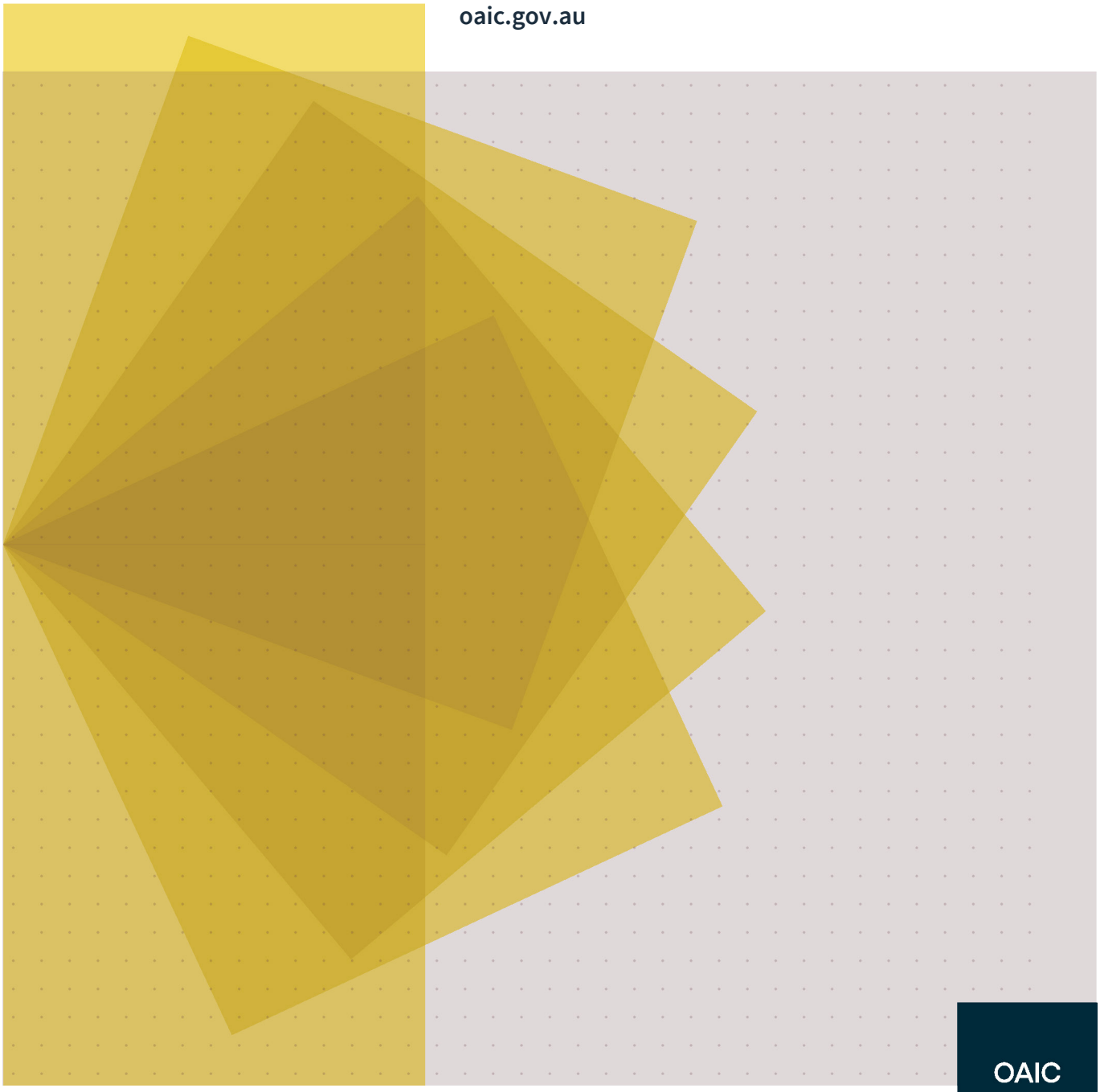
Australian Government

Office of the Australian Information Commissioner

The Australian Privacy Principles

From Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*

oaic.gov.au



OAIC

January 2014

The Australian Privacy Principles (APPs) replaced the National Privacy Principles and Information Privacy Principles on 12 March 2014.

This is the text of the 13 APPs from Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, which amends the *Privacy Act 1988*. For the latest versions of these Acts visit the Federal Register of Legislation.

Contents

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)

Privacy Policy

Rupin Network Pty Ltd ('the Company') and its offices, branches and related companies ("We" or"our" or "us") are committed to ensuring that when handling your personal information, including how your personal information is captured, collected, used, disclosed and stored, we do so in accordance with the Australian Privacy Principles under the Privacy Act 1988

Rupin Network Pty Ltd Privacy Policy

1. Introduction

We manage personal information in accordance with the *Privacy Act 1988* and *Australian Privacy Principles*.

