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body (APP 8.2(f)).

8.53 This exception is intended to enable an agency that is an enforcement body to cooperate with international counterparts for enforcement related activities.

8.54 ‘Enforcement body’ is defined in s 6(1) as a list of specific bodies and is discussed in Chapter B (Key concepts). The list includes Commonwealth, State and Territory bodies that are responsible for policing, criminal investigations, and administering laws to

---

17 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 84
protect the public revenue or to impose penalties or sanctions. Examples of Commonwealth enforcement bodies are the Australian Federal Police, Australian Crime Commission, Customs, the Integrity Commissioner,\(^{18}\) the Immigration Department,\(^{19}\) Australian Prudential Regulation Authority, Australian Securities and Investments Commission and AUSTRAC.

8.55 ‘Enforcement related activities’ is defined in s 6(1) and discussed in Chapter B (Key concepts). For further discussion of a similar exception in APP 6.2(e), see Chapter 6 (APP 6).

**When is an APP entity accountable for personal information that it discloses to an overseas recipient?**

8.56 An APP entity that discloses personal information to an overseas recipient is accountable, in certain circumstances, for an act or practice of the overseas recipient in relation to the information that would breach the APPs (s 16C(1)). Accountable means that the act or practice is taken to have been done by the APP entity and to be a breach of the APPs by that entity (s 16C(2)).

8.57 This accountability provision applies where:

- APP 8.1 applies to the disclosure. That is, none of the exceptions in APP 8.2 apply to the disclosure
- the APPs do not apply to the overseas recipient in relation to the personal information (for more information about when the APPs will apply see Chapter A (Introductory matters)), and
- an act or practice by the overseas recipient would breach the APPs (other than APP 1) if they had applied (s 16C(1)).

8.58 Under the accountability provision, an APP entity may be liable for the acts or practices of the overseas recipient (and the individual will have a means of redress) even where:

- the entity has taken reasonable steps to ensure the overseas recipient complies with the APPs (see APP 8.1) and the overseas recipient subsequently does an act or practice that would breach the APPs
- the overseas recipient discloses the individual’s personal information to a subcontractor and the subcontractor breaches the APPs\(^ {20}\)
- the overseas recipient inadvertently breaches the APPs in relation to the information.

8.59 However, an APP entity will not be accountable where, for example, it discloses personal information to an overseas recipient under an exception in APP 8.2 (see

---

\(^{18}\) ‘Integrity Commissioner’ is defined in s 6(1) as having the same meaning as in the *Law Enforcement Integrity Commissioner Act 2006*.

\(^{19}\) ‘Immigration Department’ is defined in s 6(1) as the Department administered by the Minister administering the *Migration Act 1958*.

\(^{20}\) Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 84.
paragraphs 8.19–8.55 above), or where personal information is disclosed to an overseas recipient with an ‘Australian link’. A recipient that has an ‘Australian link’ will be covered by the Privacy Act. ‘Australian link’ is defined in s 5B(2) and discussed in more detail in Chapter B (Key concepts).

**Overseas acts or practices required by a foreign law**

8.60 Section 6A(4) provides that an act or practice required by an applicable law of a foreign country will not breach the APPs if it is done, or engaged in, outside Australia and the external Territories. The meaning of ‘required’ by a law is discussed in Chapter B (Key concepts).

8.61 The effect of this provision is that where an overseas recipient of personal information does an act or practice that is required by an applicable foreign law, this will not breach the APPs. The APP entity will also not be responsible for the act or practice under the accountability provision.

8.62 For example, the USA PATRIOT Act may require the overseas recipient to disclose personal information to the Government of the United States of America. In these circumstances, the APP entity would not be responsible under the accountability provision for the disclosure required by that Act.

8.63 An APP entity could consider notifying an individual, if applicable, that the overseas recipient may be required to disclose their personal information under a foreign law. The entity could also explain that the disclosure will not breach the APPs. This information could be included in the APP entity’s APP 5 notice, particularly if the entity usually discloses personal information to overseas recipients (see APP 5.2(l), Chapter 5), or in its APP Privacy Policy (see Chapter 1 (APP 1)).

8.64 This provision does not apply to acts or practices that are done or engaged in, within Australia. Where a foreign law requires an APP entity in Australia to disclose personal information to an overseas recipient the entity must comply with APPs 6 and 8.

---

21 See *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT ACT) of 2001* (USA).
Chapter 9: Australian Privacy Principle
9 — Adoption, use or disclosure of government related identifiers

Version 1.0, February 2014

Key points ................................................................. 2
What does APP 9 say? .................................................. 2
‘Government related identifier’ .................................... 3
‘Identifiers’ ................................................................. 3
‘Government related identifiers’ ............................... 3
When are agencies covered by APP 9? ....................... 4
Adopting government related identifiers ..................... 4
‘Adoption’ ................................................................. 4
Adopting a government related identifier as required or authorised by or under an Australian law or a court/tribunal order .................................................. 5
Adopting a government related identifier as prescribed by regulations ............................ 5
Using and disclosing government related identifiers .......... 5
Using or disclosing a government related identifier where reasonably necessary to verify the identity of the individual ................................................................. 6
Using or disclosing a government related identifier where reasonably necessary to fulfil obligations to an agency or a State or Territory authority .................................................. 6
Using or disclosing a government related identifier as required or authorised by or under an Australian law or a court/tribunal order .................................................. 7
Using or disclosing a government related identifier where a permitted general situation exists ........................................................................................................... 7
Using or disclosing a government related identifier to an enforcement body for enforcement related activities ................................................................. 8
Using or disclosing a government related identifier as prescribed by regulations .......... 8
Key points

- APP 9 restricts the adoption, use and disclosure of government related identifiers by organisations. APP 9 may also apply to some agencies in the circumstances set out in s 7A.
- An identifier is a number, letter or symbol, or a combination of any or all of those things, that is used to identify the individual or to verify the identity of the individual.
- A government related identifier is an identifier that has been assigned by an agency, a State or Territory authority, an agent of an agency or authority, or a contracted service provider for a Commonwealth or State contract.
- Where an identifier, including a government related identifier, is personal information, it must be handled in accordance with the APPs.
- An organisation must not adopt a government related identifier of an individual as its own identifier of the individual, unless an exception applies.
- An organisation must not use or disclose a government related identifier of an individual, unless an exception applies.

What does APP 9 say?

9.1 An organisation must not adopt, use or disclose a government related identifier unless an exception applies. APP 9 may apply to an agency in the circumstances set out in s 7A (see paragraphs 9.10–9.11 below).

9.2 The objective of APP 9 is to restrict general use of government related identifiers by organisations so that they do not become universal identifiers. That could jeopardise privacy by enabling personal information from different sources to be matched and linked in ways that an individual may not agree with or expect.

9.3 An individual cannot consent to the adoption, use or disclosure of their government related identifier.

9.4 APP 9 restricts how an organisation is permitted to handle government related identifiers, irrespective of whether a particular identifier is the personal information of an individual. An identifier will be personal information if the individual is identifiable or reasonably identifiable from the identifier, including from other information held by, or available to, the entity that holds the identifier. If it is personal information, the identifier must be handled by the entity in accordance with other APPs. ‘Personal information’ is discussed in more detail in Chapter B (Key concepts), including examples of when an individual may be ‘reasonably identifiable’.
‘Government related identifier’

‘Identifiers’

9.5 An ‘identifier’ of an individual is defined in s 6(1) as a number, letter or symbol, or a combination of any or all of those things, that is used to identify the individual or to verify the identity of the individual.

9.6 The following are explicitly excluded from the definition of identifier:

- an individual’s name
- an individual’s Australian Business Number (ABN)
- anything else prescribed by the regulations made under the Privacy Act.¹ This provides flexibility to exclude any specified type of identifier from the definition, and therefore the operation of APP 9, as required.

‘Government related identifiers’

9.7 A ‘government related identifier’ of an individual is defined in s 6(1) as an identifier that has been assigned by:

- an agency
- a State or Territory authority
- an agent of an agency, or a State or Territory authority, acting in its capacity as agent, or
- a contracted service provider for a Commonwealth contract, or a State contract, acting in its capacity as contracted service provider for that contract.

9.8 The following are given as examples of government related identifiers:

- Medicare numbers
- Centrelink Reference numbers
- driver licence numbers issued by State and Territory authorities
- Australian passport numbers.

9.9 Some government related identifiers are regulated by other laws that restrict the way that entities can collect, use or disclose the particular identifier and related personal information. Examples include tax file numbers and individual healthcare identifiers.²

¹ See Comlaw <www.comlaw.gov.au> for up-to-date versions of the regulations made under the Privacy Act.
² For more information about the legislative regimes, visit the OAIC’s Tax File Numbers page and healthcare identifiers page <www.oaic.gov.au>.
When are agencies covered by APP 9?

9.10 An agency must comply with the adoption, use and disclosure requirements of APP 9 when dealing with government related identifiers in the circumstances set out in s 7A.

9.11 These circumstances include where:

- the agency is listed in Part I of Schedule 2 to the Freedom of Information Act 1982 (the FOI Act) and is prescribed in regulations, or
- the act or practice relates to the commercial activity of an agency that is specified in Part II of Schedule 2 to the FOI Act.

Adopting government related identifiers

9.12 An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless an exception applies (APP 9.1).

‘Adoption’

9.13 The term ‘adopt’ is not defined in the Privacy Act and so it is appropriate to refer to its ordinary meaning. An organisation adopts a government related identifier if it collects a particular government related identifier of an individual and organises the personal information that it holds about that individual with reference to that identifier.

9.14 The following are examples of when an organisation will be considered to have adopted a government related identifier of an individual:

- a health service provider uses an individual’s Medicare number as the basis for the provider’s own identification system.
- an accountant uses an individual’s tax file number as the basis of the accountant’s own identification system.

9.15 Adoption is to be distinguished from merely collecting, using or disclosing a government related identifier. APP 9 does not specifically address the collection of government related identifiers. However, as noted in paragraph 9.4, if an organisation collects a government related identifier that is considered to be personal information, the organisation must comply with other APPs, including APP 3 (collection of solicited personal information) and APP 4 (dealing with unsolicited personal information). These APPs are discussed in Chapters 3 and 4 respectively.

9.16 APP 3 provides that an organisation must only collect personal information that is reasonably necessary for one or more of the organisation’s functions or activities. If an organisation collects an identifier that it cannot lawfully use or disclose under APP 9.2 (see paragraphs 9.22–9.46), then the collection is not reasonably necessary for one of the

---


organisation’s functions or activities. This means that the collection would not be permitted under APP 3.2.

**Adopting a government related identifier as required or authorised by or under an Australian law or a court/tribunal order**

9.17 An organisation may adopt a government related identifier of an individual as its own identifier of the individual if the adoption is required or authorised by or under an Australian law or a court/tribunal order (APP 9.1(a)). The meaning of ‘required or authorised by or under an Australian law or a court/tribunal order’ is discussed in Chapter B (Key concepts).

9.18 The Australian law or court/tribunal order should specify a particular government related identifier, the organisations or classes of organisations permitted to adopt it, and the particular circumstances in which they may do so.

9.19 For example, healthcare providers are authorised by law to adopt the individual healthcare identifiers of their patients as their own identifier. That is, they may organise the personal information of their patients by reference to the patients’ individual healthcare identifiers.

**Adopting a government related identifier as prescribed by regulations**

9.20 An organisation may adopt a government related identifier of an individual as its own identifier of the individual if:

- the identifier is prescribed by regulations
- the organisation, or a class of organisations that includes the organisation, is prescribed by regulations, and
- the adoption occurs in the circumstances prescribed by the regulations (APP 9.1(b)).

9.21 Regulations may be made under the Privacy Act to prescribe these matters.6

**Using and disclosing government related identifiers**

9.22 An organisation must not use or disclose a government related identifier of an individual, unless an exception applies (APP 9.2). The terms ‘use’ and ‘disclosure’ are discussed in Chapter B (Key concepts).

9.23 The circumstances in which an organisation may use or disclose government related identifiers under APP 9.2 are narrower in scope than the circumstances in which an organisation may use or disclose other personal information under APP 6. APP 6 does not apply to the disclosure of government related identifiers (APP 6.7(b)) (see Chapter 6 (APP 6)).

---


Using or disclosing a government related identifier where reasonably necessary to verify the identity of the individual

9.24 An organisation may use or disclose the government related identifier of an individual if the use or disclosure is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation’s activities or functions (APP 9.2(a)).

9.25 This exception allows an organisation to use a government related identifier both to establish the identity of an individual and to verify that an individual is who or what they claim to be, for example, to verify their name or age.

9.26 Government related identifiers are usually contained in high-integrity documents, and are therefore likely to be highly reliable for verifying an individual’s identity. An example is that driver licences and passports are used in some circumstances to verify the identity of individuals.

9.27 The use and disclosure of the government related identifier to verify the identity of the individual must be reasonably necessary for the purposes of the organisation’s functions or activities. Whether the use or disclosure is ‘reasonably necessary’ is an objective test. This is discussed in more detail in Chapter B (Key concepts). The functions and activities of the organisation are limited to those in which it may lawfully engage. See Chapter 3 (APP 3) for a discussion of identifying the functions and activities of an organisation.

9.28 There are a number of factors that an organisation should consider in deciding whether the use or disclosure is reasonably necessary to verify the identity of an individual. For example, it may not be reasonably necessary where:

- the organisation can carry out the function or activity without verifying the individual’s identity
- there are other practicable means of verifying the individual’s identity available to the organisation. For example, an organisation may be able to verify an individual’s identity by using or disclosing other types of personal information, rather than the government related identifier (noting that the use and disclosure of other personal information must comply with the relevant APPs).

Using or disclosing a government related identifier where reasonably necessary to fulfil obligations to an agency or a State or Territory authority

9.29 An organisation may use or disclose a government related identifier of an individual if the use or disclosure is reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority (APP 9.2(b)).

