Australian Privacy Principles — a summary for APP entities

from 12 March 2014

Australian Government
Office of the
Australian Information Commissioner

APP 1 — Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 — Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 — Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 — Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

APP 5 — Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 — Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 — Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 — Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 — Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP 10 — Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 — Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 — Access to personal information

Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 — Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

www.oaic.gov.au

For private sector organisations, Australian Government and Norfolk Island agencies covered by the *Privacy Act 1988*

Checklist for access under Privacy Act (APP 12)

	Grounds for refusal under APP 12	Example	Action
1.	Giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety	Reasonable grounds to believe disclosure of information may cause that person significant distress or lead to self-harm or harm to another individual	Refer to InfoGov Team
2.	Giving access would have an unreasonable impact on the privacy of other individuals	Record of personal information that an individual has requested contains personal information of another individual	Redact personal information of other individuals Where not possible, refer to InfoGov Team
3.	Request is frivolous or vexatious	Repeated requests for same information or abusive language	Refer to InfoGov Team
4.	Legal proceedings between the individual and the organisation are underway or anticipated, and the information would not be accessible by the process of discovery, subpoena, notice to produce, or any other similar processes in those proceedings	A legal proceeding is anticipated if there is a real prospect of proceedings being commenced, as distinct from a mere possibility.	Refer to InfoGov Team Refer to relevant team within Legal Compliance and Enforcement working on anticipated or actual proceedings.
5.	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.	A claim brought by the individual for compensation	Refer to InfoGov Team Refer to Legal Group for advice
6.	Giving access would be unlawful	Giving access would be a breach of legal professional privilege, a breach of confidence or a breach of copyright	Refer to Info Gov Team Refer to Legal Group for advice

	Grounds for refusal under APP 12	Example	Action
7.	Denying access is required or authorised by law or a court/tribunal order	Court order preventing release of the information	Refer to InfoGov Team Refer to Legal Group for advice
8.	Giving access would likely prejudice the taking of appropriate action in relation to suspected unlawful activity or serious misconduct	The suspected unlawful activity or serious misconduct must relate to functions or activities under the FW Act	Refer to InfoGov Team Refer to Legal Group for advice
9.	Giving access would be likely to prejudice an enforcement related activity conducted by, or on behalf of, an enforcement body	Access would reveal the existence of a criminal investigation or interfere with preparation for court proceedings	Refer to InfoGov Team Refer to Legal Group for advice
10.	Giving access would reveal evaluation information in connection with a commercially sensitive decision-making process	A score card rating system and results for a procurement activity	Redact evaluation information Where not possible, refer to InfoGov Team who may seek legal advice from Legal Group.

Privacy Awareness Week

Privacy Awareness Week (PAW) is an annual event to promote and raise awareness of the importance of **protecting personal information.**

It is led by the Office of the Australian Information Commissioner (OAIC) in partnership with state and territory privacy regulators and Asia Pacific Privacy Authorities members.

Power up your privacy

For this Privacy Awareness Week, the call is to 'power up your privacy'. This sits under the overarching theme of:

Privacy and technology: Improving transparency, accountability and security.

Now is the ideal time to 'power up' our existing privacy practices ahead of privacy law reform and changing technological landscape.

The Office of the Fair Work Ombudsman is glad to be supporting Privacy Awareness Week and helping to promote good privacy practices.

Community attitudes to privacy

- 3 in 5 Australians see the protection of their personal information as a major concern in their life (62%).
- Only a third feel in control of their data privacy, and 84% want more control and choice over the collection and use of their personal information.
- 74% feel data breaches are one of the biggest privacy risks they face today.
- 70% say privacy is extremely or very important when choosing a product or service, and another 26% state it is quite important.
- After quality and price, data privacy is the third most important factor when choosing a product or service.

Source: Australian Community Attitudes to Privacy Survey 2023

Privacy and personal information

What is privacy?

Privacy is a fundamental human right that protects our human dignity and underpins other rights such as freedom of association, thought and expression, and freedom from discrimination.

Information privacy is about promoting the protection of information that says:

- who we are
- what we do
- what we believe.

The Privacy Act 1988

The Privacy Act was introduced to promote and protect the privacy of individuals.

It sets out how organisations covered by the Act must handle your personal information, sensitive information, tax file number and credit information.

It gives you a number of rights, such as asking for access to your personal information.

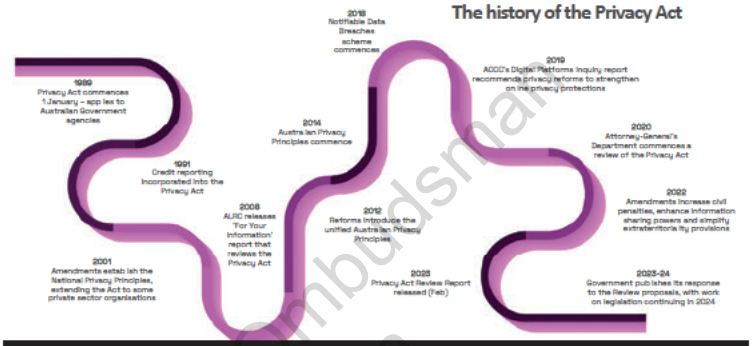
The Australian Government has committed to strengthening the Australian privacy framework with updates to the Privacy Act, making now an ideal time to 'power up' privacy practices and culture in advance of privacy law reform.

Who has responsibilities under the Privacy Act?

- Most Australian Government agencies
- Private sector organisations with an annual turnover over $3 million
- All private health service providers
- Credit providers and reporting agencies
- Tax file number recipients
- Small businesses that meet certain criteria, for example, who trade in personal information.