You can request a copy of our full policy, or just read the parts that interest you. We only collect information that is reasonably necessary for the proper performance of our activities or functions.

We may decline to collect unsolicited personal information from or about you and take steps to purge it from our systems.

We manage personal information according to our usual information flow. There may sometimes be departures from our usual information flow.

By following the links in this document, you will be able to find out how we manage your personal information as an APP Entity under the Australian Privacy Principles (APPs).

You will also be able to find out about the information flows associated with that information.

APP Entity

Rupin Network Pty Ltd manages personal information, as an APP Entity, under the AustralianPrivacy Principles (APPs) it might become necessary for us to collect and manage personal information.

Information Flow

When we collect your personal information:

- we check that it is reasonably necessary for our **functions or activities.**
- we check that it is current, complete and accurate. This will sometimes mean that we have to cross check the information that we collect from you with third parties;
- we record and hold your information in our **Information Record System**
- we retrieve your information when we need to use or disclose it for our **functions and activities.** At that time, we check that it is current, complete, accurateand relevant. This will sometimes mean that we have to cross-check the information thatwe collect from

you with third parties once again - especially if some time has passed since we last checked.

- subject to some exceptions and conditions, we permit you to access your personal information in accordance with APP:12.

- we **correct** your personal information in accordance with APP:13.

- we destroy or de-identify your personal information when it is no longer needed for any **purpose** for which it may be used or disclosed provided that it is lawful for us to do so. We do not destroy or de-identify information that is contained in a Commonwealth Record

2. Kinds of information that we collect and hold

Personal information that we collect and hold is information that is reasonably necessary for the proper performance of our **functions and activities** as an On-hire firm and is likely to differ depending on whether you are:

- a **Client**;
- a **Referee**.

For Clients

The type of information that we typically collect and hold about Clients is information that is necessary to help us manage the presentation and delivery of our services and includes:

- roles, reporting lines, inter-personal communication, and cultural fit requirements within your organisation;
- business, social, or personal interests about which we may be able to provide news and information;
- celebration milestones and dates, preferred social media contact channels, etc that you choose to share with us.

For Referees

The type of information that we typically collect and hold about Referees is information that is necessary to help to make determinations about the suitability of one of our Work seekersfor particular jobs or particular types of work and includes:

- your name;
- your relationship with and knowledge and opinions of our Candidate as relevant to the reference we are seeking;
- other background and contextual information as relevant to the reference we are seeking.
- your contact details for follow up (if necessary);
- confirmation of your identity and authority to provide a reference (if necessary).

3. Purposes

The purposes for which we collect, hold, use and disclose your personal information are likely to differ depending on whether you are:

- a **Client**;
- a **Referee**.

For Clients

Personal information that we collect, hold, use and disclose about Clients is typically used for:

- client and business relationship management;
- recruitment functions;
- marketing services to you;
- statistical purposes and statutory compliance requirements;

For Referees

Personal information that we collect, hold, use and disclose about Referees is typically used:

- to confirm identity and authority to provide references;
- for Workseeker suitability assessment;
- for recruitment functions;

4. How your personal information is collected

The means by which we will generally collect your personal information are likely to differ depending on whether you are:

- a **Client**;
- a **Referee**.

We sometimes collect information from third parties and publicly available sources when it is necessary for a specific purpose such as checking information that you have given us or where you have consented or would reasonably expect us to collect your personalinformation in this way.
Sometimes the technology that is used to support communications between us will provide personal information to us.

For Clients

Personal information about you may be collected:

- when you provide it to us for business or business related social purposes;

We may also collect personal information about you from a range of publicly available sources including newspapers, journals, directories, the Internet and social media sites. When we collect personal information about you from publicly available sources for inclusion in our records we will manage the information in accordance with the APPs and our Privacy Policy.

For Referees

Personal information about you may be collected when you provide it to us.
We may also collect personal information about you from a range of publicly available sources including newspapers, journals, directories, the Internet and social media sites. When we collect personal information about you from publicly available sources for inclusion in our records we will manage the information in accordance with the APPs and our Privacy Policy.

Electronic Transactions

Sometimes, we collect personal information that individuals choose to give us via online forms or by email, for example when individuals:

- ask to be on an email list such as a job notification list;
- register as a site user to access facilities on our site such as a job notification board;
- make a written online enquiry or email us through our website;
- submit a resume by email or through our website;
- use web-based application and placement management apps to submit identification documents, receive job offers, undertake inductions, or upload time sheets etc.

Some apps might invite you to use your social media log-in details (e.g.; Facebook or Google log-in user names and passwords).

