Australian Privacy Principles

Australian Privacy Principles introduced March 2014

The Privacy Act is the national legislation which ensures that organisations (this includes NGOs, businesses and government agencies) protect people’s personal information and are transparent about how they handle this information. It was amended in the Privacy Amendment (Enhancing Privacy Protection) Act 2012 and these changes came into force 12 March 2014.

The main changes were the replacement of the National Privacy Principles (NPPs) by the Australian Privacy Principles (APPs). The Privacy Principles regulate the handling of personal information. There are now 13 APPs and a number of them are significantly different from the previous 10 NPPs:

Part 1 - Consideration of personal information privacy
Australian Privacy Principle 1 - open and transparent management of personal information
Australian Privacy Principle 2 - anonymity and pseudonymity

Part 2 - Collection of personal information
Australian Privacy Principle 3 - collection of solicited personal information
Australian Privacy Principle 4 - dealing with unsolicited personal information
Australian Privacy Principle 5 - notification of the collection of personal information

Part 3 - Dealing with personal information
Australian Privacy Principle 6 - use or disclosure of personal information
Australian Privacy Principle 7 - direct marketing
Australian Privacy Principle 8 - cross-border disclosure of personal information
Australian Privacy Principle 9 - adoption, use or disclosure of government related identifiers

Part 4 - Integrity of personal information
Australian Privacy Principle 10 - quality of personal information
Australian Privacy Principle 11 - security of personal information

Part 5 - Access to, and correction of, personal information
Australian Privacy Principle 12 - access to personal information
Australian Privacy Principle 13 - correction of personal information

For a full copy of The Australian Privacy Principles

Is your organisation subject to the Privacy Principles?

If your organisation turns over $3 million OR collects personal or sensitive information then the Privacy Principles will apply to your organisation.

Even if your organisation is not currently affected by this legislation, it may still be in your
organisation’s interest to review your organisation’s privacy policy and practices on handling personal and sensitive information to ensure that they are in line with the Australian Privacy Principles. Making improvements in organisational practice will benefit the organisation’s risk management, improve protection of client’s rights and protect the privacy of personnel (staff, volunteers, Board members).

If your organisation handles ‘personal information’ or ‘sensitive information’ and is affected by this reform (see definitions below) it will need to review its policies and practices on how that information is collected, stored, shared and disposed of. This review should ensure that your organisation is complying with the new Australian Privacy Principles (APPs). It should assist you to check that the privacy policy is up-to-date, and that clients have easy access to be able to read the organisation’s privacy policy and find out how their personal information is handled.

**What do the Australian Privacy Principles (APPs) mean for individuals?**

The APPs are designed to help ensure that the quality of personal information is complete, accurate, up-to-date and used only for the purposes it was collected.

The APPs assist people to make more informed choices about how they want their personal information to be handled so they can decide whether they want to deal with particular organisations (including NGOs and service providers) and businesses.

The APPS enable people to know:

- how their personal information will be handled
- whether their information is likely to be sent overseas
- how to complain about a possible privacy breach

The APPs also regulate:

- the way in which personal information can be used for direct marketing
- the credit reporting system.

The privacy laws also give the Commissioner powers to resolve privacy complaints and investigations, including the ability to impose a penalty of up to $1.7 million for serious breaches.

**What are the implications for your organisation?**

Some of the key changes and implications for organisations (including NGOs and service provider organisations) as a result of the Australian Privacy Principles (APPs) replacing the NPPs are:

- There are now specific definitions about what constitutes ‘personal information’ and ‘sensitive information’ under the Privacy Act.
- Organisations need to have an up to date APP privacy policy that is reviewed regularly. The legislation sets out some requirements for privacy policies, including requirements for content and availability.
Organisations must take reasonable steps to comply with the new APPs, including the implementation of new practices, procedures and systems that will ensure the organisation can handle privacy inquiries and complaints from individuals. This may include training staff or establishing procedures to identify and manage privacy risks.

- Organisations must give individuals the option to be anonymous or use a pseudonym.
- There are new rules that apply to collection practices and notices when collecting personal information and/or sensitive information (such as health information).
- There are new rules on when personal information and sensitive information can be used or disclosed.
- There are new exceptions to the general ban against the adoption, use or disclosure of government related identifiers (e.g. Medicare number).
- There are new rules on how organisations are to respond to requests for access to and correction of personal information (including timeframes, the manner in which access is to be given, when written reasons are required).

Quick checklist

<table>
<thead>
<tr>
<th>1. Availability of your organisation’s privacy policy</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is your organisation’s privacy policy easily and freely available to clients?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2. Personal and sensitive information</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Is your organisation aware of the differences between personal and sensitive information? (see definitions on page 4)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the organisation aware of the different requirements for both forms of information?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3. Collecting, maintaining and storing information</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Does staff know what is required when collecting information from clients?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the organisation have reasonable measures in place to keep client’s information accurate, up-to-date and complete?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the organisation provide clients with information on how to request access to their information? What steps does your organisation take to ensure client’s information is secure?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4. Use or disclosure of personal information</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Is your organisation’s use of or disclosure of client information consistent with the new privacy requirements?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does your organisation record government indicators (e.g. Medicare or tax file numbers)? If so, is it aware that there are restrictions around their use and disclosure?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Resources

**Essential information and resources for all organisations**, including useful checklists are available via the [Office of the Australian Information Commission](http://www.oaic.gov.au/privacy/privacy-topics/health-for-service-providers/)

**Health services**

Specific information for health services from the Office of the Information Commissioner

**Tenancy and real estate**


**Education and child care**


Please note: The information provided in this info sheet is of a general nature. It is not a substitute for legal advice.

For more information see:

- Policy template: Privacy
- Policy template: Access to confidential information
- Policy template: Client records
- Policy template: Confidentiality
- Tool: Data collection planner
- Tool: Staff: Confidentiality agreement
Key definitions

'personal information' means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

'sensitive information' means:

a) information or an opinion about an individual's:
   i. racial or ethnic origin; or
   ii. political opinions; or
   iii. membership of a political association; or
   iv. religious beliefs or affiliations; or
   v. philosophical beliefs; or
   vi. membership of a professional or trade association; or
   vii. membership of a trade union; or
   viii. sexual preferences or practices; or
   ix. criminal record:
      that is also personal information; or

b) health information about an individual; or

c) genetic information about an individual that is not otherwise health information.

Source: PRIVACY ACT 1988 - SECT 6 Interpretation