Note: Various state and territory privacy laws apply to state & territory govt agencies.

The history of the Privacy Act



Individuals' rights under the Privacy Act

- Know why your personal information is being collected, how it will be used and who it will be disclosed to
- Not identify yourself or use a pseudonym
- Access your personal information
- Not receive unwanted direct marketing
- Correct your personal information
- Make a complaint.

What is personal information?

- Your name, signature, contact details and date of birth
- Your medical records, bank account details and credit history
- Your photo, fingerprint, voice print, the iris of your eye
- Your political opinions and religious beliefs, and a wide range of other information.

Organisations' responsibilities under the Privacy Act

- Manage personal information openly and transparently
- Only collect personal information you really need
- Let customers know when you collect their personal information and why
- Only use or disclose personal information in certain circumstances (usually this means only for the purpose for which you collected it)
- Take reasonable steps to ensure personal information is accurate, up to date, complete and relevant
- Protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure
- Destroy or de-identify personal information that you no longer need
- Give your customers access to their personal information if they request it

Australian Privacy Principles

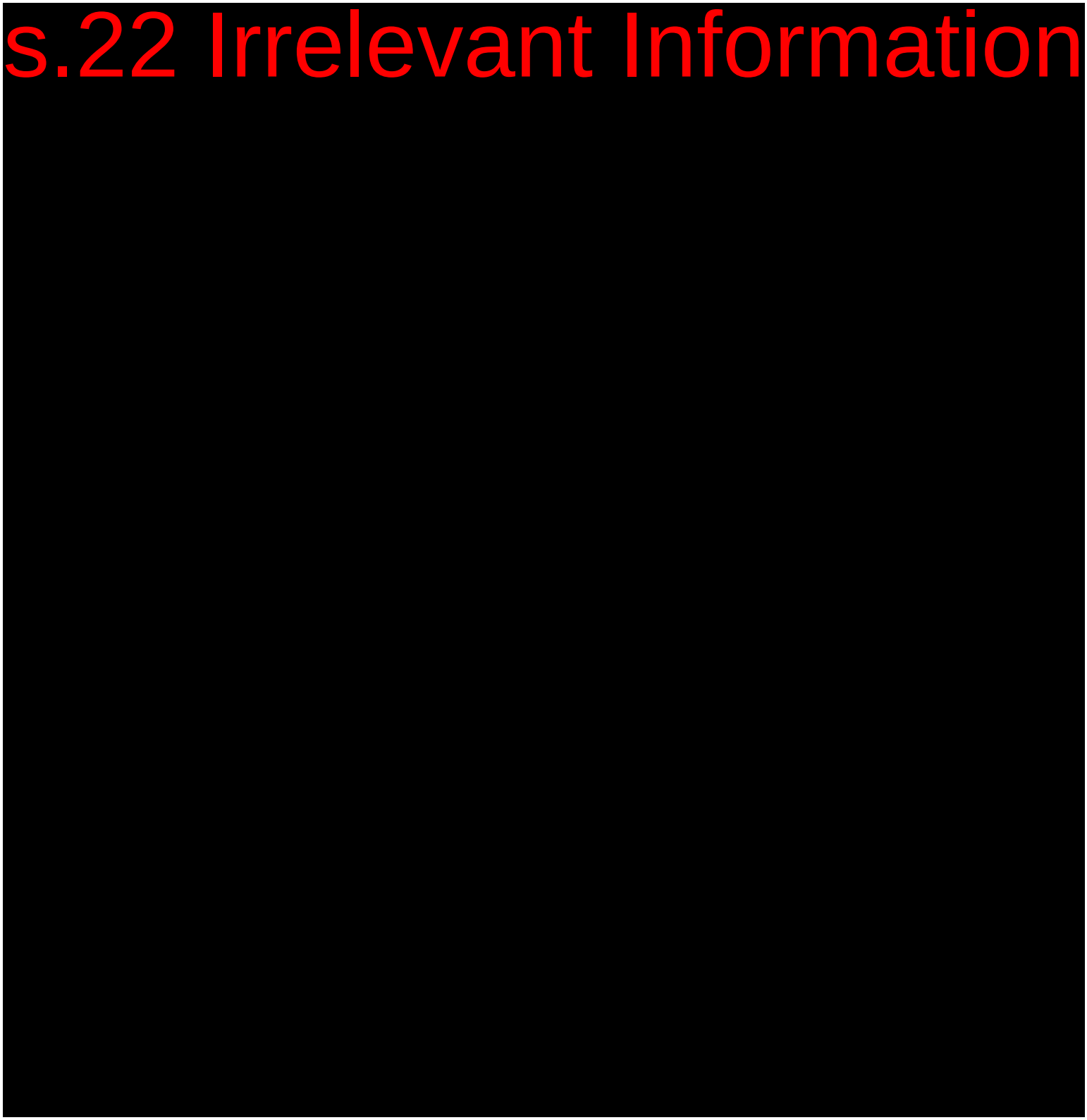
1. Open and transparent management of personal information
2. Anonymity and pseudonymity
3. Collection of solicited personal information
4. Dealing with unsolicited personal information
5. Notification of the collection of personal information
6. Use or disclosure of personal information
7. Direct marketing
8. Cross-border disclosure
9. Government-related identifiers
10. Quality of personal information
11. Security of personal information
12. Access to personal information
13. Correction of personal information

[redacted]

[redacted]

s.22 Irrelevant Information

[redacted]


s.22 Irrelevant Information

s.22 Irrelevant Information

s.22 Irrelevant Information

s.22 Irrelevant Information

Australian Government
Office of the Australian Information Commissioner

Privacy fact sheet 17

Australian Privacy Principles

January 2014

From 12 March 2014, the Australian Privacy Principles (APPs) will replace the National Privacy Principles and Information Privacy Principles and will apply to organisations, and Australian Government (and Norfolk Island Government) agencies.