It is important that you understand that there are risks associated with use of the Internet and you should take all appropriate steps to protect your personal information. It might help you to look at the OAIC's resource on Social Media & Online Privacy.

You can contact us by land line telephone or post if you have concerns about making contact via the Internet.

5. How your personal information is held

Personal information is held in our **Information Record System** until it is no longer needed for any purpose for which it may be used or disclosed at which time it will be de-identified or destroyed provided that it is lawful for us to do so.

Our Information Record System

Information access to our information record system is confined to a hierarchy-based delegation of control which is managed by the Privacy Coordinator.

Information can be stored in the following various ways:

- Hard copy
- Electronic format – portable and electronic devices
- Cloud Storage

Information Security

Rupin Network Pty Ltd takes reasonable steps to keep personal information secure, accurate andup to date. The Internet is not always a secure method of transmitting information.
Accordingly, while we seek to protect your personal information by implementing digital security systems in various parts of our website, Rupin Network Pty Ltd cannot accept responsibility for the security of information you send to or receive from us over the Internet or for any unauthorised access or use of that information.
Where we have links to websites outside Rupin Network Pty Ltd, we cannot ensure that your privacy will be protected in accordance with this policy. You should consult these other websites' privacy policies as we have no control over them and are not responsible for anyinformation that is submitted to or collected by these third parties.

Data Breach Notifications & Response

In the event of a data breach, we would respond by measures appropriate to the nature and seriousness of the breach and the size and resources of our organisation taken in accordance with the four steps set out in the OAIC's data breach notification guidance and advice.

6. Disclosures

We may disclose your personal information for any of the **purposes** for which it is primarily held or for a lawful **related purpose**.

We may disclose your personal information where we are under a legal duty to do so.
Disclosure will usually be:

- internally and to our related entities
- to our Clients
- to Referees for suitability and screening purposes.
- to our contracted service providers, insurers, professional advisors and others with a proper interest in receiving your personal information for a lawful related purpose.

Related Purpose Disclosures

We outsource a number of services to contracted service suppliers (CSPs) from time to time. Our CSPs may see some of your personal information. Typically, our CSPs would include:

- Software solutions providers;
- I.T. contractors, database designers and Internet service suppliers;
- Legal and other professional advisors;
- Insurance brokers, loss assessors and underwriters;
- Background checking and screening agents;

We take reasonable steps to ensure that terms of service with our CSPs recognise that we are bound by obligations to protect the privacy of your personal information and that they will not do anything that would cause us to breach those obligations.

7. Access & Correction

Subject to some exceptions set out in privacy law, you can gain access to your personal information that we hold.

Important exceptions include:

- Evaluative opinion material obtained confidentially in the course of our performing reference checks; and access that would impact on the privacy rights of other people.

In many cases evaluative material contained in references that we obtain will be collected under obligations of confidentiality that the person who gave us that information is entitled to expect will be observed. We do refuse access if it would breach confidentiality.

For more information about access to your information see our **Access Policy**.

For more information about applying to correct your information see our **Correction Policy**.

Access Policy

If you wish to obtain access to your personal information you should contact our Privacy Co-ordinator. You will need to be in a position to verify your identity.

Consistently with guidance and advice provided by the OAIC, we may impose a charge (provided it is not excessive) for retrieving and providing access to your personal information. Any such charge would be calculated having regard to:

- our staff costs in searching for, locating and retrieving the requested personal information, and deciding which personal information to provide to you;
- our staff costs in reproducing and sending the personal information;
- the costs of postage or materials involved in giving access

- the costs associated with using an intermediary – e.g., where access might be granted indirectly or to paraphrased information.

In determining the amount to charge, we would consider:

- our relationship with you;
- any known financial hardship factors;
- any known adverse consequences for you if you do not get access to the personal information.

Correction Policy

If you find that personal information that we hold about you is inaccurate, out of date, incomplete, irrelevant or misleading, you can ask us to correct it by contacting us.

We will take such steps 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.

If we have disclosed personal information about you that is inaccurate, out of date, incomplete, irrelevant or misleading, you can ask us to notify the third parties to whom we made the disclosure and we will take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

8. Complaints

At Rupin Network Pty Ltd we aim to acknowledge receipt as soon as possible and commit to resolve all complaints no later than 30 days. However, there may be instances where this isnot possible due to the contents of the complaint. In such circumstances, we will respond toyour complaint in a reasonable and practical time. You may wish to contact the Australian Information Commissioner (OAIC) if you are not satisfied with our response to your complaint.

Complaints procedure

If you are making a complaint about our handling of your personal information, it should be made to us in writing, and sent to info@rupin.network

You can also make complaints to the Office of the Australian Information Commissioner through the Commission's website.