9.30 This exception is most likely to be relevant to a contracted service provider, and will allow them to use or disclose a government related identifier if this is reasonably necessary to perform a Commonwealth or State or Territory contract. Whether the use or disclosure is ‘reasonably necessary’ is an objective test. This is discussed in more detail in Chapter B (Key concepts).

7 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 84.
Using or disclosing a government related identifier as required or authorised by or under an Australian law or a court/tribunal order

9.31 An organisation may use or disclose a government related identifier of an individual if the use or disclosure is required or authorised by or under an Australian law or a court/tribunal order (APP 9.2(c)).

9.32 The meaning of ‘required or authorised by or under an Australian law or a court/tribunal order’ is discussed in Chapter B (Key concepts).

9.33 The Australian law or court/tribunal order should specify a particular government related identifier, the organisations or classes of organisations permitted to use or disclose it, and the particular circumstances in which they may do so.

9.34 For example, the Healthcare Identifiers Act 2010 permits the use or disclosure of healthcare identifiers for limited purposes by healthcare providers and other entities specified in that Act.

Using or disclosing a government related identifier where a permitted general situation exists

9.35 An organisation may use or disclose a government related identifier of an individual if a ‘permitted general situation’ (other than the situations referred to in Items 3, 4 or 5 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the identifier (APP 9.2(d)).

9.36 Section 16A lists two permitted general situations that apply to the use or disclosure of government related identifiers. The two situations are set out below, and are discussed in Chapter C (Permitted general situations) (including the meaning of relevant terms).

Lessening or preventing a serious threat to life, health or safety

9.37 An organisation may use or disclose a government related identifier of an individual if:

- the organisation reasonably believes the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety, and
- it is unreasonable or impracticable to obtain consent (s 16A(1), Item 1).

Taking appropriate action in relation to suspected unlawful activity or serious misconduct

9.38 An organisation may use or disclose a government related identifier of an individual if:

- the organisation has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the organisation’s functions or activities has been, is being or may be engaged in, and
• the organisation reasonably believes that the use or disclosure is necessary in order for the organisation to take appropriate action in relation to the matter (s 16A(1), Item 2).

9.39 For example, this permitted general situation might apply where the organisation uses or discloses a government related identifier, such as a customer’s Centrelink number, as part of an investigation into suspected fraud by a client in relation to the organisation’s functions or activities.

Using or disclosing a government related identifier to an enforcement body for enforcement related activities

9.40 An organisation may use or disclose a government related identifier of an individual if the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body (APP 9.2(e)).

9.41 An organisation that collects or holds a government related identifier will be able to rely on this exception to cooperate with relevant enforcement bodies in certain circumstances.

9.42 ‘Enforcement body’ is defined in s 6(1) as a list of specific bodies. The list includes Commonwealth, State and Territory bodies that are responsible for policing, criminal investigations, and administering laws to protect the public revenue or to impose penalties or sanctions. Examples of Commonwealth enforcement bodies are the Australian Federal Police, Australian Crime Commission, Customs, the Integrity Commissioner,8 the Immigration Department,9 Australian Prudential Regulation Authority, Australian Securities and Investments Commission and AUSTRAC.

9.43 ‘Enforcement related activities’ is defined in s 6(1) and discussed in Chapter B (Key concepts). ‘Reasonably believes’, ‘reasonably necessary’ and ‘enforcement body’ are also discussed in Chapter B (Key concepts). For further discussion of a similar exception in APP 6.2(e), see Chapter 6.

9.44 For example, this exception might apply where the Australian Federal Police are investigating fraud committed by an individual against the organisation. The organisation may reasonably believe that disclosure of a copy of a driver licence to the AFP is reasonably necessary for the AFP’s investigation, where the AFP needed to obtain information provided by that individual to the organisation.

Using or disclosing a government related identifier as prescribed by regulations

9.45 An organisation may use or disclose a government related identifier of an individual if:

• the identifier is prescribed by regulations

---

8 ‘Integrity Commissioner’ is defined in s 6(1) as having the same meaning as in the Law Enforcement Integrity Commissioner Act 2006.

9 ‘Immigration Department’ is defined in s 6(1) as the Department administered by the Minister administering the Migration Act 1958.
• the organisation, or a class of organisations that includes the organisation, is prescribed by regulations, and
• the adoption occurs in the circumstances prescribed by the regulations (APP 9.2(f)).

9.46 Regulations may be made under the Privacy Act to prescribe these matters.\(^{10}\)

\(^{10}\) See Comlaw <www.comlaw.gov.au> for up to date versions of regulations made under the Privacy Act.
Chapter 10: Australian Privacy Principle
10 — Quality of personal information

Version 1.0, February 2014

Key points .............................................................................................................................. 2
What does APP 10 say? ......................................................................................................... 2
When an APP entity must take reasonable steps to ensure the quality of personal information ........................................................................................................................... 2
Taking reasonable steps ........................................................................................................ 2
Examples of reasonable steps ............................................................................................ 3
What are the quality considerations? .................................................................................. 4
Accurate ............................................................................................................................. 4
Up-to-date .......................................................................................................................... 5
Complete ............................................................................................................................ 5
Relevant ............................................................................................................................. 6
Interaction with other APPs .................................................................................................. 6
APP 3 (collection of solicited personal information) ......................................................... 6
APP 11 (security of personal information) ......................................................................... 6
APP 12 (access to personal information) and APP 13 (correction of personal information) ........................................................................................................................................ 6
Key points

- An APP entity must take reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete.
- An APP entity must take reasonable steps to ensure that the personal information it uses and discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

What does APP 10 say?

10.1 An APP entity must take reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete (APP 10.1).

10.2 An APP entity must also take reasonable steps to ensure that the personal information it uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant (APP 10.2). It is implicit that this requirement only applies to personal information ‘held’ by an entity (see Chapter 6 (APP 6)). ‘Holds’ is discussed in Chapter B (Key concepts).

10.3 Handling poor quality personal information can have significant privacy impacts for individuals. The requirements in APP 10 ensure that an APP entity takes reasonable steps to only handle high quality personal information, which builds community trust and confidence in an entity’s information handling practices.

When an APP entity must take reasonable steps to ensure the quality of personal information

10.4 An APP entity must take reasonable steps to ensure the quality of personal information at two distinct points in the information handling cycle. The first is at the time the information is collected. The second is at the time the information is used or disclosed.

10.5 Regular reviews, at other times, of the quality of personal information held by the APP entity may also assist in ensuring it is accurate, up-to-date, complete and relevant at the time it is used or disclosed.

Taking reasonable steps

10.6 The reasonable steps that an APP entity should take will depend upon circumstances that include:

- the sensitivity of the personal information. More rigorous steps may be required if the information collected, used or disclosed is ‘sensitive information’ (defined in s 6(1) and discussed in Chapter B (Key concepts)) or other personal information of a sensitive nature
- the nature of the APP entity holding the personal information. Relevant considerations include an entity’s size, resources and its business model. For
example, the reasonable steps expected of an entity that operates through franchises or dealerships, or gives database and network access to contractors, may differ from the reasonable steps required of a centralised entity

- the possible adverse consequences for an individual if the quality of personal information is not ensured. More rigorous steps may be required as the risk of adversity increases
- the practicability, including time and cost involved. However an entity is not excused from taking particular steps by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances.

10.7 In some circumstances it will be reasonable for an APP entity to take no steps to ensure the quality of personal information. For example, where an entity collects personal information from a source known to be reliable (such as the individual concerned) it may be reasonable to take no steps to ensure the quality of personal information. It is the responsibility of the entity to be able to justify that this is reasonable.

**Examples of reasonable steps**

10.8 The following are given as examples of reasonable steps that an APP entity could consider:

- implementing internal practices, procedures and systems to audit, monitor, identify and correct poor quality personal information (including training staff in these practices, procedures and systems). For example, if the entity commonly uses or discloses personal information in time-critical situations such that it may not be possible to take steps to ensure quality at the time of the use or disclosure, the entity might take steps to ensure the quality of personal information at regular intervals
- implementing protocols that ensure personal information is collected and recorded in a consistent format. For example, to help assess whether personal information is up-to-date, an entity might, where practicable, note on a record when the personal information was collected and the point in time to which it relates, and if it is an opinion, that fact
- ensuring updated or new personal information is promptly added to relevant existing records
- providing individuals with a simple means to review and update their personal information on an on-going basis, for example through an online portal
- reminding individuals to update their personal information each time the entity engages with the individual
- contacting the individual to verify the quality of personal information when it is used or disclosed, particularly if there has been a lengthy period since collection
• checking that a third party, from whom personal information is collected, has implemented appropriate practices, procedures and systems to ensure the quality of personal information. Depending on the circumstances, this could include:
  o making an enforceable contractual arrangement to ensure that the third party implements appropriate measures to ensure the quality of personal information the entity collects from the third party
  o undertaking due diligence in relation to the third party’s quality practices prior to the collection
• if personal information is to be used or disclosed for a new purpose that is not the primary purpose of collection, assessing the quality of the personal information having regard to that new purpose before the use or disclosure.

What are the quality considerations?

10.9 The three terms listed in APPs 10.1 and 10.2, ‘accurate’, ‘up-to-date’, ‘complete’, and the additional term in APP 10.2, ‘relevant’, are not defined in the Privacy Act. These terms are also listed in APP 13.1, which deals with the correction of personal information held by an APP entity.  

10.10 The following analysis of each term draws on the ordinary dictionary meaning of the terms, as well as case law concerning the meaning of those terms in the Privacy Act, Freedom of Information Act 1982 (FOI Act) and other legislation. As the analysis indicates, there is overlap in the meaning of the terms.

10.11 In applying the terms to the use and disclosure of personal information, it is necessary to have regard to ‘the purpose of the use or disclosure’ (APP 10.2). This is also a necessary consideration when applying these terms to the collection of personal information (see paragraph 10.21 below). That is, personal information may be of poor quality having regard to one purpose for which it is collected, used or disclosed, but not another. ‘Purpose’ is discussed in Chapter B (Key concepts).

Accurate

10.12 Personal information is inaccurate if it contains an error or defect. Personal information is also inaccurate if it is misleading. An example is incorrect factual information about a person’s name, date of birth, residential address or current or former employment.

---

1 Similar terms are used also in Part V of the Freedom of Information Act 1982 concerning a person’s right to apply to an agency to amend or annotate personal information.


10.13 An opinion about an individual given by a third party is not inaccurate by reason only that the individual disagrees with that opinion or advice. For APP 10 purposes, the opinion may be ‘accurate’ if it is presented as an opinion and not objective fact, it accurately records the view held by the third party, and is an informed assessment that takes into account competing facts and views. Other matters to consider under APP 10 are whether the opinion is ‘up-to-date’, ‘complete’, ‘not misleading’ or ‘relevant’.

10.14 In relation to a similar issue, s 55M of the FOI Act provides that the Information Commissioner (in conducting an Information Commissioner review) cannot alter a record of opinion unless satisfied that it was based on a mistake of fact, or the author of the opinion was biased, unqualified to form the opinion or acted improperly in conducting the factual inquiries that led to the formation of the opinion.

**Up-to-date**

10.15 Personal information is out-of-date if it contains facts, opinions or other information that is no longer current. An example is a statement that an individual lacks a particular qualification or accreditation that the individual has subsequently obtained.

10.16 Personal information about a past event may have been accurate at the time it was recorded, but has been overtaken by a later development. Whether that personal information is out-of-date will depend on the purpose for which it is collected, used or disclosed. If current personal information is required for the particular purpose, the personal information will, to that extent, be out-of-date. Personal information held by an APP entity that is no longer needed for any purpose, may need to be destroyed or de-identified under APP 11.2 (Chapter 11 (APP 11)).

**Complete**

10.17 Personal information is incomplete if it presents a partial or misleading picture, rather than a true or full picture. An example is a tenancy database which records that a tenant owes a debt, which in fact has since been repaid. The personal information will be incomplete under APP 10 if the tenancy database is used or disclosed for the purpose of providing members with personal information about defaults on tenant agreements. Similarly, a statement that a person has only two rather than three children will be incomplete under APP 10 if that personal information is used for the purpose of, and is relevant to, assessing a person’s eligibility for a benefit or service.

10.18 Where an APP entity is required to collect additional personal information to ensure that the information is complete, having regard to the purpose for which the information is collected, used or disclosed, the collection of that information will be reasonably necessary for the entity’s functions or activities (see Chapter 3 (APP 3)).

---

4 The definition of ‘personal information’ includes ‘information or an opinion’ (s 6(1)).

5 For further discussion of reasonable steps in these circumstances, see *Tenants’ Union of Queensland Inc, Tenants’ Union of NSW Co-op Ltd and complainants C, D, E, F and G v TICA Default Tenancy Control Pty Ltd* [2004] PrivCmrACD 2 (16 April 2004).
Relevant

10.19 Personal information is irrelevant if it does not have a bearing upon or connection to the purpose for which the personal information is used or disclosed. An example is an APP entity that holds personal information about a client collected for the purpose of providing financial advice. If the entity later discloses personal information to purchase shares on the client’s behalf, it should only disclose parts of the personal information relevant to that secondary purpose.

Interaction with other APPs

10.20 The requirements in APP 10 to take reasonable steps to ensure the quality of personal information are complemented by other requirements in APP 3 (collection of solicited personal information), APP 11 (security of personal information), APP 12 (access to personal information) and APP 13 (correction of personal information).

APP 3 (collection of solicited personal information)

10.21 APP 10.1 does not specifically require an APP entity to take reasonable steps to ensure that the personal information it collects is relevant to the purpose of collection. However, this requirement is implied in APP 3. Under APP 3, an APP entity must only collect personal information which is reasonably necessary for ‘one or more of the entity’s functions or activities’. Agencies may, in addition, collect personal information that is directly related to one or more of the agency’s functions or activities. For sensitive information, an entity will also need the individual’s consent, unless an exception applies (see Chapter 3 (APP 3)).