This privacy fact sheet provides 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 ComLaw website: www.comlaw.gov.au.

Part 1—Consideration of personal information privacy

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.

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

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.

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.

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

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.

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.

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.

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

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.

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

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.

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).

The information provided in this fact sheet is of a general nature. It is not a substitute for legal advice.

For further information

telephone: 1300 363 992
email: enquiries@oaic.gov.au
write: GPO Box 5218, Sydney NSW 2001
GPO Box 2999, Canberra ACT 2601
or visit our website at **www.oaic.gov.au**

Australian Government Fair Work OMBUDSMAN

Privacy policy summary

This document summarises how we handle personal information. You can find out more by reading our full Privacy policy.

We collect, hold, use and disclose personal information when it's needed for, or related to, our legislative functions or activities.

Collecting your personal information

We collect personal information from:

- you directly
- third parties
- publicly available sources.

For example, we collect personal information when giving information to the public, handling requests for assistance, conducting education activities, investigating suspected breaches of workplace laws and taking court action.

We also collect personal information through our website and social networking services such as Facebook and Twitter. We use this information to seek feedback from the community and improve our online products and services.

Using and disclosing personal information

If you request assistance from us, we may use the personal information you provide (such as your contact details or pay slips) to keep you up to date about your matter and check whether your entitlements have been met.

To ensure fairness, we may give personal information to another party in a dispute resolution process. For example, we may give information about an employee who has requested our assistance to their employer as part of a mediation process.

We're also authorised to give information to other Commonwealth, State or Territory bodies where it's likely to help with the administration or enforcement of a law. For example, we may give information to the Department of Immigration and Border Protection if we suspect an employer has breached the conditions of a skilled migration visa.

Accessing or correcting your personal information

If you ask, in most cases we will give you access to the personal information that we have about you. We will also take reasonable steps to correct your personal information if we agree that it's incorrect.

We try to make these processes as simple as possible.

How to make a complaint

You can complain to us about the handling of your personal information by emailing us at yourfeedback@fwo.gov.au.

Contact us

For questions about your privacy, you can contact our Privacy Officer at:

Privacy Officer
Customer Feedback & Information Access
Fair Work Ombudsman
GPO Box 9887
Sydney NSW 2001
privacy@fwo.gov.au

Further information

The Office of the Australian Information Commissioner's website contains further information on privacy. Please visit www.oaic.gov.au

Australian Government Fair Work OMBUDSMAN

Privacy Policy

Version 1.9

May 2024

Version	Date	Author	Revision Comments
V0.1	March 2015	Sally Dennington	Initial Draft
V1.0	November 2016	Sally Dennington	Approved first version of the document
V1.1	May 2020	Nicola Forbes	Additions related to surveys, health information and data matching
V1.2	October 2020	Nicola Forbes	Additions related to collection of protected information from Australian Taxation Office in relation to JobKeeper and additional see reference under Our Regulatory Activities
V1.3	June 2021	Nicola Forbes	Additions related to the collection of COVID-19 vaccination status information
V1.4	July 2021	Nicola Forbes	Additions related to Small Business Employer Advisory Service
V1.5	September 2022	Nicola Forbes	Update to new template
V1.6	June 2023	Nicola Forbes	Amendments required due to introduction of SJBP Act, updates to sections related to social media and website notices, clarification of FWO's use and disclosure of sensitive information and expanded section on how long personal information is retained by the FWO.
V1.7	November 2023	Nicola Forbes	Amendments required to reflect that the FWO will need to collect Tax File Numbers (TFNs) to comply with its tax withholding and reporting obligations when paying unclaimed moneys to claimants and minor amendment from FWO to FWO to reflect administrative change.

V1.8	February 2024	Nicola Forbes	Amendment to clarify when individual may deal with us anonymously and to reflect collection of biometric templates from FWO employees.
V1.9	May 2024	Nicola Forbes	Remove reference to collection of information from ATO as part of JobKeeper scheme. JobKeeper scheme ended on 28 March 2021.

Table of Contents

About this policy

The Office of the Fair Work Ombudsman (FWO) is an independent statutory office that supports harmonious, productive, cooperative and compliant workplaces and ensures compliance with Australian workplace laws, including the *Fair Work Act 2009.* The FWO consists of the Fair Work Ombudsman, the staff of the Office of the FWO and Inspectors appointed under the Fair Work Act.

In 2023, the Australian Building and Construction Commission (ABCC) was abolished. Personal and sensitive information originally collected by the ABCC was transferred to the Fair Work Ombudsman due to its resumed building and construction compliance functions and will be handled in accordance with this privacy policy, the Privacy Act 1988 (Privacy Act), Fair Work Legislation Amendment (Secure Jobs Better Pay) Act 2022, Fair Work Act 2009, and any other relevant legislation such as the Freedom of Information Act 1982.

We are bound by the Privacy Act when collecting, holding, using and disclosing your personal information. The Privacy Act contains 13 Australian Privacy Principles which outline government agencies' responsibilities and individuals' rights designed to protect privacy. This policy applies to our treatment of all personal information, whether it relates to a customer, an employee, or another person.
This policy describes how we comply with the Privacy Act and explains:

- the types of personal information we collect
- how this information is used
- when it can be disclosed
- who it can be disclosed to.

