



Australian Privacy Principles

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;
 - (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
 - (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
 - (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
 - (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;
- (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:
- (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
 - (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
 - (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.

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
 - (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.

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).

Definitions

1 Definition of personal information

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.

2 Definition of sensitive information

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
- e) biometric verification or biometric identification; or
- f) biometric templates.

Permitted general situations

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

Permitted general situations			
Item	Column 1 Kind of entity	Column 2 Item applies to	Column 3 Condition(s)
1	APP entity	(a) personal information; or (b) a government related identifier.	(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.
2	APP entity	(a) personal information; or (b) a government related identifier.	(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.
3	APP entity	Personal information	(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

Permitted general situations			
Item	Column 1 Kind of entity	Column 2 Item applies to	Column 3 Condition(s)
			complies with the rules made under subsection (2).
4	APP entity	Personal information	The collection, use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim.
5	APP entity	Personal information	The collection, use or disclosure is reasonably necessary for the purposes of a confidential alternative dispute resolution process.
6	Agency	Personal information	The entity reasonably believes that the collection, use or disclosure is necessary for the entity's diplomatic or consular functions or activities.
7	Defence Force	Personal information	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.

- (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.

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;
 - (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:
 - (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.



Our people

Frank Higginson, Director

e: frank.higginson@hyneslegal.com.au

p: +61 (7) 3135 0588

Frank's focus has been purely on property law with a specialisation in strata matters including management rights, body corporate law and property projects.

Frank is one of only four panel lawyers for ARAMA (the peak management rights body). He is also actively involved with Strata Community Australia (Queensland) (SCA Qld). He is regularly asked to present to both management rights and body corporate industry groups on the issues facing their respective industries.

Frank is a member of the Legislation Committee for the SCA (Qld).

Qualifications

- Bachelor of Laws, Queensland University of Technology
- Admitted as a solicitor in the Supreme Courts of Queensland, New South Wales, England & Wales and the High Court of Australia

Areas of practice

- Body corporate law
- Management rights
- Property projects

Recent Projects

- Acting in the purchase of some of the biggest management rights businesses in Australia, including notable buildings such as:
 - M on Mary (existing corporate – 367 lots);
 - Hamilton Harbour 1 and 2 (off the plan permanent – 475 lots);
 - Chelsea Bowen Hills (off the plan permanent – 195 lots);
 - Madison Heights (off the plan permanent – 303 lots);
 - Turtle Beach 1 and 2 (existing holiday – 295 lots);
 - Mosaic (off the plan permanent and off the plan hotel – 212 lots and 41 rooms respectively);
 - Ocean Plaza and Points North (existing holiday – 300 + lots); and
 - Varsity Apartments (existing student – 128 lots).

These matters contained issues such as mixed use commercial and residential issues, volumetric titling, GST and going concern issues, NRAS and negotiation of claw-back arrangements along with all other usual due diligence issues.

- Preparing partnership agreements for many buildings (some mentioned above) with from two to up to 15 partners.
- Acting and managing upwards of 30 individual management rights transactions at any given time. These include a range of off-the-plan and completed projects as well as existing permanent, corporate let and holiday let complexes. Our team acts for several major unlisted industry groups that have portfolios of more than ten complexes each.
- Acting for receivers appointed by secured financiers to distressed management rights assets in relation the recovery of the value of the asset.

Professional Memberships

- Australian Resident Accommodation Managers' Association
- Strata Community Association (Queensland)
- Director of Gold Coast Titans Community Foundation Ltd
- Queensland Law Society