APP 11 (security of personal information)

10.22 Where an APP entity amends personal information or adds new personal information to a record to comply with APP 10, it should consider whether it needs to take action under APP 11 to destroy or de-identify other personal information that it holds (for example a copy of that information). APP 11 requires an APP entity to take reasonable steps to destroy or de-identify personal information that it no longer needs, unless it is contained in a Commonwealth record or the entity is required by or under an Australian law, or a court/tribunal order, to retain it (see Chapter 11 (APP 11)).

APP 12 (access to personal information) and APP 13 (correction of personal information)

10.23 APPs 12 and 13 can support an APP entity in meeting its obligation under APP 10 to ensure the quality of personal information that it collects, uses and discloses. Providing an individual with access to their personal information under APP 12 will allow the individual to identify whether any personal information is inaccurate, out-of-date, incomplete or irrelevant. Similarly, taking reasonable steps to correct incorrect personal information at the request of an individual under APP 13 can also enhance the quality of that information.
10.24  APP 13 also requires an APP entity to take reasonable steps to correct personal information where an APP entity is satisfied, independently of any request, that personal information it holds, is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to a purpose for which the information is held (see Chapter 13 (APP 13)).

10.25  In addition to responding to requests for access and correction under APPs 12 and 13, an APP entity should proactively provide individuals with a simple means to access and update their personal information on an on-going basis (see paragraph 10.8 above).
Chapter 11: Australian Privacy Principle
11 — Security of personal information

Version 1.1, March 2015

Key points.............................................................................................................................................. 2
What does APP 11 say? .......................................................................................................................... 2
‘Holds’ .................................................................................................................................................. 2
Taking reasonable steps......................................................................................................................... 3
What are the security considerations? ................................................................................................... 4
  Misuse ................................................................................................................................................ 4
  Interference .................................................................................................................................... 4
  Loss .................................................................................................................................................. 4
  Unauthorised access ........................................................................................................................... 5
  Unauthorised modification .................................................................................................................. 5
  Unauthorised disclosure ..................................................................................................................... 5
Destroying or de-identifying personal information .................................................................................. 5
  Personal information held by an agency ............................................................................................ 6
  Personal information held by an organisation .................................................................................. 6
  Required by or under an Australian law or a court/tribunal order ....................................................... 7
Taking reasonable steps to destroy or de-identify personal information .................................................. 7
  Destroying personal information — irretrievable destruction.............................................................. 8
  Destroying personal information held in electronic format – putting beyond use.............................. 8
  De-identifying personal information .................................................................................................. 9
Key points

- An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

- Where an APP entity no longer needs personal information for any purpose for which the information may be used or disclosed under the APPs, the entity must take reasonable steps to destroy the information or ensure that it is de-identified. This requirement applies except where:
  - the personal information is part of a Commonwealth record, or
  - the APP entity is required by law or a court/tribunal order to retain the personal information.

- Many of the issues discussed in this Chapter are discussed in more detail in the Office of the Australian Information Commissioner’s (OAIC) *Guide to securing personal information*.¹

What does APP 11 say?

11.1 APP 11 requires an APP entity to take active measures to ensure the security of personal information it holds, and to actively consider whether it is permitted to retain personal information.²

11.2 An APP entity that holds personal information must take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure (APP 11.1).

11.3 An APP entity must take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for any purpose for which the personal information may be used or disclosed under the APPs. This requirement does not apply where the personal information is contained in a Commonwealth record or where the entity is required by law or a court/tribunal order to retain the personal information (APP 11.2).

‘Holds’

11.4 APP 11 only applies to personal information that an APP entity holds. An entity holds personal information ‘if the entity has possession or control of a record that contains the personal information’ (s 6(1)).

11.5 The term ‘holds’ extends beyond physical possession of a record to include a record that an APP entity has the right or power to deal with. For example, an entity that outsources the storage of personal information to a third party, but retains the right to

---

² Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 86.
deal with that information, including to access and amend it, holds that personal information.

11.6 The term ‘holds’ is discussed in more detail in Chapter B (Key concepts).

**Taking reasonable steps**

11.7 The ‘reasonable steps’ that an APP entity should take to ensure the security of personal information will depend upon circumstances that include:

- the nature of the APP entity. Relevant considerations include an APP entity’s size, resources, the complexity of its operations and its business model. For example, the reasonable steps expected of an entity that operates through franchises or dealerships, or that outsources its personal information handling to a third party may be different to those it would take if it did not operate in this manner.

- the amount and sensitivity of the personal information held. Generally, as the amount and/or sensitivity of personal information that is held increases, so too will the steps that it is reasonable to take to protect it. ‘Sensitive information’ (defined in s 6(1)) is discussed in more detail in Chapter B (Key concepts)

- the possible adverse consequences for an individual in the case of a breach. More rigorous steps may be required as the risk of adversity increases

- the practical implications of implementing the security measure, including time and cost involved. However an entity is not excused from taking particular steps to protect information by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances

- whether a security measure is in itself privacy invasive. For example, while an APP entity should ensure that an individual is authorised to access information, it should not require an individual to supply more information than is necessary to identify themselves when dealing with the entity (see also Chapter 12 (APP 12)).

11.8 Reasonable steps should include, where relevant, taking steps and implementing strategies in relation to the following:

- governance, culture and training
- internal practices, procedures and systems
- ICT security
- access security
- third party providers (including cloud computing)
- data breaches
- physical security
- destruction and de-identification
- standards.
11.9 As part of taking reasonable steps to protect personal information (also known as ‘personal information security’) an APP entity should consider how it will protect personal information at all stages of the information lifecycle. This should be considered before an entity collects personal information (including whether it should collect the information at all), as well as when the information is collected and held, and when it is destroyed or de-identified when no longer needed.

11.10 For further discussion of personal information security and the information lifecycle and examples of steps that may be reasonable for an APP entity to take under APP 11.1, see the OAIC’s Guide to securing personal information.  

What are the security considerations?

11.11 The six terms listed in APP 11, ‘misuse’, ‘interference’, ‘loss’, ‘unauthorised access’, ‘unauthorised modification’ and ‘unauthorised disclosure’, are not defined in the Privacy Act. The following analysis and examples of each term draws on the ordinary meaning of the terms. As the analysis indicates, there is overlap in the meaning of the terms.

Misuse

11.12 Personal information is misused if it is used by an APP entity for a purpose that is not permitted by the Privacy Act. APP 6 sets out when an entity is permitted to use personal information (see Chapter 6). APPs 7 and 9 also contain requirements relating to an organisation’s use of personal information for the purpose of direct marketing, and use of government related identifiers, respectively (see Chapters 7 and 9).

11.13 ‘Use’ is discussed in more detail in Chapter B (Key concepts).

Interference

11.14 ‘Interference’ with personal information occurs where there is an attack on personal information that an APP entity holds that interferes with the personal information but does not necessarily modify its content. ‘Interference’ includes an attack on a computer system that, for example, leads to exposure of personal information.

Loss

11.15 ‘Loss’ of personal information covers the accidental or inadvertent loss of personal information held by an APP entity. This includes when an APP entity:

- physically loses personal information, (including hard copy documents, computer equipment or portable storage devices containing personal information), for example, by leaving it in a public place, or

---

• electronically loses personal information, such as failing to keep adequate backups of personal information in the event of a systems failure.

11.16 Loss may also occur as a result of theft following unauthorised access or modification of personal information or as a result of natural disasters such as floods, fires or power outages.

11.17 However, it does not apply to intentional destruction or de-identification of that personal information that is done in accordance with the APPs.

Unauthorised access

11.18 ‘Unauthorised access’ of personal information occurs when personal information that an APP entity holds is accessed by someone who is not permitted to do so. This includes unauthorised access by an employee of the entity or independent contractor, as well as unauthorised access by an external third party (such as by hacking).

Unauthorised modification

11.19 ‘Unauthorised modification’ of personal information occurs when personal information that an APP entity holds is altered by someone who is not permitted to do so, or is altered in a way that is not permitted under the Privacy Act. For example, unauthorised modification may occur as a result of unauthorised alteration by an employee, or following unauthorised access to databases by an external third party.

Unauthorised disclosure

11.20 ‘Unauthorised disclosure’ occurs when an APP entity:

• makes personal information accessible or visible to others outside the entity, and

• releases that information from its effective control in a way that is not permitted by the Privacy Act.

11.21 This includes an unauthorised disclosure by an employee of the APP entity. The term ‘disclosure’ is discussed in more detail in Chapter B (Key concepts).

Destroying or de-identifying personal information

11.22 An APP entity must take reasonable steps to destroy personal information or ensure it is de-identified if it no longer needs the information for any purpose for which it may be used or disclosed under the APPs (APP 11.2).

---

4 Under s 8(1) of the Privacy Act, an APP entity needs to take reasonable steps to ensure that an employee does not gain unauthorised access to personal information ‘in the performance of the duties of the person’s employment’.

5 See Chapter 6 (APP 6) for more information about disclosures that are permitted by the Privacy Act.

6 An APP entity needs to take reasonable steps to ensure that an employee does not carry out an unauthorised disclosure of personal information ‘in the performance of the duties of the person’s employment’ (s 8(1)).
11.23 This means that an APP entity will not need to destroy or de-identify personal information it holds if the information is still necessary for the primary purpose of collection or for a secondary purpose for which it may be used or disclosed under APP 6 (see Chapter 6). Where the entity is an organisation and the personal information is needed for the purpose of direct marketing, or is a government related identifier, whether it may be used or disclosed under APPs 7 and 9 may also be relevant (see Chapters 7 and 9 respectively). ‘Purpose’ is discussed in more detail in Chapter B (Key concepts).

11.24 The requirement to take reasonable steps to destroy or de-identify does not apply if personal information is contained in a Commonwealth record, or if an Australian law or a court/tribunal order requires it to be retained (APP 11.2). In practice, this means that different rules apply to agencies and organisations.

## Personal information held by an agency

11.25 The term ‘Commonwealth record’ in s 6(1) has the same meaning as in s 3 of the *Archives Act 1983* (the Archives Act) and is discussed in more detail in Chapter B (Key concepts). The definition is likely to include all or most personal information held by agencies. It may also include personal information held by contracted service providers.

11.26 If the personal information is contained in a Commonwealth record, the agency is not required to destroy or de-identify the personal information under APP 11.2, even if it no longer needs the personal information for any purpose for which it may be used or disclosed under the APPs. The agency will instead be required to comply with the provisions of the Archives Act in relation to those Commonwealth records.

11.27 A Commonwealth record can, as a general rule, only be destroyed or altered in accordance with s 24 of the Archives Act. The grounds on which this may be done include with the permission of the National Archives of Australia (as set out in a records disposal authority) or in accordance with a ‘normal administrative practice’. See Chapter B (Key concepts) for more information about Commonwealth records.

## Personal information held by an organisation

11.28 Where an organisation ‘holds’ personal information it no longer needs for a purpose that is permitted under the APPs, it must ensure that it takes reasonable steps to destroy or de-identify the personal information. This obligation applies even where the organisation does not physically possess the personal information, but has the right or power to deal with it. ‘Holds’ is discussed in more detail in paragraphs 11.4–11.6 above and Chapter B (Key concepts).

11.29 Where an organisation holds personal information that needs to be destroyed or de-identified, it must take reasonable steps to destroy or de-identify all copies it holds of

---

7 *Archives Act 1983* section 3: Commonwealth record means:

- a record that is the property of the Commonwealth or of a Commonwealth institution; or
- a record that is to be deemed to be a Commonwealth record by virtue of a regulation under subsection (6) or by virtue of section 22;

but does not include a record that is exempt material or is a register or guide maintained in accordance with Part VIII.
that personal information, including copies that have been archived or are held as back-ups.

11.30 An organisation should have practices, procedures and systems in place to identify personal information that needs to be destroyed or de-identified (see APP 1.2, Chapter 1).

**Required by or under an Australian law or a court/tribunal order**

11.31 If an organisation is required by or under an Australian law or a court/tribunal order to retain personal information, it is not required to take reasonable steps to destroy or de-identify it (APP 11.2(d)).

11.32 ‘Australian law’ and ‘court/tribunal order’ are defined in s 6(1). The term ‘required by or under an Australian law or court/tribunal order’ is discussed in Chapter B (Key concepts).

**Taking reasonable steps to destroy or de-identify personal information**

11.33 The ‘reasonable steps’ that an organisation should take to destroy or de-identify personal information will depend upon circumstances that include:

- the amount and sensitivity of the personal information — more rigorous steps may be required as the quantity of personal information increases, or if the information is ‘sensitive information’ (defined in s 6(1) and discussed in Chapter B (Key concepts)) or other personal information of a sensitive nature
- the nature of the organisation. Relevant considerations include an organisation’s size, resources and its business model. For example, the reasonable steps expected of an organisation that operates through franchises or dealerships, or gives database and network access to contractors, may differ from the reasonable steps required of a centralised organisation
- the possible adverse consequences for an individual if their personal information is not destroyed or de-identified — more rigorous steps may be required as the risk of adversity increases
- the organisation’s information handling practices, such as how it collects, uses and stores personal information, including whether personal information handling practices are outsourced to third parties
- the practicability, including time and cost involved — however an organisation is not excused from destroying or de-identifying personal information by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances.
11.34 For further discussion of the relevant considerations, and examples of steps that may be reasonable for an APP entity to take under APP 11.2, see the OAIC’s Guide to securing personal information.  

11.35 While APP 11.2 requires an organisation to take reasonable steps to either destroy or de-identify personal information, in some circumstances one or the other may be more appropriate (see paragraphs 11.38 and 11.44 below).

Destroying personal information — irretrievable destruction

11.36 Personal information is destroyed when it can no longer be retrieved. The steps that are reasonable for an organisation to take to destroy personal information will depend on whether the personal information is held in hard copy or electronic form.