We regularly review this policy to ensure it contains up to date information about how we manage your personal information.

Overview

We collect, hold, use and disclose personal information to carry out our functions and activities, including when we:

- investigate a breach of the Fair Work Act 2009
- advise, assist, educate and inquire into workplace matters
- take action in Courts or Tribunals to address unlawful conduct
- monitor compliance with visa conditions
- respond to access to information requests

- communicate with the public, stakeholders and the media
- publish information on our website
- conduct or facilitate surveys (either directly or through a third-party provider)
- recruit and hire employees.

Dealing with us anonymously

When you deal with us you have the right to be anonymous and the right to use a pseudonym. You can report an issue anonymously to us through our website, in English or another language.

If you wish to ask us a question or request assistance, we will collect some personal information from you. You may be able to limit the types and amount of personal information you provide. You can discuss this with us.

Collecting your personal information

We collect personal information when it is reasonably necessary for, or directly related to, our functions or activities under the Fair Work Act, the *Public Service Act 1999,* the *Paid Parental Leave Act 2010* and other relevant legislation.

The types of personal information we collect include:

- names, addresses, dates of birth, telephone numbers and email addresses
- letters of offer and employment contracts
- work rosters, sign-in sheets, pay slips and bank statements
- statements taken by the Fair Work Ombudsman which identify individuals
- health information, including COVID-19 vaccination status information

We only collect personal information using lawful and fair means.

Collecting personal information directly from you

The main way we collect personal information about you is when you give it to us, including when:

- you contact us by phone, email or through our website
- you request assistance from us
- you register for or use MyAccount
- you participate in a survey conducted or facilitated by us or through a third-party provider

- we conduct an investigation.

Collecting your personal information from others

We may collect personal information about you from other people or publicly available records. We do this when:

- it is unreasonable or impractical to collect the information from you
- you consent to it or
- we are required or authorised to do so by law.

For example, we may use internet search engines, white pages, internet articles and social media to locate people who are owed money where other methods of locating them have failed.

Fair Work Inspectors are also authorised under the Fair Work Act to require employers and other people to produce records or documents (for example, pay slips and work rosters) to check whether workforce obligations are being met and which may contain your personal information.

There are some circumstances where it may not be reasonable or possible to tell you that we are collecting your personal information from a third party. This may include when we collect information about a large number of individuals in similar circumstances, such as when we collect information from:

- government agencies; or
- listed public entities such as companies and trusts.

We may also collect your personal information when we are conducting a targeted campaign or an audit of a particular industry to assist us to decide which employment arrangements warrant scrutiny.

We only collect health information, including COVID-19 vaccination status information, with your consent.

Sensitive information

Sometimes we may need to collect sensitive information about you with your consent, including from your employer. This may include information about your health, sexual orientation or practices, your membership of a professional or trade association or trade union, or your criminal record.

We may also collect sensitive information without your consent when we reasonably believe that the collection of the information is reasonably necessary for, or related to, one or more of our functions or activities (for example, investigating breaches of the Fair Work Act or taking action in a Court or Tribunal).

Visiting our website

The type of personal information we collect will depend on how you use our website.

Browsing our website

When you visit fairwork.gov.au and our related sites and services, we collect information from your browser via Google Analytics, a web analysis service provided by Google. Google Analytics uses cookies to help analyse how users use our website. The information generated by the cookie about your use of our website will be transmitted to and stored by Google on servers overseas. You can read more about what information Google collects and what they do with it, in the Google Privacy Policy.

We do not collect information from Google Analytics that would identify you as an individual (for example your name or email). We capture web browsing information to understand how people engage with the information provided on our website and to help us improve our online services. We use high level data for reporting purposes – including total website visits and page views.

The types of information we collect include:

- your server address
- your operating system, for example, Windows, Mac
- your top-level domain name, for example, .com, .gov, .au, .uk
- your approximate city/location
- the date and time of your visit to our site
- the pages visited and how you engaged with them
- the documents you downloaded
- the previous site you visited
- how you found our website
- the type of device and browser used, for example, Chrome, Microsoft Edge
- the language selected for translation.

By using our website, you consent to Google processing information about you in the manner and for the purposes set out above. To opt out and prevent your information from being collected by Google Analytics, you can download the Google Analytics opt-out add-on.

Cookies

We use cookies to track your website browsing behaviour. A cookie is a small text file a server puts on your hard drive. It shows us if you have visited our website more than once.

Your browser shares cookies with our server anonymously, so we won't know your name or email. This lets us see the patterns of how you use our website. Cookies 'remember' your browser between page visits and identify your browser when you return to the site.

Subscribing to email alerts

We use Swift Digital, an online marketing platform service provider, to send and manage emails for our subscribers.

When you subscribe to our email and media updates:

- we record your email address
- we only use your email address for the reasons you gave it
- we won't add your email address to other mailing lists, unless you ask us to
- you can use a pseudonym if you supply a valid email address.

We do not share personal information collected using Swift Digital with any third parties. For more information about how Swift Digital handles personal information, you can read Swift Digital's Privacy Policy and Terms and Conditions.

Social media

We use our Facebook, Instagram, LinkedIn and Twitter pages to post information on your workplace rights and obligations under Australian workplace laws.

