

# Legislative Summary: Privacy and Data Protection Overview



Making sure  
it's secure.™

## The Privacy Act (Australia)

Enacted: 1988; Into force: 1989 – under the Office of the Australian Information Commissioner (OAIC)

### 1 What the law covers:

- How personal information must be protected during its collection, handling and disclosure
- The 13 Australian Privacy Principles (APPs) that set out the standards, rights and obligations that must be met by APP entities

### 2 What is “personal data”:

Any information about an identified individual or an individual who is reasonably identifiable. Examples of identifiable information: name, address, date of birth and rare or unique characteristic(s).

### 3 The APPs and information management:

The Australian Privacy Principles (APPs) set the basic standard for privacy protection and stipulate how organisations can collect, use and disclose personal information. They are also technology neutral, applying equally to paper-based and digital environments.

**Collection:** the act of gathering, acquiring or obtaining personal information from any source or by any means.

**Use:** the handling or undertaking of an activity with the information that is within the APP entity's effective control.

**Disclosure:** the act of making the information accessible to others outside the APP entity and releasing the subsequent handling from its effective control.

### 4 Who must adhere to the regulations:

Any APP entity. They include:

1. Commonwealth government agencies
2. Private sector organisations with an annual turnover of \$3 million or more that are carrying on business in Australia or collecting information from individuals physically present in Australia
3. A small business or individual, body corporate, partnership, unincorporated association or trust that provides a health service or holds any health information (except in an employee record)

### 5 How to comply:

APP 11 relates directly to document management. It stipulates that all personal information should be handled fairly and lawfully, and that the APP entity must take reasonable steps to:

- **Protect** the information from misuse, interference, loss, unauthorised access, modification or disclosure
- **Destroy or de-identify** the information as soon as it is no longer required for its intended purpose, or to be retained to meet other legal obligations

**Recommended security management and information controls:**

- Use passwords to restrict access
- Train staff on the APPs
- Ensure facilities are secure
- Properly dispose of printed material

## 6 Offences/penalties for non-compliance

Individuals and corporations can be subject to civil penalties for offences that contravene The Privacy Act.

For example, under s 13G, a serious or repeated interference with privacy is subject to a maximum penalty of \$340,000 for an individual or \$1.7 million for a corporation.



## 7 Secure document retention and disposal requirements:

The Privacy Act requires APP entities to securely destroy or de-identify personal information once it is no longer required for its intended purpose. However, prior to any action, the organisation must also take into account the document retention periods of other applicable legislation, and their penalties for non compliance.

**Regulatory document retention periods are in place for:**

- Employment records (Fair Work Act 2009)
- GST records
- Corporate tax records
- Transaction records and formal company documents (Corporations Act 2001)

**Implementing a document retention policy can help to demonstrate compliance.**

**Recommended inclusions:**

- ☐ A statement of purpose
- ☐ Categories of documents and how long they should be kept
- ☐ Definition of “document” and the format and length of time in which it is to be retained (electronic or hard copy)
- ☐ Guidance on creation of documents
- ☐ Members of staff designated to deal with the document management system
- ☐ Methods of document destruction
- ☐ How to keep an accurate record of documents destroyed

## 8 How Shred-it can help:

**Secure Document and Hard Drive Destruction**

- Secure end-to-end chain of custody
- Security trained and vetted staff
- Tailored solutions to your organisation’s needs

**Advice and Expertise**

- Trained experts in information security
- Help assess document security risks in your organisation
- Helpful resources available at [shredit.com.au/resource-centre](https://shredit.com.au/resource-centre)

**For peace of mind,  
contact Shred-it today**

**1800 012 012 | [shredit.com.au](https://shredit.com.au)**



**Making sure  
it's secure.™**

**For more information:**

Privacy Commissioner – [oaic.gov.au](https://oaic.gov.au)  
Privacy Act – [comlaw.gov.au](https://comlaw.gov.au)  
Corporations Act 2001 – [comlaw.gov.au](https://comlaw.gov.au)