11.37 For example, for personal information held:

- in hard copy, disposal through garbage or recycling collection would not ordinarily constitute taking reasonable steps to destroy the personal information, unless the personal information had already been destroyed through a process such as pulping, burning, pulverising, disintegrating or shredding
- in electronic form, reasonable steps will vary depending on the kind of hardware used to store the personal information. In some cases, it may be possible to ‘sanitise’ the hardware to completely remove stored personal information. For hardware that cannot be sanitised, reasonable steps must be taken to destroy the personal information in another way, such as by irretrievably destroying it. Where it is not possible to irretrievably destroy personal information held in electronic format, an organisation could instead comply with APP 11.2 by taking reasonable steps to de-identify the personal information (see paragraphs 11.41–11.45 below), or should put the information beyond use (see paragraphs 11.38–11.40 below)
- on a third party’s hardware, such as cloud storage, where the organisation has instructed the third party to irretrievably destroy the personal information, reasonable steps would include taking steps to verify that this has occurred.

Destroying personal information held in electronic format – putting beyond use

11.38 Where it is not possible for an organisation to irretrievably destroy personal information held in electronic format, reasonable steps to destroy it would include putting the personal information ‘beyond use’. However, an organisation could instead consider whether de-identifying the data would be appropriate (see paragraphs 11.41–11.45 below) and if so, take reasonable steps to de-identify the personal information.

11.39 Personal information is ‘beyond use’ if the organisation:

---

9 See the ‘Controls’ section of the Australian Government Information Security Manual (ISM) on the Australian Signals Directorate website <www.asd.gov.au>. The ISM also discusses how various forms of hardware should be sanitised or destroyed. Although the ISM only applies to Australian Government agencies, it may be of interest to organisations in complying with APP 11.2.
• is not able, and will not attempt, to use or disclose the personal information
• cannot give any other entity access to the personal information
• surrounds the personal information with appropriate technical, physical and organisational security. This should include, at a minimum, access controls including logs and audit trails, and
• commits to take reasonable steps to irretrievably destroy the personal information if, or when, this becomes possible.

It is expected that only in very limited circumstances would it not be possible for an organisation to destroy personal information held in electronic format. For example, where technical reasons may make it impossible to irretrievably destroy the personal information without also irretrievably destroying other information held with that personal information, which the entity is required to retain.

De-identifying personal information

11.41 Personal information is de-identified ‘if the information is no longer about an identifiable individual or an individual who is reasonably identifiable’ (s 6(1)). De-identification is discussed in more detail in Chapter B (Key concepts).

11.42 An organisation that intends to comply with APP 11.2 by taking reasonable steps to ensure that personal information is de-identified should consider whether de-identification is appropriate in the circumstances. For more information on when and how to de-identify information, and how to manage and mitigate the risk of re-identification, see Privacy Business Resource 4 — De-identification of Data and Information and Information Policy Agency Resource 1 — De-identification of Data and Information.10

11.43 De-identification of personal information may be more appropriate than destruction where the de-identified information could provide further value or utility to the organisation or a third party. For example, where:

• an organisation shares de-identified information with researchers, or
• an organisation uses de-identified information to develop new products.

11.44 Regardless of the de-identification technique chosen, the risk of re-identification must be actively assessed and managed to mitigate this risk. Where it is not possible for the risk of re-identification to be appropriately minimised, the organisation could instead consider taking reasonable steps to destroy the personal information (see paragraphs 11.36–11.42 above).

11.45 Where the personal information is held on a third party’s hardware, such as cloud storage, and the organisation has instructed the third party to de-identify the personal information, reasonable steps to de-identify the personal information would include taking steps to verify that this has occurred.

---

Chapter 12: Australian Privacy Principle 12 — Access to personal information

Version 1.0, February 2014

Key points ................................................................................................................................................. 3
What does APP 12 say? ............................................................................................................................ 3
‘Holds’ .................................................................................................................................................... 4
Access to ‘personal information’ ............................................................................................................ 4
Verifying an individual’s identity ............................................................................................................. 5
Giving access under APP 12 — general processing requirements ....................................................... 6
Giving access under APP 12 — further processing requirements for agencies ................................. 6
Refusing to give access under APP 12 — agencies ............................................................................ 7
Authority to refuse access under the FOI Act ....................................................................................... 8
Required or authorised to refuse access under another Act ............................................................... 9
Refusing to give access under APP 12 — organisations ................................................................. 9
Giving access would pose a serious threat to the life, health or safety of any individual .......................... 10
or to public health or public safety ....................................................................................................... 10
Giving access would have an unreasonable impact on the privacy of other individuals .................. 10
The request for access is frivolous or vexatious .................................................................................... 11
The information requested relates to an existing or anticipated legal proceeding ............................ 11
Giving access would prejudice negotiations between the organisation and the individual ................. 12
Giving access would be unlawful ......................................................................................................... 12
Denying access is required or authorised by law or a court/tribunal order ........................................ 12
Giving access would likely prejudice the taking of appropriate action in relation to suspected unlawful activity or serious misconduct ..................................................................................... 12
Giving access would be likely to prejudice an enforcement related activity conducted by, or on behalf of, an enforcement body ......................................................................................... 13
Giving access would reveal evaluative information in connection with a commercially sensitive decision-making process ............................................................................................................................. 14
APP 12 minimum access requirements ............................................................................................. 14
Difference with access requirements applying to agencies under FOI Act .................................... 14
Timeframe for responding to a request for access under APP 12 — agencies .................................... 15
Timeframe for responding to a request for access under APP 12 — organisations .......................... 15
How access is to be given under APP 12 ............................................................................................ 15
Giving access by other means ............................................................................................................. 16
Giving access through an intermediary ................................................................. 16
Access charges under APP 12 — agencies ............................................................... 17
Access charges under APP 12 — organisations ....................................................... 17
Giving written notice where access is refused, or not given in the manner requested
under APP 12 ............................................................................................................. 18
Key points

- APP 12 requires an APP entity that holds personal information about an individual to give the individual access to that information on request.

- APP 12 also sets out other requirements in relation to giving access, including how access is to be given and when access can be refused. There are separate grounds on which agencies and organisations may refuse to give access.

- APP 12 operates alongside and does not replace other informal or legal procedures by which an individual can be provided with access to information, including, for agencies, the Freedom of Information Act 1982 (FOI Act) that provides a right of access to information held by agencies.

What does APP 12 say?

12.1 An APP entity that holds personal information about an individual must, on request, give that individual access to the information (APP 12.1). The grounds on which access may be refused differ for agencies and organisations.

12.2 APP 12 also sets out minimum access requirements, including the time period for responding to an access request, how access is to be given, and that a written notice, including the reasons for the refusal, must be given to the individual if access is refused.

12.3 APP 12 operates alongside and does not replace other informal or legal procedures by which an individual can be given access to information. In particular, APP 12 does not prevent an APP entity from giving access to personal information under an informal administrative arrangement, provided the minimum access requirements stipulated in APP 12 have been met.

12.4 For agencies, APP 12 operates alongside the right of access in the FOI Act. The FOI Act provides individuals with a right of access to documents held by most Australian Government agencies, including documents containing personal information.

12.5 Some paragraphs in this Chapter are only relevant to agencies or to organisations:

- paragraphs only for agencies: 12.22–12.24; 12.25–12.32; 12.66; 12.76

---

1 For information about administrative access schemes, see OAIC, FOI Agency Resource 14: Administrative access schemes, OAIC website <www.oaic.gov.au>.

2 The FOI Act is expressed to apply separately to Ministers’ offices in respect of ‘an official document of a Minister’ (s 48). APP 12 also applies to Ministers’ offices: see the discussion of ‘APP entity’ in Chapter B (Key concepts), and the Privacy Act s 7(1)(d),(e).

3 The Australian Information Commissioner has issued Guidelines (the FOI Guidelines) under s 93A of the FOI Act to which regard must be had for the purposes of performing a function, or exercising a power, under that Act. The FOI Guidelines are available at OAIC website <www.oaic.gov.au>.
‘Holds’

12.6 APP 12 only applies to personal information that an APP entity ‘holds’. An APP entity ‘holds’ personal information ‘if the entity has possession or control of a record that contains the personal information’ (s 6(1)).

12.7 The term ‘holds’ extends beyond physical possession of a record to include a record that an APP entity has the right or power to deal with. For example, an entity that outsources the storage of personal information to a third party, but retains the right to deal with that information, including to access and amend it, holds that personal information. In these circumstances, the entity must comply with APP 12 by giving the individual access (unless an exception applies). It cannot simply refer the individual to the third party that has physical possession. However, the individual has a separate right to request access from the third party, if the third party is an APP entity.

12.8 An agency that has placed a record of personal information in the care of the National Archives of Australia, or in the custody of the Australian War Memorial, is considered to be the agency that holds the record for the purposes of the Privacy Act (s 10(4)).

12.9 Upon receiving a request for access, an APP entity should search the records that it possesses or controls to assess whether the requested personal information is contained in those records. For example, an entity may search hard copy records and electronic databases and make enquiries of staff or contractors with relevant knowledge. A discussion with the individual may assist the entity to locate the information.

12.10 The term ‘holds’ is discussed in more detail in Chapter B (Key concepts).

Access to ‘personal information’

12.11 APP 12 requires an APP entity to provide access to ‘personal information’. It does not provide a right of access to other kinds of information. ‘Personal information’ is defined in s 6(1) as ‘information or an opinion about an identified individual, or an individual who is reasonably identifiable:

• whether the information or opinion is true or not, and
• whether the information or opinion is recorded in a material form or not’.

12.12 Personal information of one individual may also be personal information of another individual. For example:

• information in a marriage certificate may be personal information of both parties to the marriage
• an opinion may be personal information of both the subject and the giver of the opinion.

12.13 APP 12 requires an APP entity to provide access to all of an individual’s personal information it holds, even if that information is also the personal information of another individual, unless a ground to refuse access applies. The grounds are discussed below, and include the ground that giving access would have an unreasonable impact on the
privacy of another individual. ‘Personal information’ is discussed in more detail in Chapter B (Key concepts).

12.14 As to other requested information that is not personal information:

- If the APP entity is an organisation, it could consider whether the person has a right of access to that information under other legislation. If not, the organisation may make a discretionary decision either to grant access to that other information or to refuse access.

- If the entity is an agency, it could consider whether access to that information can be granted under the FOI Act, or on an administrative basis. Before refusing access to that other information, the agency should advise the individual to consider making the request under the FOI Act.

**Verifying an individual’s identity**

12.15 An APP entity must be satisfied that a request for personal information under APP 12 is made by the individual concerned, or by another person who is authorised to make a request on their behalf, for example, as a legal guardian or authorised agent. If an entity gives access to the personal information of another person, this could constitute a disclosure, which may not comply with APP 6 (see Chapter 6).

12.16 It would generally be impracticable for an APP entity to deal with an anonymous request for personal information. However, it may be practicable to deal with a pseudonymous request, for example, where the individual has previously transacted under that pseudonym, can establish their identity as that individual and the request for access relates to information about that pseudonymous identity (see Chapter 2 (APP 2)).

12.17 The steps appropriate to verify an individual’s identity will depend on the circumstances. In particular, whether the individual is already known to or readily identifiable by the APP entity, the sensitivity of the personal information and the possible adverse consequences for the individual of unauthorised disclosure. The minimum amount of personal information needed to establish an individual’s identity should be sought. Where possible, the personal information should be sighted rather than copied or collected for inclusion in a record. For example, in a face-to-face dealing with an individual, an entity may be able to record that an identity document was sighted without copying the document. In a telephone contact it may be adequate to request information that can be checked against records held by the entity. An entity that collects personal information to verify an individual’s identity should consider the requirement in APP 11.2, to take reasonable steps to destroy or de-identify personal information no longer needed for any purpose for which it may be used or disclosed (unless an exception applies) (see Chapter 11 (APP 11)).
Giving access under APP 12 — general processing requirements

12.18 APP 12 requires that personal information be given to an individual ‘on request’. APP 12 does not stipulate formal requirements for making a request, or require that a request be made in writing, or require the individual to state that it is an APP 12 request.4

12.19 It is open to an APP entity to provide access to personal information on an informal basis, provided the minimum access requirements in APP 12 are met. The access requirements in APP 12 relate to response times (see paragraphs 12.66–12.67 below), how access is to be given (see paragraphs 12.68–12.75 below), access charges (see paragraphs 12.76–12.81 below), and providing a written notice, including the reasons for the refusal, if access is refused (see paragraphs 12.82–12.87 below). These are only the minimum requirements. An entity should endeavour to provide access in a manner that is as prompt, uncomplicated and inexpensive as possible.

12.20 An APP entity is required by APP 1.4(d) to state in an APP Privacy Policy ‘how an individual may access personal information about the individual’ (see Chapter 1 (APP 1)). An APP entity is also required by APP 5.2(g) to take reasonable steps to notify an individual, or ensure they are aware, of the fact that the entity’s APP Privacy Policy contains information about how the individual may access their personal information held by the entity.

12.21 If an APP entity wishes an individual to follow a particular procedure in requesting access to their personal information, the entity could publish that procedure and draw attention to it, for example, by providing a link in the entity’s APP Privacy Policy and on the entity’s website homepage to the access procedure, to an online request form, or to an online portal that enables an individual to access their personal information. However, an entity cannot require an individual to follow a particular procedure, use a designated form or explain the reason for making the request. Any recommended procedure should be regularly reviewed to ensure that it is flexible and facilitates rather than hinders access.