Social media platforms are controlled and operated by third parties and are not government websites or applications. Please be mindful about disclosing personal information on our social media pages, as they are public and any post you make may be visible to others. You can learn more about your privacy when using social media platforms through the following links:

- Facebook
- Instagram
- LinkedIn
- Twitter.

We may collect and use information about you to respond to your social media posts. We may also use your personal information to monitor and evaluate the advice we provide to you. Without this information, we may not be able to assist you or ensure that we are providing consistent and reliable advice.

We use Sprout Social to report on interactions between the Fair Work Ombudsman (FWO) and individuals on our social media pages. For more information about how Sprout Social handles personal information, you can read Sprout Social's Privacy Policy.

Using and disclosing personal and sensitive information

We only use or disclose your personal and sensitive information to perform our statutory functions under the Fair Work Act or to improve our service delivery unless we are required to use or disclose your information in another way by law. For example, if required for a law enforcement purpose.

Our regulatory activities

We usually need to use and disclose your personal or sensitive information when we perform functions or exercise powers under the Fair Work Act, including the conduct of investigations or other compliance activities.

For example, if you request assistance from us, the personal information you provide (such as your pay slips) may be used to check whether your employment entitlements have been met. Other personal information that you provide (such as your contact details) may be used to contact you and keep you up to date with your enquiry.

During a dispute resolution process, a Fair Work Inspector may give personal information relating to one party to the dispute (for example, the employee) to the other party (for example, the employer) for the purpose of resolving the matter and contributing to procedural fairness.

For example, a Fair Work Inspector may provide a statement obtained from you to the other party in a proceeding that potentially contains sensitive information such as details about your health, sexual orientation or practices (where it is relevant to the complaint) for the purpose of resolving a sexual harassment complaint under the Fair Work Act 2009.

We may share your personal information with other regulatory agencies where another agency has regulatory responsibility under their legislation. For example, if we identify issues of misuse or fraud concerning payment or non—payment of taxation we may refer the matter to the Australian Taxation Office.

We may use and disclose your personal information as part of large-scale activities to monitor and review compliance with the Fair Work Act. This may involve the exchange of information with other government agencies. These activities comply with the data matching guidelines issued by the Privacy Commissioner.

For further information see the **Data matching** section on page 10 of this document.

Employee information

We collect personal information from our employees to ensure our employee information is up to date for employment related purposes. We may also collect personal information from others where we are authorised or required to by the *Public Service Act 1999*, the *Public Service Regulations 1999* or other legislation.

This information can include job applications, notes made by selection committees during selection processes, employment contracts, copies of training and academic qualifications, bank account details, medical certificates, or health related information. We may collect biometric templates as part of multi-factor authentication processes. This will only occur with consent.

Referral to law enforcement authorities

We are authorised under the Fair Work Act to give information to other Commonwealth, State or Territory bodies when it is likely to assist with the administration or enforcement of a law. Examples include providing the police with personal and other necessary information if it is needed to assist in a criminal investigation and providing the Australian Taxation Officer with information to assist in an inquiry regarding an entity's compliance with tax laws. Another example is giving information to the Commonwealth Director of Public Prosecutions if we suspect a person has committed fraud against the Commonwealth.

Public health and safety concerns

We may need to urgently disclose personal information to a State or Commonwealth authority for the purpose of virus (e.g. COVID-19) contact tracing or management, in order to prevent the spread of a communicable disease and fulfill our work health and safety obligations. We might also share limited personal information to an infected individual's work colleagues or other contacts, if the disclosure is necessary to lessen or prevent a serious threat to the health or safety of others. Where reasonable, we will obtain the consent of the relevant individual before any such disclosure if made. The disclosures are authorised under public health laws and under the Privacy Act.

Advisers, contractors and outsourcing

Sometimes we engage recognised expert advisers from outside the FWO for assistance and advice. We use external lawyers to provide advice about matters and to represent us in court. The information we provide to our external lawyers often necessarily includes personal information.

We also engage specialised advisers including universities to assist us with research projects.

We use third party providers to manage our contact centre software, interactive voice response service and call recording service. You can ask us to not capture a call recording when you call us or we call you.

If a third party is contracted to carry out some of our functions, such as providing legal or research services, the contractor and its employees are bound by the Privacy Act when dealing with personal information. This would apply where they provided services through their own websites.

We also ensure that the privacy and confidentiality of your personal information is addressed in these contracts.

We disclose personal information to a number of service providers including IT service providers that host our website servers, manage our IT and store our information (including human resources information).

Enquiries, education and improvement

We may also use your personal information to:

- contact you about an enquiry or you have made or information you have provided
- tell you about the assistance or information we can give you
- seek feedback about your dealings with us for business improvement, training and reporting purposes, or
- conduct surveys or research.

When we provide your personal information to third parties for surveys and research, we require them to only use or disclose your personal information for the reasons we have engaged them.

Third parties conducting surveys or research for us must comply with the same legal obligations we follow when it comes to your personal information.

If you don't want your personal information to be used by or disclosed to third parties conducting research or surveys for us, or if you want to inspect, amend, or remove personal information we have about you, email us at privacy@fwo.gov.au, or write to us at:

Privacy Officer
Information Governance
Fair Work Ombudsman
GPO Box 9887
Sydney NSW 2001

Freedom of information requests

We are authorised to disclose information under the *Freedom of Information Act 1982*. This legislation provides any person with the right to obtain documents held by us, other than exempt documents, and the right to ask for information held by us about them to be corrected or annotated if it is incomplete, incorrect, out of date, or misleading.

The information we disclose under this legislation may include your personal information, but we will consult with you where appropriate before such a disclosure if made.

Overseas disclosure of personal information

It is unlikely that we will disclose your personal information to people or organisations located overseas.

If we need to do this (for example, if your employer is located overseas), we will make the overseas disclosure in accordance with the Privacy Act.

Web traffic information is disclosed to Google Analytics when you visit our website. Google stores information across multiple countries. For further information see Google Data Centres and Google Locations.

Information you shouldn't give us

Tax file numbers

Sections 8WA and 8WB of the *Taxation Administration Act 1953* and the Australian Information Commissioner's Privacy (Tax File Number) Rule contain special rules relating to the collection and use of tax file numbers.

You should not provide us with your own tax file number unless:

- you're an employee or contractor engaged by us and we have your consent, or
- you're an individual seeking payment of unclaimed monies under section 559 of the Fair Work Act and we have asked for your TFN for this purpose.

If you're an employer, you should never provide us with the tax file numbers of employees.

If you are not working for us or are not an employee who is seeking payment of unclaimed monies and your tax file number is in the documents you give us (such as your group certificate or payment summary as evidence as amounts paid to you), we cannot record, use, or disclose your tax file number. If a tax file number is inadvertently recorded, we will do our best efforts to ensure it is not used or disclosed unlawfully.

For more information about your rights relating to tax file numbers, visit the Office of the Australian Information Commission's website or the Australian Taxation Office's website.

Covert recordings

Depending on the laws that apply in your state or territory, it can be illegal to make, possess and/or communicate a covert recording without the consent of all the parties recorded.

You should not provide us with any recordings of conversations (including any transcripts or records of the recording) that are made without the knowledge or consent of all the parties to the conversation.

Health information

Do not send us health or medical information that relates to another person unless we request it from you. We can only collect a person's health information, including COVID-19 vaccination status information, with their consent or when we reasonably believe that the collection of information is reasonably necessary for, or related to our functions or activities.

Accessing and correcting your personal or sensitive information

You can ask to access the personal or sensitive information we have about you or ask that we change this information if it is inaccurate, out-of-date, incomplete, irrelevant or misleading.

We may ask you to put your request in writing and give us proof of identification before we release or change your personal information. We will respond to your request within 30 days and there are no fees for requesting access to your personal information.

If we refuse to give you access to or correct your personal information, we will give you written reasons why.

If you want to access or correct your personal information, please contact our **Privacy Officer.** The Privacy Officer's contact details are given below.

Data matching

We do checks to test whether or not employers are complying with the law. These checks include audit and verification programs and computer-based information matching, known as data matching. This allows information from a variety of sources to be brought together, compiled and applied to a range of public policy purposes. Data matching helps us to identify people who are not complying with their obligations under the Fair Work Act.

Our usual data sources include government agencies managing the registration of businesses and company directors. The supply of this data is authorised by law. We match this data with information provided to us through our call centres and website. Data matching in this way can enable us to detect people who are not meeting their obligations under the Fair Work Act, such as paying their employees their full entitlements under a relevant Award or not taking adverse action against an employee for exercising their workplace rights, and so on.

We also undertake large scale activities involving information exchange with other government agencies which are authorised by law. Data-matching projects may be conducted in order to address particular compliance risks or issues or to address trends related to specific industries.

We compare externally sourced data with information that we already hold. If we check information related to you it doesn't mean we think you're not compliant with the Fair Work Act, but if we find discrepancies, we may take follow-up action.

The data is also used to check trends within industries and helps us to focus on future compliance risks.

To better protect your privacy, we comply with voluntary guidelines about data matching issued by the Privacy Commissioner.

The protocols that we follow to protect your information include:

- publishing data-matching protocols that describe our data-matching activities
- advertising these protocols in the Commonwealth gazette
- secure storage of data-matching information
- only giving access only to authorised employees
- regularly reviewing the progress of projects and checking that information is being properly used and protected
- providing the Information Commissioner with protocols for programs involving more than 5,000 individuals.

Storage and security of personal and sensitive information

We use a range of physical and electronic security measures to protect your personal and sensitive information from loss, misuse, interference, unauthorised access, modification or disclosure. We have policies and systems in place aimed at ensuring your personal information will only be accessed by employees or contactors on a need-to-know basis. We may hold and analyse your personal information within an e-Discovery Platform for the purposes of managing investigations and potential litigation.

Disposal of personal and sensitive information

When we receive personal information about you (whether solicited or unsolicited) the information will, in almost all cases, be treated as a Commonwealth record. We are bound by the *Archives Act 1983* to retain Commonwealth records until we can lawfully dispose of them, generally either in accordance with:

- a 'records authority' issued or agreed to by the National Archives – a records authority determines how long we hold information and when we dispose of it
- 'normal administrative practice' – which permits the destruction of information that is duplicated, unimportant or of short-term facilitative value.

Generally speaking, the information we collect is retained for seven years. This includes when we advise, assist, educate and inquire into workplace matters or investigate a breach of the Fair Work Act 2009. We may retain information for longer for example, if an investigation is controversial, of major public interest or sets a legal precedent.

Complaints

You can complain to us about the handling of your personal information by emailing us at privacy@fwo.gov.au.

We will make all attempts to respond to and deal with your complaint quickly and within a reasonable time. If we decide that a complaint should be investigated further, it will usually be handled by a more senior officer than the officer whose actions you are complaining about.

If you are not satisfied with our response, you can complain to the Privacy Commissioner. For more information, visit www.oaic.gov.au or phone 1300 363 992.