Giving access under APP 12 — further processing requirements for agencies

12.22 Agencies should ensure that APP 12 access procedures are integrated with FOI Act procedures. The FOI Act sets out comprehensive rules about requesting and providing access to documents held by most Australian Government agencies, including documents containing personal information, and resolving access disputes. An important FOI requirement is that an agency has a duty to take reasonable steps to assist an individual to make an access request that complies with the FOI Act access requirements (FOI Act, s 15(3)). That means an agency could refer to the FOI Act in the agency’s APP Privacy Policy and, in appropriate circumstances, draw the FOI Act to an individual’s attention. Agencies should also consider providing this information through an ‘Access to information’ link on the agency’s website homepage.5

---

4 This differs from the formal requirements relating to requests for access to documents under Part III of the FOI Act. See Part III of the FOI Act and Part 3 of the FOI Guidelines, OAIC website <www.oaic.gov.au>.

12.23 Agencies are not required to advise individuals to request personal information under the FOI Act rather than under an administrative arrangement or by relying on APP 12. As explained in the FOI Guidelines, agencies should consider establishing administrative access arrangements that operate alongside the FOI Act and that provide easier and less formal means for individuals to obtain access to government information, including personal information. Providing access to personal information under an administrative arrangement will fulfil an agency’s obligation under APP 12 to provide access upon request, provided the arrangement meets the minimum access requirements in APP 12.

12.24 In some circumstances it may be preferable for an agency to suggest that an individual make an access request under the FOI Act:

- an FOI access request can relate to any document in the possession of an agency (FOI Act, s 15(1)) and is not limited to personal information held in an agency record (APP 12.1)
- the FOI Act contains a consultation process for dealing with requests for documents that contain personal or business information about a person other than the requester (FOI Act, ss 27, 27A)
- an applicant who applies for access under the FOI Act can complain to the Information Commissioner about an action taken by an agency under that Act (FOI Act, s 70) (complaint mechanisms under the Privacy Act are discussed in paragraph 12.30 and 12.87 below)
- an applicant who is refused access under the FOI Act has a right to apply for internal review or Information Commissioner review of the access refusal decision (FOI Act, ss 54, 54L).

### Refusing to give access under APP 12 — agencies

12.25 An agency is not required by APP 12 to give access to personal information if the agency is required or authorised to refuse access to that information by or under:

- the FOI Act (APP 12.2(b)(i))
- any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents (APP 12.2(b)(ii)).

12.26 The meaning of ‘required or authorised’ is discussed in Chapter B (Key concepts). In summary, an agency is ‘required’ to refuse access by an Act that prohibits the disclosure of the personal information; and an agency is ‘authorised’ to refuse access by an Act that authorises or confers discretion on the agency to refuse a request for access to the personal information.

---

Authority to refuse access under the FOI Act

12.27 The FOI Act lists several grounds on which an agency can refuse a request under the Act for access to documents. An agency may rely on any of those grounds to refuse access under APP 12. It is nevertheless open to an agency not to rely on any such ground and to provide access upon request, unless disclosure is prohibited, for example, by a secrecy provision.7

12.28 The grounds on which an access request can be declined under the FOI Act include:8

- a document is an exempt document under Part IV, Division 2 of the FOI Act, for example, the document is a Cabinet document, is subject to legal professional privilege, contains material obtained in confidence, or a secrecy provision applies
- a document is a conditionally exempt document under Part IV, Division 3 of the FOI Act, for example, the document contains deliberative matter, or disclosure of the document would involve the unreasonable disclosure of personal information about another person and it would be contrary to the public interest to release the document at that time
- the individual is not entitled to obtain access to a document of the kind requested, for example, the document is available for purchase from an agency (FOI Act, ss 12, 13)
- providing access in the terms requested by a person would substantially and unreasonably divert an agency’s resources from its other operations (s 24AA)
- processing a person’s request would require an agency to disclose the existence or non-existence of a document, where that would otherwise be exempt information (s 25).

12.29 The FOI Act specifies consultation processes that may apply to requests made under that Act, for example, where a ‘practical refusal reason’ may apply (FOI Act, s 24) to the request, or where a requested document contains a third party’s personal or business information (FOI Act, ss 27, 27A). An agency is not required to undertake any of those consultation processes before refusing access on any of those grounds under APP 12. This is required only if the person decides to make a request under the FOI Act.

12.30 A decision to refuse access under APP 12.2(b)(i) (on one of the FOI grounds listed above) is a decision made under the Privacy Act, not the FOI Act. As required by APP 12.9, the agency must provide the individual with a written notice that sets out the reasons for the refusal and the complaint mechanisms available to the individual (see paragraph 12.87 below). The individual may have a right to complain to the Information Commissioner under the Privacy Act. After investigation, the Commissioner may make a

---

7 The same discretionary principle applies under the FOI Act. Section 3A of the FOI Act provides that it does not limit any power of an agency to publish or grant access to information under other legislative or administrative schemes.

8 The Australian Information Commissioner has issued guidelines (the FOI Guidelines) under s 93A of the FOI Act to which regard must be had for the purposes of performing a function, or exercising a power, under that Act. See OAIC, Guidelines issued by the Australian Information Commissioner under s 93A of the Freedom of Information Act 1982, OAIC website <www.oaic.gov.au>.
determination that the agency has failed to comply with APP 12 and require, for example, that the agency give access (Privacy Act, s 52). However, the individual will not have a right to seek internal review or Information Commissioner review under the FOI Act.

Required or authorised to refuse access under another Act

12.31 APP 12.2(b)(ii) provides that an agency is not required to give access to personal information if it is required or authorised to refuse to give access by another Act that provides for access by persons to documents. An example is a statutory secrecy provision that requires or authorises that access be refused in certain circumstances.

12.32 A further example is that the National Archives of Australia (NAA) is authorised to refuse access to certain ‘exempt records’ under the Archives Act 1983 (the Archives Act). The Archives Act provides that the NAA must make available for public access Commonwealth records in the open access period that are in the care of the NAA and that are not exempt records (s 31 of the Archives Act). The categories of exempt records include information whose disclosure would constitute a breach of confidence, would involve the unreasonable disclosure of information relating to the personal affairs of any person, or would unreasonably affect a person adversely in relation to his or her business, financial or professional affairs (s 33 of the Archives Act).9

Refusing to give access under APP 12 — organisations

12.33 APP 12.3 lists ten grounds on which an organisation can refuse to give access to personal information. It is nevertheless open to an organisation not to rely on any such ground and to provide access upon request, unless disclosure is prohibited. Before relying on any of these grounds an organisation should consider whether redacting some information would enable access to be provided (for example, redacting personal information about another person).

12.34 The grounds, which are considered separately below, are:

- the organisation reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety (APP 12.3(a))
- giving access would have an unreasonable impact on the privacy of other individuals (APP 12.3(b))
- the request for access is frivolous or vexatious (APP 12.3(c))
- the information relates to existing or anticipated legal proceedings between the organisation and the individual, and would not be accessible by the process of discovery in those proceedings (APP 12.3(d))
- giving access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations (APP 12.3(e))

---

9 For further information about the National Archives of Australia’s obligation to make available Commonwealth records for public access, see National Archives of Australia website <www.naa.gov.au>.
• giving access would be unlawful (APP 12.3(f))
• denying access is required or authorised by or under an Australian law or a court/tribunal order (APP 12.3(g))
• the organisation has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the organisation’s functions or activities has been, is being or may be engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter (APP 12.3(h))
• giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body (APP 12.3(i))
• giving access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process (APP 12.3(j)).

Giving access would pose a serious threat to the life, health or safety of any individual or to public health or public safety

12.35 The phrase, ‘serious threats to the life, health or safety of any individual, or to public health or public safety’ is discussed in Chapter C (Permitted general situations).

12.36 An example of where this ground might apply is a healthcare provider having reasonable grounds to believe that giving an individual access to their personal information may cause that person significant distress or lead to self-harm or harm to another person.

Giving access would have an unreasonable impact on the privacy of other individuals

12.37 This ground may apply where the record of personal information that an individual has requested contains personal information of another individual. As noted above (paragraph 12.12), a record of an individual’s opinions or views (for example, a referee comment) may be personal information of that individual.  

12.38 Before relying on this ground an organisation must be satisfied that giving access would have ‘an unreasonable impact’ on the privacy of another. Factors that may be relevant in deciding that issue include:

• the nature of the personal information about the other individual. For example, if the personal information is of a sensitive or confidential nature it may be unreasonable to provide it to others
• the reasonable expectation of the other individual about how that personal information will be handled (this should be assessed objectively and on the basis that the other individual may not have special knowledge of the industry or activity involved). For example, if both individuals were present when the personal

---

10 For further discussion of where giving access would have an unreasonable impact on the privacy of other individuals, see Smallbone v New South Wales Bar Association [2011] FCA 1145 (6 October 2011).
information was collected, there may be a reasonable expectation that each individual could later access the personal information

• the source of the personal information. For example, if the individual requesting access provided the personal information about the other individual, access may not have an unreasonable impact on that person

• whether the personal information of another individual could be redacted from the record provided to the individual requesting access

• whether access could be provided through an intermediary (see paragraphs 12.72–12.75 below)

• whether the other individual consents to access being given to the individual requesting access.

12.39 In applying this ground, an organisation may consult the other individual about whether giving access would have an unreasonable impact on their privacy. The view expressed by that individual may be relevant but not determinative. However, before consulting another individual, an organisation should consider whether doing so poses a privacy risk for the individual seeking access.

The request for access is frivolous or vexatious

12.40 A request should not be refused on this ground unless there is a clear and convincing basis for deciding that a request is frivolous or vexatious. It is not a sufficient basis, for example, that a request would cause inconvenience or irritation to an organisation.

12.41 The following are given as examples of requests that may be treated as frivolous or vexatious:

• repeated requests for access to personal information that has already been provided to the requester

• a request that contains offensive or abusive language, or that does not appear to be a genuine request for personal information

• a repeat request for personal information that an organisation has earlier explained to an individual it does not hold, has been destroyed, or cannot be located after a reasonable search

• a request made for the apparent purpose of harassing or intimidating the staff of an organisation, or interfering unreasonably with its operations.

The information requested relates to an existing or anticipated legal proceeding

12.42 This ground applies where legal proceedings between the individual and the organisation are underway or anticipated, and the information would not be accessible by the process of discovery in those proceedings. A legal proceeding is anticipated if there is a real prospect of proceedings being commenced, as distinct from a mere possibility.
Giving access would prejudice negotiations between the organisation and the individual

12.43 This ground applies where giving access would prejudice negotiations between the organisation and the individual by revealing the intentions of the organisation in relation to the negotiations. The negotiations may be current or reasonably anticipated.

12.44 Examples of where this ground might apply is an organisation negotiating:

- a claim brought by an individual for compensation (for example, for negligence or wrongful dismissal), and releasing the personal information requested by the individual may reveal the organisation’s strategy to settle or defend the claim
- a sponsorship arrangement with an individual, and releasing the personal information requested by the individual may reveal the organisation’s strategy in relation to negotiating the arrangement.

12.45 This exception applies only to personal information that would prejudice negotiations, and not to all information relevant to the negotiations. Access should be provided to other personal information that is requested, unless another exception applies.

Giving access would be unlawful

12.46 ‘Unlawful activity’ is not defined in the Privacy Act. The core meaning is activity that is criminal, illegal or prohibited or proscribed by law, and can include unlawful discrimination or harassment, but does not include breach of a contract. Examples of unlawful activity include criminal offences, unlawful discrimination, and trespass.

12.47 Examples of where this ground might apply are where giving access would be a breach of legal professional privilege, a breach of confidence or a breach of copyright.

Denying access is required or authorised by law or a court/tribunal order

12.48 The meaning of ‘required or authorised by or under an Australian law or a court/tribunal order’ is discussed in Chapter B (Key concepts). This ground applies where an Australian law or court or tribunal order forbids the disclosure of information; or a law or order authorises or confers discretion on an organisation to refuse a request from an individual for access to their personal information. (There is overlap between this ground and the preceding ground ‘giving access would be unlawful’.)

12.49 An example of where this ground might apply is a court order providing that an organisation is not required to provide personal information to an individual who is in the care of or is undergoing treatment by the organisation.

Giving access would likely prejudice the taking of appropriate action in relation to suspected unlawful activity or serious misconduct

12.50 There are a number of separate elements to this ground.

12.51 First, an organisation must have reason to suspect that unlawful activity or misconduct of a serious nature has been, is being or may be engaged in. The term
‘unlawful activity’ is not defined in the Privacy Act. The core meaning is activity that is criminal, illegal or prohibited or proscribed by law, and can include unlawful discrimination or harassment, but does not include breach of a contract. Examples of unlawful activity include criminal offences, unlawful discrimination, and trespass.

12.52 Misconduct is defined in s 6(1) to include ‘fraud, negligence, default, breach of trust, breach of duty, breach of discipline or any other misconduct in the course of duty’. An added requirement of this ground is that the misconduct is ‘serious’ in nature. This excludes minor breaches or transgressions.

12.53 The organisation must have ‘reason to suspect’ the unlawful activity or serious misconduct has been, is being or may be engaged in. This is a different and lesser standard to ‘reasonably believes’, which is used in some other APPs (see Chapter B (Key concepts)). There should nevertheless be a reasonable basis for the suspicion. It is the responsibility of the organisation to be able to justify its reasonable basis for the suspicion.

12.54 The suspected unlawful activity or serious misconduct must relate to the organisation’s functions or activities. As discussed in Chapter 3 (APP 3), an organisation’s functions or activities include current, proposed and support functions and activities.

12.55 Lastly, giving access must be likely to prejudice the organisation in taking appropriate action in relation to the suspected unlawful activity or serious misconduct. The proposed action may include investigation of the activity or misconduct, or reporting it to the police or another relevant person or authority. There should again be a reasonable basis for this expectation of prejudice. For example, in some instances giving an individual access would not prejudice the taking of appropriate action, but would allow the individual to provide further information relevant to the suspected unlawful activity.

12.56 An example of where this ground might apply is where giving access to the requested personal information would reveal that, covertly but lawfully, an organisation is investigating suspected misconduct of a client and disclosure would prejudice the covert investigation.