If you are not satisfied with our complaint handling process in response to your privacy complaint, you have the option of contacting the Commonwealth Ombudsman.

Contact us

For questions about your privacy, you can contact our Privacy Officer by emailing privacy@fwo.gov.au or writing to:

Privacy Officer

Information Governance

Fair Work Ombudsman

GPO Box 9887

Sydney NSW

s.22 Irrelevant Information

s.22 Irrelevant Information

s.22 Irrelevant Information

Privacy Act 1988 (Cth)

- APP 12:
  An APP entity that holds personal information about an individual must, on request, give that individual access to the information
- Access for personal information
- Some exceptions

11

s.22 Irrelevant Information

s.22 Irrelevant Information

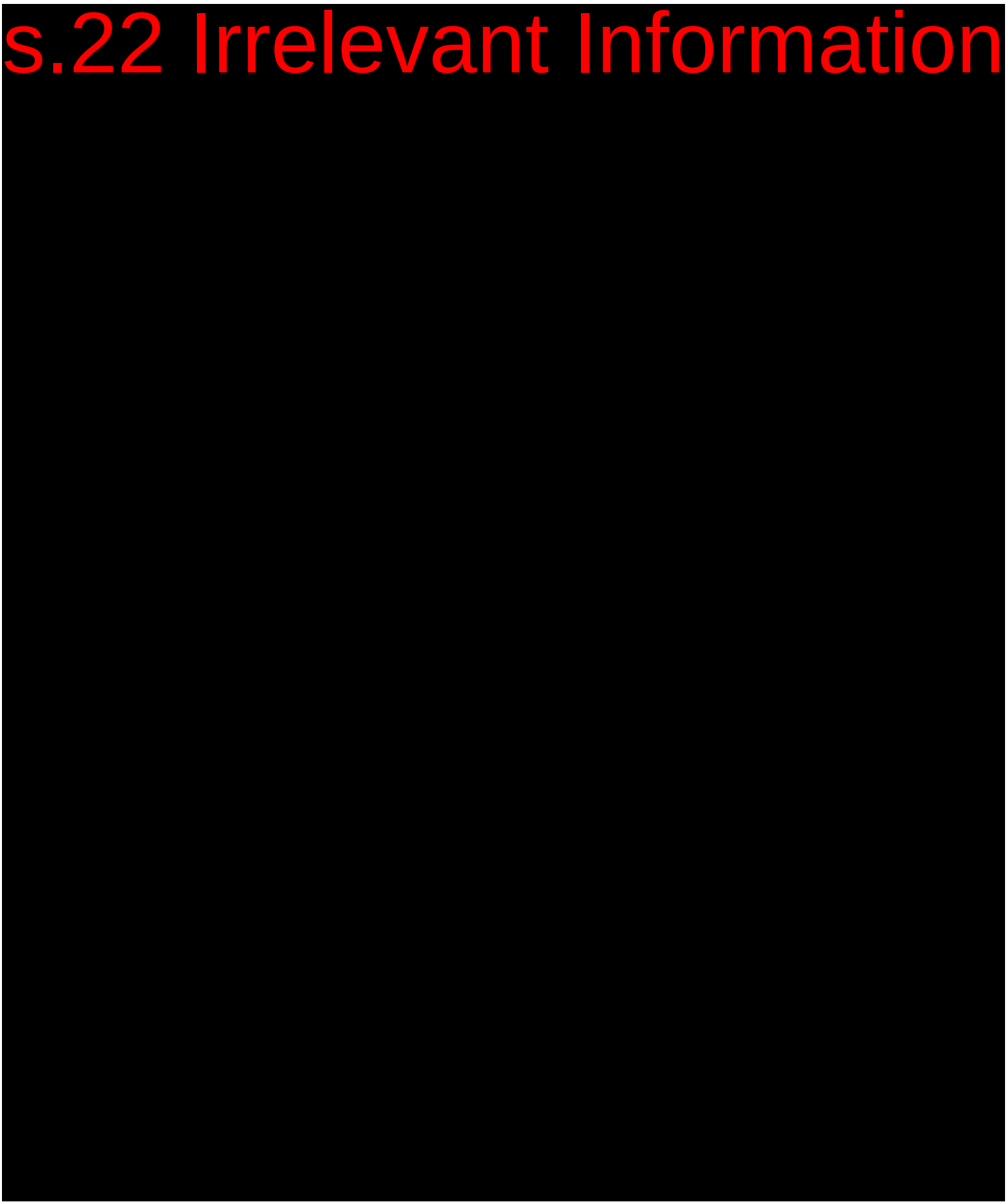
s.22 Irrelevant Informatiors.22 Irrelevant Information

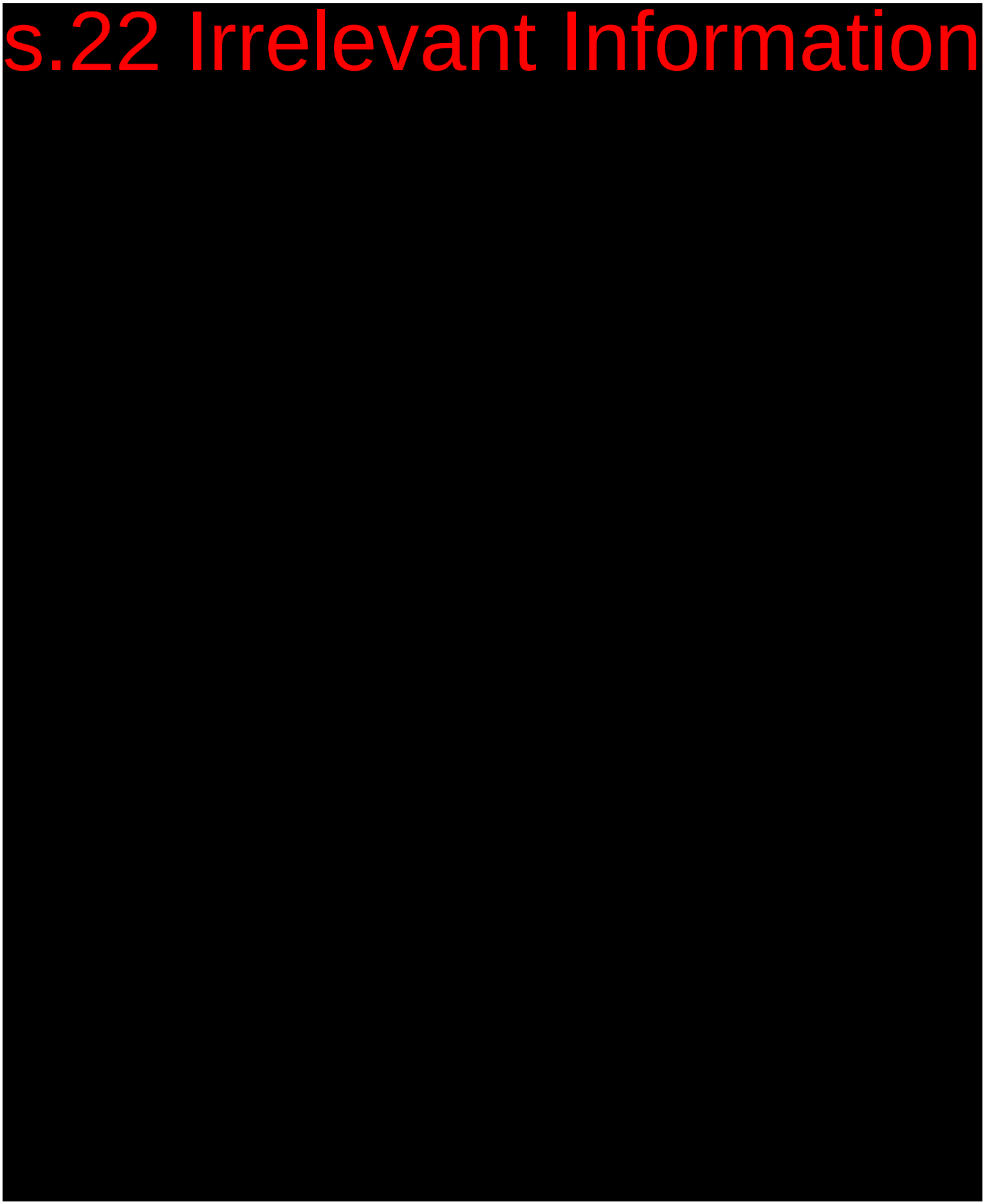
[redacted]

Privacy Act 1988 (Cth)

- APP 12:
  An APP entity that holds personal information about an individual must, on request, give that individual access to the information
- Access for personal information
- Some exceptions

s.22 Irrelevant Information


s.22 Irrelevant Information


s.22 Irrelevant Information

s.22 Irrelevant Information

s.22 Irrelevant Information

Attachment E: Grounds for refusal under Privacy Act (APP 12)

	Grounds for refusal under APP 12	Example	Action
1.	Giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety	Reasonable grounds to believe disclosure of information may cause that person significant distress or lead to self-harm or harm to another individual	Refer to InfoGov Team
2.	Giving access would have an unreasonable impact on the privacy of other individuals	Record of personal information that an individual has requested contains personal information of another individual	Redact personal information of other individuals Where not possible, refer to InfoGov Team
3.	Request is frivolous or vexatious	Repeated requests for same information or abusive language	Refer to InfoGov Team
4.	Legal proceedings between the individual and the organisation are underway or anticipated, and the information would not be accessible by the process of discovery, subpoena, notice to produce, or any other similar processes in those proceedings	A legal proceeding is anticipated if there is a real prospect of proceedings being commenced, as distinct from a mere possibility.	Refer to InfoGov Team Refer to relevant team within Legal Compliance and Enforcement working on anticipated or actual proceedings.
5.	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.	A claim brought by the individual for compensation	Refer to InfoGov Team Refer to Legal Group for advice
6.	Giving access would be unlawful	Giving access would be a breach of legal professional privilege, a breach of confidence or a breach of copyright	Refer to Info Gov Team Refer to Legal Group for advice
7.	Denying access is required or authorised by law or a court/tribunal order	Court order preventing release of the information	Refer to InfoGov Team

	Grounds for refusal under APP 12	Example	Action
			Refer to Legal Group for advice
8.	Giving access would likely prejudice the taking of appropriate action in relation to suspected unlawful activity or serious misconduct	The suspected unlawful activity or serious misconduct must relate to functions or activities under the FW Act	Refer to InfoGov Team Refer to Legal Group for advice
9.	Giving access would be likely to prejudice an enforcement related activity conducted by, or on behalf of, an enforcement body	Access would reveal the existence of a criminal investigation or interfere with preparation for court proceedings	Refer to InfoGov Team Refer to Legal Group for advice
10.	Giving access would reveal evaluation information in connection with a commercially sensitive decision-making process	A score card rating system and results for a procurement activity	Redact evaluation information Where not possible, refer to InfoGov Team who may seek legal advice from Legal Group.