**Giving access would be likely to prejudice an enforcement related activity conducted by, or on behalf of, an enforcement body**

12.57 ‘Enforcement body’ is defined in s 6(1) as a list of specific bodies. The list includes Commonwealth, State and Territory bodies that are responsible for policing, criminal investigations, and administering laws to protect the public revenue or to impose penalties or sanctions. Examples of Commonwealth enforcement bodies are the Australian Federal Police, the Australian Crime Commission, Customs, the Integrity Commissioner, the Immigration Department, the Australian Prudential Regulation Authority, the Australian Securities and Investments Commission and AUSTRAC.

---

11 ‘Integrity Commissioner’ is defined in s 6(1) as having the same meaning as in the *Law Enforcement Integrity Commissioner Act 2006*.

12 ‘Immigration Department’ is defined in s 6(1) as the Department administered by the Minister administering the *Migration Act 1958*. 
12.58 ‘Enforcement related activity’ is also defined in s 6(1). It includes the prevention, detection, investigation and prosecution or punishment of criminal offences and intelligence gathering activities.

12.59 The terms ‘enforcement related activity’ and ‘enforcement body’ are discussed in Chapter B (Key concepts).

12.60 An example of where this ground might apply is an enforcement body asking an organisation not to give an individual access to certain personal information, as doing so would be likely to reveal the existence of a criminal investigation or interfere with preparation for court proceedings.

Giving access would reveal evaluative information in connection with a commercially sensitive decision-making process

12.61 This ground applies if giving access would reveal ‘evaluative information’ generated within an organisation in connection with a commercially sensitive decision-making process. An example of evaluative information is a score card weighting system and score card result. The ground applies only to the evaluative information, and not to personal information on which a decision was based.\(^{13}\)

12.62 APP 12.10 provides that if an organisation refuses to give access to personal information under this ground, its written notice explaining the reasons for refusal may include an explanation for the commercially sensitive decision. This may include explaining the reasons for the decision and giving a copy of the personal information that informed the decision. For discussion of the requirement to give a written notice refusing access, see paragraphs 12.82–12.87 below.

APP 12 minimum access requirements

12.63 APP 12 sets out minimum access requirements that must be met when an APP entity receives a request from an individual for access to their personal information. The access requirements relate to the response time, how access is to be given, access charges and giving a written notice, including the reasons for refusal, if access is refused.

12.64 An individual may complain under s 36 to the Information Commissioner about the failure of an APP entity to comply with any of the APP 12 minimum access requirements. The Commissioner will not investigate a complaint if the person has not first raised the matter with the entity complained about, unless it was not appropriate to require that as a first step (s 40(1A)). When investigating a complaint, the OAIC will initially attempt to conciliate the complaint (s 40A), before considering the exercise of other complaint resolution powers (s 52).

Difference with access requirements applying to agencies under FOI Act

12.65 The APP 12 minimum access requirements and the Privacy Act complaint and review mechanisms differ in important respects from those applying to agencies in

---

\(^{13}\) See also C v Insurance Company [2006] PrivCmrA 3 (1 February 2006).
Chapter 12: APP 12 — Access to personal information

12.66 APP 12.4(a)(i) provides that an agency must ‘respond’ to a request for access within 30 calendar days. The 30 day time period commences on the day after the day the agency receives the request. The agency must respond by giving access to the personal information that is requested, or by notifying its refusal to give access. If this is impracticable (for example, there is a justifiable need to clarify the scope of an individual’s request, or to locate and assemble the requested information, or to consult a third party), the agency is expected to contact the individual to explain the delay and provide an expected timeframe for finalising the request. These are matters the Information Commissioner may examine if a complaint is made about an agency’s failure to comply with the timeframe in APP 12.4(a).

12.67 APP 12.4(a)(ii) provides that an organisation must respond ‘within a reasonable period after the request is made’. As with agencies, an organisation must respond by giving access to the personal information that is requested, or by notifying its refusal to give access. Factors that may be relevant in deciding what is a reasonable period include the scope and clarity of a request, whether the information can be readily located and assembled, and whether consultation with the individual or other parties is required. However, as a general guide, a reasonable period should not exceed 30 calendar days.

12.68 An APP entity must give access to personal information in the manner requested by the individual, if it is reasonable and practicable to do so (APP 12.4(b)). The manner of access may, for example, be by email, by phone, in person, hard copy, or an electronic record.

---

14 The circumstances in which an individual may apply to the Administrative Appeals Tribunal for review of a decision of the Information Commissioner are set out in s 96.

12.69 Factors relevant in assessing whether it is reasonable and practicable to give access in the manner requested by an individual include:

- the volume of information requested. For example, it may be impracticable to provide a large amount of personal information by telephone
- the nature of the information requested. For example, it may be impracticable to give access to digitised information in hard copy and it may be unreasonable to give access to information of a highly sensitive nature by telephone if the APP entity cannot sufficiently verify the individual’s identity over the telephone
- any special needs of the individual requesting the information. For example, it may be reasonable to give information in a form that can be accessed via assistive technology where this meets the special needs of the individual.

**Giving access by other means**

12.70 APP 12.5 applies where an APP entity refuses to give access to personal information under APP 12 on a permitted ground, or refuses to give access in the manner requested by the individual. The entity must take reasonable steps to give access in a way that meets the needs of the entity and the individual. This should be done within 30 calendar days where practicable.

12.71 The APP entity is expected to consult the individual to try to satisfy their request. The following are given as examples of alternative manners of access that may meet the needs of the entity and the individual, and in particular result in more rather than less personal information being provided to an individual:

- deleting any personal information for which there is a ground for refusing access and giving the redacted version to the individual
- giving a summary of the requested personal information to the individual
- giving access to the requested personal information in an alternative format
- facilitating the inspection of a hard copy of the requested personal information and permitting the individual to take notes
- facilitating access to the requested personal information through a mutually agreed intermediary (see paragraphs 12.72–12.75 below).

**Giving access through an intermediary**

12.72 APP 12.6 provides that, without limiting APP 12.5, ‘access may be given through the use of a mutually agreed intermediary’.

12.73 The role of an intermediary is to enable an individual to be given access to their personal information and to have the content of that information explained, where direct access would otherwise be refused. An example is an organisation refusing direct access under APP 12.3(a) on the reasonable belief that access may lead the individual to self-harm, but deciding that access through an intermediary may not pose a similar threat. The role of the intermediary in conveying or explaining the information to the individual

---

16 Explanatory memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 87.
will need to be tailored to the nature of the information and any instructions given by the APP entity to the intermediary.

12.74 The intermediary must be acceptable to both the APP entity and the individual. In seeking an individual’s agreement to use an intermediary, an entity should clearly explain the process and the type of access that will be provided through this process. Depending on the nature of the personal information to which access is sought, the intermediary may need particular skills or knowledge. For example, an intermediary may need to be a qualified health service provider if used to give access to health information.

12.75 If an individual does not agree to the use of an intermediary, or agreement cannot be reached on whom to use as the intermediary, the APP entity must still take reasonable steps to give access through another manner that meets the needs of the entity and the individual.

Access charges under APP 12 — agencies

12.76 An agency cannot impose upon an individual any charge for providing access to personal information under APP 12 (APP 12.7). This includes:

- a charge for the making of the request to access personal information
- a charge for giving access to requested personal information, such as charges for copying costs, postage costs and costs associated with using an intermediary.

Access charges under APP 12 — organisations

12.77 An organisation cannot impose upon an individual a charge for the making of the request to access personal information.

12.78 An organisation may, however, impose a charge for giving access to requested personal information, provided the charge is not excessive (APP 12.8). Items that may be charged for include:

- staff costs in searching for, locating and retrieving the requested personal information, and deciding which personal information to provide to the individual
- staff costs in reproducing and sending the personal information
- costs of postage or materials involved in giving access
- costs associated with using an intermediary (see paragraphs 12.72–12.75 above).

12.79 Whether a charge is excessive will depend on the nature of the organisation, including the organisation’s size, resources and functions, and the nature of the personal information held. The following charges may be considered excessive:

- a charge that exceeds the actual cost incurred by the organisation in giving access
- a charge associated with obtaining legal or other advice in deciding how to respond to an individual’s request
- a charge for consulting with the individual about how access is to be given
• a charge that reflects shortcomings in the organisation’s information management systems. An individual should not be disadvantaged because of the deficient record management practices of an organisation.

12.80 An organisation should also consider waiving, reducing or sharing any charge that may be imposed, so that the charge is not excessive. In determining the amount to charge, an organisation should consider:

• the organisation’s relationship with the individual
• any known financial hardship factors claimed by the individual
• any known adverse consequences on the individual if they do not get access to the personal information.

12.81 A charge by an organisation for giving access must not be used to discourage an individual from requesting access to personal information. To the extent practicable, an organisation should advise an individual in advance if a charge may be imposed, and the likely amount of the charge. The individual should be invited to discuss options for altering the request to minimise any charge. This may include options for giving access in another manner that meets the needs of the entity and the individual (see APP 12.5 and paragraphs 12.70–12.71 above). Any charge that is imposed should be clearly communicated and explained before access is given.

**Giving written notice where access is refused, or not given in the manner requested under APP 12**

12.82 APP 12.9 provides that if an APP entity refuses to give access, or to give access in the manner requested by the individual, the entity must give the individual a written notice setting out:

• the reasons for the refusal, except to the extent that it would be unreasonable to do so, having regard to the grounds for refusal
• the complaint mechanisms available to the individual, and
• any other matters prescribed by regulations made under the Privacy Act.

12.83 The reasons for refusal should explain, where applicable:

• that the entity does not hold the requested personal information
• the ground of refusal. For example, if the entity is required or authorised by an Australian law to refuse access, notice should include the name of that law and, if practicable, could include the provision relied upon
• that access cannot be given in the manner requested by the individual, and the reason why
• that the steps necessary to give access in a way that meets the needs of the entity and the individual under APP 12.5 are not reasonable in the circumstances.

12.84 The notice could, in addition, set out any steps that may be taken by the individual that would mean that access would not be refused, for example, by re-framing or narrowing the scope of the individual’s request.
12.85  APP 12.10 additionally provides that, where an organisation relies on the commercially sensitive decision ground in APP 12.3(j), the written notice may provide an explanation for the commercially sensitive decision (see paragraphs 12.61–12.62 above).

12.86  An APP entity is not required to explain the ground of refusal to the extent that it would be unreasonable to do so. This course should be adopted only in justifiable circumstances. Examples for organisations include that an explanation may prejudice action by an organisation to respond to unlawful activity (APP 12.3(h)); may prejudice enforcement action by an enforcement body (APP 12.3(i)). An example for agencies is that this would reveal the existence of a document whose existence an agency would be entitled to neither confirm nor deny under s 25 of the FOI Act.

12.87  The description of the complaint mechanisms available to an individual should explain the internal and external complaint options, and the steps that should be followed. In particular, the individual should be advised that:

- a complaint should first be made in writing to the APP entity (s 40(1A))
- the entity should be given a reasonable time (usually 30 days) to respond
- a complaint may then be taken to a recognised external dispute resolution scheme of which the entity is a member (if any), and
- lastly, a complaint may be made to the Information Commissioner (s 36).
Chapter 13: Australian Privacy Principle
13 — Correction of personal information

Version 1.0, February 2014

Key points ................................................................................................................................................ 2
What does APP 13 say? ................................................................................................................................ 2
Interaction of APP 13 and other correction procedures ................................................................. 3
Interaction of APP 13 and other APPs ................................................................................................. 3
‘Holds’ .................................................................................................................................................... 4
Taking reasonable steps to correct personal information .............................................................. 5
Correcting at the APP entity’s initiative ............................................................................................... 5
Correcting at the individual’s request .................................................................................................... 5
Agencies — comparison of APP 13 and FOI Act procedures ............................................................... 6
Grounds for correcting personal information ....................................................................................... 8
Accurate .................................................................................................................................................... 9
Up-to-date ............................................................................................................................................... 9
Complete ............................................................................................................................................... 9
Relevant ................................................................................................................................................ 10
Not misleading ..................................................................................................................................... 10
Being satisfied and taking reasonable steps ....................................................................................... 10
Being satisfied ..................................................................................................................................... 10
Reasonable steps to correct .................................................................................................................. 11
APP 13 minimum procedural requirements ....................................................................................... 12
Taking reasonable steps to notify another APP entity ...................................................................... 12
Giving written notice where correction is refused .............................................................................. 14
Taking reasonable steps to associate a statement .............................................................................. 14
Timeframe for responding to a request for correction under APP 13 .......................................... 15
Access charges under APP 13 ................................................................................................................. 16
Key points

- **APP 13** requires an APP entity to take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading.

- This requirement applies where:
  - the APP entity is satisfied the personal information is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to a purpose for which it is held, or
  - the individual requests the entity to correct the personal information.

- Special considerations apply to Commonwealth records, which can only be destroyed or altered in accordance with the *Archives Act 1983* (Archives Act).

- APP 13 also sets out other minimum procedural requirements in relation to correcting personal information, including when an APP entity must:
  - take reasonable steps to notify other APP entities of a correction
  - give notice to the individual which includes reasons and available complaint mechanisms if correction is refused
  - take reasonable steps to associate a statement with personal information it refuses to correct
  - respond to a request for correction or to associate a statement, and
  - not charge an individual for making a request, correcting personal information or associating a statement.

- APP 13 operates alongside and does not replace other informal or legal procedures by which an individual can seek correction of their personal information, including informal arrangements and, for agencies, the *Freedom of Information Act 1982* (FOI Act).

**What does APP 13 say?**

13.1 **APP 13.1** provides that an APP entity must take reasonable steps to correct personal information it holds, to ensure it is accurate, up-to-date, complete, relevant and not misleading, having regard to the purpose for which it is held. The shorthand expression used in this chapter is that an APP entity is required to correct ‘incorrect personal information’.

13.2 The requirement to take reasonable steps applies in two circumstances:

- where an APP entity is satisfied, independently of any request, that personal information it holds is incorrect, or
- where an individual requests an APP entity to correct their personal information.
13.3 Special considerations apply to Commonwealth records. A Commonwealth record can, as a general rule, only be destroyed or altered in accordance with the Archives Act (see paragraph 13.48).

13.4 APP 13 also sets out other minimum procedural requirements in relation to correcting personal information. An APP entity must:

- upon request by an individual whose personal information has been corrected, take reasonable steps to notify another APP entity of a correction made to personal information that was previously provided to that other entity (APP 13.2)
- give a written notice to an individual when a correction request is refused, including the reasons for the refusal and the complaint mechanisms available to the individual (APP 13.3)
- upon request by an individual whose correction request has been refused, take reasonable steps to associate a statement with the personal information that the individual believes it to be inaccurate, out-of-date, incomplete, irrelevant or misleading (APP 13.4)
- respond in a timely manner to an individual’s request to correct personal information or to associate a statement with the personal information (APP 13.5(a))
- not charge an individual for making a request to correct personal information or associate a statement, or for making a correction or associating a statement (APP 13.5(b)).

Interaction of APP 13 and other correction procedures

13.5 APP 13 operates alongside and does not replace other informal or legal procedures by which an individual can request that personal information be corrected. In particular, APP 13 does not prevent an APP entity from correcting personal information under an informal administrative arrangement, provided the arrangement satisfies the requirements of APP 13. For example, an entity may allow individuals to correct their personal information by providing updated information through an online portal.

13.6 For agencies, APP 13 operates alongside the right to amend or annotate personal information in Part V of the Freedom of Information Act 1982 (FOI Act). The FOI Act procedures, criteria and review mechanisms differ in important respects from those applying under APP 13 and the Privacy Act. These differences, and when it is more appropriate to use one Act rather than another, are considered below at paragraphs 13.25–13.29.

Interaction of APP 13 and other APPs

13.7 The correction requirements in APP 13 complement and overlap with the requirements in other APPs, including APP 10 (quality of personal information) and APP 11 (security of personal information).

13.8 APP 10 provides that an APP entity must take reasonable steps to ensure the quality of personal information it collects, uses or discloses (see Chapter 10 (APP 10)). If reasonable steps are taken to comply with APP 10, this reduces the likelihood that
personal information will need correction under APP 13. Similarly, by taking reasonable steps to correct personal information under APP 13, an entity can better ensure that it complies with APP 10 by ensuring that information is accurate, up-to-date, complete and relevant when it is used or disclosed.

13.9 APP 11.1 provides that an APP entity must take reasonable steps to protect the personal information it holds, including from interference, loss and unauthorised modification. If reasonable steps are taken to comply with APP 11.1, this reduces the likelihood that personal information will need correction under APP 13. APP 11.2 provides that an entity must take reasonable steps to destroy or de-identify personal information that it no longer needs for any purpose for which it may be used or disclosed. This requirement does not apply where the information is contained in a Commonwealth record or where the entity is required by law or a court/tribunal order to retain the personal information (see Chapter 11 (APP 11)). When taking steps to identify and correct incorrect personal information under APP 13, an entity should consider whether it still needs the personal information for a permitted purpose, or whether reasonable steps must be taken to destroy or de-identify the information under APP 11.2.

‘Holds’

13.10 APP 13 only applies to personal information that an APP entity ‘holds’. An entity ‘holds’ personal information ‘if the entity has possession or control of a record that contains the personal information’ (s 6(1)).

13.11 The term ‘holds’ extends beyond physical possession of a record to include a record that an entity has the right or power to deal with. For example, an APP entity that has outsourced the storage of personal information to a third party, but retains the right to deal with that information, including to access and amend it, holds that personal information and must comply with APP 13 (see paragraph 13.47 below). In addition, the individual has a separate right to request correction of the information by the third party, if the third party is an APP entity.

13.12 An agency that has placed a record of personal information in the care of the National Archives of Australia, or in the custody of the Australian War Memorial, is considered to be the agency that holds the record for the purposes of the Privacy Act (s 10(4)).

13.13 Upon receiving a request for correction, an APP entity should search the records that it possesses or controls to assess whether the personal information to be corrected is contained in those records. For example, an entity may search hard copy records and electronic databases and make enquiries of staff or contractors with relevant knowledge. A discussion with the individual may assist the entity to locate the information.

13.14 The term ‘holds’ is discussed in more detail in Chapter B (Key concepts).
Taking reasonable steps to correct personal information

13.15 APP 13.1 requires an APP entity to take reasonable steps to correct personal information it holds, in two circumstances: on its own initiative, and at the request of the individual to whom the personal information relates.

Correcting at the APP entity’s initiative

13.16 An APP entity is required to take reasonable steps to correct personal information it holds if the entity is satisfied, having regard to a purpose for which the personal information is held, that it is inaccurate, out-of-date, incomplete, irrelevant or misleading (that is, the personal information is incorrect). Implicit in that requirement is that an entity should be alert to the possibility that personal information it holds may be incorrect and may require correction.

13.17 Generally, an APP entity may become aware that an item of personal information requires correction if it discovers an inconsistency during normal business practices. Examples include:

- information provided to the entity by the individual or a third party may be inconsistent with other personal information held by the entity. For example, an identity document, letter, medical record or photograph
- a court or tribunal has made a finding about the personal information, in a case involving the entity or in another case that comes to the entity’s notice
- the entity may be notified by another entity or person that the personal information is incorrect, or that similar personal information held by the other entity has been corrected
- a practice, procedure or system the entity has implemented in compliance with APP 1.2 (such as an auditing or monitoring program) indicates that personal information the entity holds requires correction.

13.18 After becoming aware that personal information may require correction, the APP entity should satisfy itself that the information is incorrect, before taking reasonable steps to correct it (see paragraphs 13.30–13.41).

Correcting at the individual’s request

13.19 An APP entity is required by APP 13.1 to take reasonable steps to correct an individual’s personal information to ensure it is not incorrect when the individual ‘requests’ the entity to do so. Upon receiving a request an entity must decide if it is satisfied that the information is incorrect, and if so, take reasonable steps to correct it (see paragraphs 13.43–13.48 below).

13.20 APP 13 does not stipulate formal requirements that an individual must follow to make a request, or require that a request be made in writing, or require the individual to state that it is an APP 13 request.¹

¹ This differs from the formal requirements relating to requests for amendment or annotation under the FOI Act (see FOI Act, Part III).
13.21 An APP entity is required by APP 1.4(d) to state in an APP Privacy Policy how an individual may seek the correction of their personal information held by the entity. An APP entity is also required by APP 5.2(g) to take reasonable steps to notify an individual, or ensure they are aware, of the fact the entity’s APP Privacy Policy contains information about how the individual may seek correction of their personal information held by the entity.

13.22 If an APP entity wishes an individual to follow a particular procedure in requesting correction of their personal information, the entity could publish that procedure and draw attention to it, for example, by providing a link in the APP Privacy Policy and on the entity’s website homepage to the correction request procedure, to an online request form, or to an online portal that enables an individual to correct their personal information. However, an entity cannot require an individual to follow a particular procedure, use a designated form or explain the reason for making the request. Any recommended procedure should be regularly reviewed to ensure that it is flexible and facilitates rather than hinders correction of personal information.

13.23 An APP entity must be satisfied that a request to correct personal information under APP 13 is made by the individual concerned, or by another person who is authorised to make a request on their behalf, for example, a legal guardian or authorised agent. The steps appropriate to verify an individual’s identity will depend on the circumstances, and in particular, whether the individual is already known to or readily identifiable by the entity. The discussion in Chapter 12 (APP 12) of steps that can be taken to verify the identity of an individual seeking access to their personal information apply also to APP 13.

13.24 APP 13 stipulates minimum procedural requirements that must be met by an APP entity when dealing with a request to correct personal information. These are discussed later in this chapter, and include taking reasonable steps if requested by the individual to notify other APP entities when a correction is made (see paragraphs 13.49–13.53), providing an individual with a written notice that includes the reasons for refusal if a correction request is refused (paragraphs 13.54–13.58), response times (paragraphs 13.63–13.64) and charging (paragraph 13.65). Provided an entity meets those minimum requirements, it may choose the arrangements (including an informal arrangement) for receiving and acting upon correction requests. An online portal through which individuals can access and correct their personal information is an example of an informal arrangement that may provide a fast and easy means of correction, and that can qualify as an APP 13 ‘request’ procedure.

Agencies — comparison of APP 13 and FOI Act procedures

13.25 For agencies, APP 13 operates alongside the right to amend or annotate personal information in Part V of the FOI Act. There is substantial overlap between the APP 13 and the FOI Act procedures, but also some noteworthy differences.
13.26 The FOI Act provides that a person may apply to an agency to amend or annotate a record of personal information about that person, to which they have lawfully had access under the FOI Act or otherwise (FOI Act, s 48). The application must be in writing, specify as far as practicable how and why the record should be amended or annotated, and provide a return address to which notices can be sent (FOI Act, ss 49, 51A). The grounds on which such an application may be made are that the record of personal information ‘is incomplete, incorrect, out of date or misleading’ (FOI Act, s 48(a)). The record must also have been used or be available for use by the agency ‘for an administrative purpose’ (FOI Act, s 48(b)). The agency may act upon an application by altering or adding a note to a record, but as far as practicable must not obliterate the text of the record as it existed prior to the amendment (FOI Act, s 50). An applicant whose application is not accepted may provide a statement specifying their disagreement with the decision, and the agency must annotate the record by attaching that statement (FOI Act, ss 51, 51B). The time period for making a decision on an applicant’s application is 30 calendar days. An applicant may apply for internal review or Information Commissioner review of an adverse decision.

13.27 While APP 13 sets out minimum procedural requirements (see paragraph 13.24), these are not as detailed as in the FOI Act. However, in two respects APP 13 goes further than the FOI Act:

- The grounds for correction in APP 13 are that the personal information is ‘inaccurate, out-of-date, incomplete, irrelevant or misleading’. The main additional ground in this list is that the information is ‘irrelevant’. The other wording difference — ‘inaccurate’ in APP 13, ‘incorrect’ in the FOI Act — is not substantive.

- If an agency corrects personal information, the agency must, if requested by the individual, take reasonable steps under APP 13 to notify that change to any APP entity to which the personal information was previously disclosed, unless it is unlawful or impracticable to do so (see paragraphs 13.49–13.53). Where an agency amends personal information under the FOI Act, an agency could consider providing similar notification on request from the individual.

13.28 The complaint options available to the individual under the FOI Act and APP 13 also differ. Under the FOI Act, a person may apply for Information Commissioner review of an agency’s or Minister’s failure to amend or annotate a record in accordance with the person’s request. The Commissioner may exercise the agency’s or Minister’s discretion to amend or annotate a record. Under the Privacy Act, an individual may complain to the Information Commissioner about an APP entity’s failure to take reasonable steps to correct personal information to ensure it is not incorrect. After investigation, the Commissioner may find that an agency has failed to take reasonable steps to correct personal information or to comply with the minimum procedural requirements (see paragraphs 13.54–13.65) under APP 13. The Commissioner may make a determination to that effect, and require, for example, the entity to correct personal information or to comply with the minimum procedural requirements (Privacy Act, s 52).

---

2 The FOI Act is expressed to apply separately to Minister’s offices in respect of ‘an official document of a Minister’ (FOI Act, s 48). APP 13 also applies to Minister’s offices: see the discussion of ‘APP entity’ in Chapter B (Key concepts), and the Privacy Act, s 7(1)(d),(e).
13.29 It is open to an individual to decide whether to make an application under the FOI Act or a request under APP 13. Agencies could ensure, in appropriate cases, that people are made aware of both options and the substantive differences. An agency could refer to the FOI Act in the agency’s APP Privacy Policy. More detailed information could be provided by an agency in other ways — such as a separate document that sets out the procedure for requesting correction of personal information (see paragraph 13.21), through an ‘Access to information’ icon on the agency’s website, or on a case-by-case basis as the need arises. An agency could draw attention to the more flexible procedure for which APP 13 provides. As explained in the FOI Guidelines, agencies should consider establishing administrative access arrangements that operate alongside the FOI Act and that provide an easier and less formal means for individuals to make information access requests (including requests to correct personal information). Correcting or annotating personal information under an administrative arrangement is consistent with an agency’s obligations under APP 13, provided the agency meets the minimum procedural requirements stipulated in APP 13.

**Grounds for correcting personal information**

13.30 The five grounds listed in APP 13 — ‘accurate’, ‘up-to-date’, ‘complete’, ‘relevant’ and ‘not misleading’ — are not defined in the Privacy Act. The first four terms are listed in APP 10.1, which deals with the quality of personal information that an APP entity can collect, use and disclose. Similar terms are used also in Part V of the FOI Act concerning a person’s right to apply to an agency to amend or annotate personal information (see paragraph 13.26 above).

13.31 The following analysis of each term draws on the ordinary dictionary meaning of the terms, as well as case law concerning the meaning of those terms in the Privacy Act, FOI Act and other legislation. As the analysis indicates, there is considerable overlap in the meaning of the terms.

13.32 In applying the terms to personal information, it is necessary to have regard to ‘the purpose for which it is held’. Personal information may be incorrect having regard to one purpose for which it is held, but not another. For a discussion of relevant considerations where personal information is held for multiple purposes, see paragraph 13.47.

---


Accurate

13.33 Personal information is inaccurate if it contains an error or defect. An example is incorrect factual information about an individual’s name, date of birth, residential address or current or former employment.\(^6\)

13.34 An opinion about an individual given by a third party is not inaccurate by reason only that the individual disagrees with that opinion or advice.\(^7\) For APP 13 purposes, the opinion may be ‘accurate’ if it is presented as an opinion and not objective fact, it accurately records the view held by the third party, and is an informed assessment that takes into account competing facts and views. Other matters to consider under APP 13, where there is disagreement with the soundness of an opinion, are whether the opinion is ‘up-to-date’, ‘complete’, ‘not misleading’ or ‘relevant’. If an individual disagrees with an opinion that is otherwise not incorrect, the individual may associate a statement with the record of the opinion (see paragraphs 13.59–13.62).

13.35 In relation to a similar issue, s 55M of the FOI Act provides that the Information Commissioner (in conducting an IC review) cannot alter a record of opinion unless satisfied that it was based on a mistake of fact, or the author of the opinion was biased, unqualified to form the opinion or acted improperly in conducting the factual inquiries that led to the formation of the opinion.

Up-to-date

13.36 Personal information is out-of-date if it contains facts, opinions or other information that is no longer current. An example is a statement that an individual lacks a particular qualification or accreditation that the individual has subsequently obtained.

13.37 Personal information about a past event may have been accurate at the time it was recorded, but has been overtaken by a later development. Whether that information is out-of-date will depend on the purpose for which it is held. If current information is required for the particular purpose, the information will to that extent be out-of-date. By contrast, if information from a past point in time is required for the particular purpose, the information may not be out-of-date for that purpose. Personal information held by an APP entity that is no longer needed for any purpose may need to be destroyed or de-identified under APP 11.2 (Chapter 11 (APP 11)).

Complete

13.38 Personal information is incomplete if it presents a partial or misleading picture, rather than a true or full picture. An example is a tenancy database which records that a tenant owes a debt, which in fact has since been repaid. The statement will be incomplete under APP 13 if the tenancy database is held for the purpose of assessing the tenancy record or reliability of individuals recorded in the database. Similarly, a statement that an individual has only two rather than three children will be incomplete

---


\(^7\) The definition of ‘personal information’ in the Privacy Act includes ‘information or an opinion’ (s 6(1)).
under APP 13 if that information is held for the purpose of, and is relevant to, assessing a person’s eligibility for a benefit or service.

**Relevant**

13.39 Personal information is irrelevant if it does not have a bearing upon or connection to the purpose for which the information is held.

**Not misleading**

13.40 Personal information is misleading if it conveys a meaning that is untrue or inaccurate or could lead a user, receiver or reader of the information into error. An example is a statement that is presented as a statement of fact but in truth is a record of the opinion of a third party. In some circumstances an opinion may be misleading if it fails to include information about the limited facts on which the opinion was based or the context or circumstances in which the opinion was first recorded.

13.41 A statement may also be misleading by failing to include other relevant information. An example is a statement that a dismissed employee was reinstated, without explaining that this followed the ruling of a court or tribunal that the dismissal was legally flawed.8

**Being satisfied and taking reasonable steps**

13.42 An APP entity is required to take ‘reasonable steps’ to correct personal information when ‘satisfied’ that it is inaccurate, out-of-date, incomplete, irrelevant or misleading for the purpose for which it is held.

**Being satisfied**

13.43 This requirement will not always involve distinct analysis or decision by an APP entity. For example, if an entity maintains an online portal through which a person can access and correct their personal information, no additional step may be required by the entity. Correction may similarly be a straightforward process in other situations where, for example, an individual presents information to indicate that their personal information is incorrect in an entity’s records.

13.44 Where correction is requested by an individual and an APP entity requires further information or explanation before it can be satisfied that personal information is incorrect, the entity should clearly explain to the individual what additional information or explanation is required and/or why the entity cannot act on the information already provided. The entity could also advise where additional material may be obtained. The individual should be given a reasonable opportunity to comment on the refusal or reluctance of the entity to make a correction without further information or explanation from the individual.

---

8 An organisation that is or was an employer of an individual is exempt from the operation of the Privacy Act where its act or practice is related directly to the employment relationship between the organisation and the individual, and an employee record held by the organisation (s 7B(3)).
13.45 An APP entity should also be prepared in an appropriate case to search its own records and other readily-accessible sources that it reasonably expects to contain relevant information to find any information in support of, or contrary to the individual’s request. For example, an entity could take into account a finding of an Australian court or tribunal relating to the personal information that has a bearing on whether it is or is not incorrect. However, an entity need not conduct a full, formal investigation into the matters about which the individual requests correction. The extent of the investigation required will depend on the circumstances, including the seriousness of any adverse consequences for the individual if the personal information is not corrected as requested.

13.46 Where personal information is held for multiple purposes, an APP entity need only be satisfied that the personal information requires correction having regard to one of the purposes for which it is held, not all purposes (see paragraph 13.46).

**Reasonable steps to correct**

13.47 A decision as to what constitutes ‘reasonable steps’ to correct personal information spans a range of options. These include making appropriate additions, deletions or alterations to a record, or declining to correct personal information if it would be unreasonable to take such steps. In some instances it may be appropriate to destroy or de-identify the personal information (there are separate requirements to destroy or de-identify personal information in APPs 4 and 11 — see Chapters 4 and 11 respectively). The reasonable steps that an APP entity should take will depend upon considerations that include:

- the sensitivity of the personal information. More rigorous steps may be required if the incorrect information is ‘sensitive information’ (defined in s 6(1) and discussed in Chapter B (Key concepts)) or other personal information of a sensitive nature
- the possible adverse consequences for an individual if a correction is not made. More rigorous steps may be required as the risk of adversity increases
- the practicability, including time and cost involved. However, an entity is not excused from correcting personal information by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances.
- the likelihood that the entity will use or disclose the personal information. For example, the likelihood of the entity using or disclosing the personal information may be relevant if it would be difficult or costly to make the correction requested by an individual.
- the purpose for which the personal information is held. As noted at paragraph 13.32, personal information may be held for multiple purposes, and require correction for one purpose but not for another purpose. Reasonable steps in these circumstances may require the entity to retain the original record of personal information for one purpose and create a record with the corrected personal information for another
• record-keeping requirements that apply to the personal information under an Australian law or court/tribunal order. For example the Health Practitioner Regulation 2010 (NSW), Schedule 2, clause 2

• whether the personal information is in the physical possession of the entity or a third party. For example, where personal information is in the physical possession of a third party, the entity may still ‘hold’ it (see discussion of ‘holds’ at paragraph 13.11) and be required to take reasonable steps to correct it. In these circumstances, it may be a reasonable step for the entity to notify the third party that the information is incorrect and request that it be corrected. It will not generally be sufficient to refer the individual to the third party with physical possession. However, the third party with physical possession may also ‘hold’ the personal information, and if so, the individual will have a separate right to request the third party to correct it.

13.48 Special considerations apply to Commonwealth records. The term ‘Commonwealth record’ is defined in s 3 of the Archives Act and is discussed in more detail in Chapter B (Key concepts). The definition is likely to include, in almost all cases, all personal information held by agencies. It may also include personal information held by contracted service providers. A Commonwealth record can, as a general rule, only be destroyed or altered in accordance with s 24 of the Archives Act. Further, s 26 of the Archives Act makes it an offence to alter a Commonwealth record that is over 15 years old. In relation to such records, and more generally, it may be reasonable (and consistent with statutory requirements) to:

• retain a version of a record which contains incorrect personal information (see paragraph 13.47)

• associate a statement to clarify that, having regard to the purpose for which the personal information is held, the personal information is not accurate, up-to-date, complete, relevant or is misleading, and either including the correct personal information in the note or cross referencing where it is held (such as in an attachment to the record).

APP 13 minimum procedural requirements

Taking reasonable steps to notify another APP entity

13.49 APP 13.2 provides that an APP entity must, on request, take reasonable steps to notify another APP entity of a correction made to personal information that was previously provided to that entity, unless it is impracticable or unlawful to do so. Implicit in this requirement is that an entity should take reasonable steps to inform the individual

---

9 Archives Act 1983, s 3: Commonwealth record means:
(a) a record that is the property of the Commonwealth or of a Commonwealth institution; or
(b) a record that is to be deemed to be a Commonwealth record by virtue of a regulation under subsection (6) or by virtue of section 22;
but does not include a record that is exempt material or is a register or guide maintained in accordance with Part VIII.

that they can make such a request. This information could be provided, for example, at the time, or as soon as practicable after, a correction is made.

13.50 The reasonable steps for an APP entity will depend upon considerations that include:

- the sensitivity of the personal information. More rigorous steps may be required for ‘sensitive information’ (defined in s 6(1) and discussed in Chapter B (Key concepts)) or other personal information of a sensitive nature
- the possible adverse consequences for an individual if notice is not provided to the other entity. More rigorous steps may be required as the risk of adversity increases
- the nature or importance of the correction. For example, it may not be reasonable to provide notice of a small typographical error that does not materially affect the quality of the personal information
- the length of time that has elapsed since the personal information was disclosed to the other entity, and the likelihood that it is still being used or disclosed by the other entity
- the materiality of the correction
- the practicability of providing notice to another entity. For example, it may be impracticable to do so if the other entity has ceased carrying on business or has been substantially restructured
- the practicability, including time and cost of providing a notice to all entities to which the personal information was previously provided. However, an entity is not excused from giving notification by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances.

13.51 An APP entity is not required to provide notice of a correction if it would be impracticable or unlawful to do so. Impracticability is addressed in the list at paragraph 13.50. An entity should consider whether it would be practicable to notify some but not all of the other APP entities to which the entity previously disclosed the personal information. In these circumstances, the entity could discuss with the individual whether there are particular entities that they wish to be notified.

13.52 The term ‘unlawful’ is not defined in the Privacy Act. The core meaning is activity that is criminal, illegal or prohibited or proscribed by law, and can include unlawful discrimination or harassment, but does not include breach of a contract. An example of when it would be unlawful to notify another APP entity is when a statutory secrecy provision prevents an agency from taking this step.

13.53 An APP entity that is notified of a correction should, in turn, consider whether to correct the personal information that it holds. As noted at paragraphs 13.16–13.18, an APP entity is required on its own initiative to take reasonable steps to correct incorrect personal information.
Giving written notice where correction is refused

13.54 APP 13.3 provides that if an APP entity refuses to correct personal information as requested by an individual, the entity must give the individual a written notice setting out:

- the reasons for the refusal, except to the extent that it would be unreasonable to do so
- the complaint mechanisms available to the individual, and
- any other matters prescribed by regulations made under the Privacy Act.

13.55 The reasons for refusal should explain, where applicable:

- that the APP entity does not hold the personal information that the individual wishes to correct
- that the entity is satisfied that the personal information it holds is accurate, up-to-date, complete, relevant and not misleading having regard to the purposes for which it is held, or
- that the steps necessary to correct the personal information as requested are not reasonable in the circumstances.

13.56 An APP entity is not required to provide its reasons for refusing to correct personal information to the extent that it would be unreasonable to do so. This course should be adopted only in justifiable circumstances. An example would be where providing reasons would prejudice an investigation of unlawful activity, or prejudice enforcement action by an enforcement body.

13.57 The description of the complaint mechanisms available to an individual should explain the internal and external complaint options, and the steps that should be followed. In particular, the individual should be advised that:

- a complaint should first be made in writing to the APP entity (s 40(1A))
- the entity should be given a reasonable time (usually 30 days) to respond
- a complaint may then be taken to a recognised external dispute resolution scheme of which the entity is a member (if any), and
- lastly, that a complaint may be made to the Information Commissioner (s 36).

13.58 Other information can also be included in the notice advising an individual that a request to correct personal information has been refused. The individual should be advised of the right under APP 13.4 to request the APP entity to associate a statement with the personal information (see paragraphs 13.59–13.62). An agency could also advise an individual of the parallel right under the FOI Act to apply for a record to be amended or annotated, and of the right to Information Commissioner review of an adverse decision under that Act (see paragraphs 13.25–13.29).

Taking reasonable steps to associate a statement

13.59 APP 13.4 provides that if an APP entity refuses to correct personal information as requested by an individual, the individual can request the entity to associate a statement
that the individual believes the personal information to be inaccurate, out-of-date, incomplete, irrelevant or misleading. Implicit in this requirement is that the entity should notify the individual of the right to request that a statement be associated, for example, in the written notice where correction is refused (see paragraphs 13.54–13.58).

13.60 The APP entity must take reasonable steps to associate the statement in a way that will make it apparent to users of the personal information. For example, a statement may be attached physically to a paper record, or by an electronic link to a digital record of personal information. The statement should be associated with all records containing personal information claimed to be incorrect.

13.61 The content and length of any statement will depend on the circumstances, but it is not intended that the statement be unreasonably lengthy. A longer statement may be appropriate in some instances, such as where there is a large volume of personal information that the APP entity has refused to correct. If it is not practicable to attach an extensive statement to the personal information or otherwise create a link to the statement, a note could be included on, or attached to, the personal information referring to the statement and explaining where it can be found. Where it is not reasonable for the entity to associate an extensive statement to the personal information, reasonable steps would generally include giving the individual an opportunity to revise the statement.

13.62 The reasonable steps for an APP entity will depend upon considerations that include:

- the information management practices of the entity, including whether the personal information is stored in hard copy or electronic form (see paragraph 13.59)
- whether content in a statement may be irrelevant, defamatory, offensive, abusive or breach another individual’s privacy — it may be unreasonable to associate a statement containing that content, however the individual should be given the option of revising the statement
- the practicability, including time and cost involved. However, an entity is not excused from associating a statement by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances.

**Timeframe for responding to a request for correction under APP 13**

13.63 APP 13.5 provides that an agency must respond to a request to correct a record or to associate a statement within 30 calendar days. The 30 day time period commences on the day after the day the agency receives the request. An organisation must respond within a reasonable period after the request is made. As a general guide, a reasonable period should not exceed 30 calendar days.

13.64 The APP entity must respond by correcting the personal information as requested by the individual, or by notifying the individual of its refusal to correct it.

---

11 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy) Bill 2012, p 88.
Access charges under APP 13

13.65 An APP entity cannot impose any charge upon an individual for correcting personal information under APP 13. This includes:

- a charge for the making of the request to correct personal information
- a charge for making a correction or for associating a statement with the personal information (APP 13.5(b)).