IM LAWYERS

What are the Australian Privacy Principles and why are they important for my business?

Date: Monday June 23, 2025

In Australia, the Privacy Act 1988 (Cth) ('Privacy Act') and the Australian Privacy Principles ('APPs') govern the way that applicable businesses collect, use and store an individual's personal information. In today's global economy, with increasing access to information and to new technology, Australia's privacy framework offers important protections for individuals as threats to the collection and retention of personal information continue to grow.

In this article, we look at each of the 13 Australian Privacy Principles and provide information about how they may apply to Australian businesses.

Application of the Privacy Act

As a general rule, the Privacy Act (and the APPs) apply to most government agencies and some private organisations with a turnover of more than $3 million. These organisations are sometimes referred to as 'APP entities'.

There are additional organisations that do not meet that threshold but which are required to comply with the Privacy Act due to the nature of their business/industry; for example, health service providers or organisations that trade in personal information. The Office of the Australian Information Commissioner provides more information about the businesses that must comply, despite not meeting the monetary threshold

Alternatively, organisations that are not required to comply with the Privacy Act, but wish to, can 'opt in' to the obligations.

The Australian Privacy Principles

There are 13 Australian Privacy Principles that outline the standards, rights and obligations relating to the collection, use and

disclosure of personal information in Australia. They also address an organisation or agency's responsibilities for governance and accountability. Additionally, the principles ensure the integrity and correction of personal information and establish the right of individuals to access their own personal information.

Below, we provide a simplified overview of the primary requirements for each of the APPs.

APP 1 – Open and transparent management of information

APP entities are required to handle personal information openly and transparently. This includes:

taking reasonable steps to comply with the APPs;

having a clear and up-to-date privacy policy which includes all necessary information (stipulated in APP1.4) relating to the entity's use and management of personal information, that is available for view by individuals free of charge.

Generally, a privacy policy should be displayed on the entity's website and should be accessible considering the special needs of those who may need to access this document (for example, written in plain English, or consideration of low vision or non-English speaking individuals).

APP 2 – Anonymity and pseudonymity

APP 2 provides that individuals must be given the opportunity to deal with an APP entity anonymously (or by use of a pseudonym) until required (for example, by law) to not do so, or it is impracticable to do so.

An example of a scenario where it may be impracticable for an entity to deal with an individual anonymously could include:

a doctor may not be able to bulk bill or provide a Medicare rebate to a patient if that patient deals with them anonymously; and

where a hospitality venue is required by the Office of the Liquor and Gaming Regulator to check a patron's identification prior to entry into the venue, it may not be possible to permit the patron to enter anonymously.

APP 3 – Collection of solicited personal information

An APP entity solicits personal information when it actively requests or collects that personal information from another entity. APP 3 sets out when APP entities are permitted to solicit this personal information.

APP entities may only solicit personal information that is reasonably necessary to perform its functions or activities. The collection and solicitation must derive directly from the individual, unless an exception applies. In the case of sensitive personal information, individual consent to the collection of that information is required at a minimum.

APP 4 – Dealing with unsolicited personal information

Sometimes, in the course of its work, an APP entity may come into possession of personal information that it did not actively solicit, and APP 4 provides guidelines for how that information is to be dealt with in that scenario.

When unsolicited personal information is received, the APP entity must consider whether it would have been permitted to solicit that information (referring to APP 3). If the answer to that question is no, then the organisation must destroy or de-identify that information as soon as practicable if it is lawful and reasonable to do so. Otherwise, the APP entity must deal with the personal information in accordance with APPs 5-13 (see below).

APP 5 – Notification of collection of personal information

APP 5 sets out certain information that an APP entity must take reasonable steps to provide to an individual once their personal information is collected. This information includes:

the entity's information (e.g. company name and ABN/ACN) and contact information;

how the information is collected;

whether the collection is required or authorised by law;

why the information is collected the purpose of the collection;

what would happen if the information is not collected (for example, would the entity not be able to provide services to that person);

how and to whom the entity usually discloses the kind of information that it collects;

the entity's privacy policy;

whether the information is likely to be disclosed overseas and if so, to which countries.

You may see these notifications referred to as "Collection Notices" by some organisations.

APP 6 – Use or disclosure of personal information

Where an APP entity has collected personal information in accordance with APP 3, then APP 6 only permits the entity to use or disclose the personal information for the purpose it was collected or for secondary purposes in some instances. For example, in some circumstances, the entity may use or disclose the personal information for a secondary purpose, for example, where the individual has provided their consent for use for that secondary purpose.

APP 7 – Direct marketing

APP 7 sets out criteria for when an APP entity is permitted to use an individual's personal information for the purposes of direct marketing, and also additional guidelines in relation to that direct marketing.

Even where the direct marketing has been sent appropriately, the individual must be given a simple opportunity to 'opt out' (e.g. unsubscribe) or select to no longer receive the direct marketing. If such a request is made, the APP entity must action this within a reasonable time without any charge to that individual.

APP 8 – Cross-border disclosure of personal information

APP 8 sets out that if an APP entity is going to disclose an individual's personal information to an overseas recipient, then it must take reasonable steps to ensure that the recipient will also comply with the APPs (or some other equivalent requirements), before providing the information.

Something that businesses should be particularly conscious of when procuring technology and software is to ensure the location of the data storage when it is used in those programs and ensure that the data privacy complies with APP standards.

APP 9 – Adoption, use or disclosure of government-related identifiers

Organisations must not use, disclose or adopt any government identifiers (e.g. Centrelink

reference numbers, Medicare numbers).

APP 10 – Quality of personal information

APP 10 requires that organisations take reasonable steps to ensure that the personal information they hold about individuals is accurate, complete, and current for the duration the information is retained by the entity. Businesses should be mindful of regularly reviewing and maintaining stored information to ensure compliance.

APP 11 – Security of personal information

Organisations are required to take reasonable and active steps to protect the personal information from unauthorised access, disclosure, loss, or misuse. What is reasonable in the circumstances may depend on various factors, which may include:

the sensitivity of the information;

the size of the entity; or

the complexity of operations.

Measures that can be taken could include things like password protection and locked storage of physical files. This may also include de-identifying the information once it is no longer reasonably required by the organisation.

APP 12 – Access to personal information

This APP requires organisations to provide individuals with the opportunity to access the personal information that the organisation holds on that individual. This APP may require some organisations to consider the way the personal information is stored and where it is stored to understand what steps they would need to take to facilitate this access.

It is important to note, though, that organisations should continue to be mindful of the obligation to provide security over the personal information when complying with requests for access pursuant to this APP.

Some things to consider include:

How the organisation will verify the identity of the person requesting access, and confirm that they are the individual or a person properly authorised by that individual.

How the organisation intends to provide access while maintaining the security of the access materials and other personal information of other individuals.

APP 13 – Correction of personal information

APP 13 is in some way quite similar to APP 12, however, rather than an individual requesting to access their information, they are requesting that the organisation correct their personal information. This could be as simple as an individual providing updated contact information after changing their phone number.

As with APP 12, it is important that the organisation satisfy itself of the identity and authority of the person making the request before taking the necessary steps to correct the information.

Stay informed about your obligations under the Australian Privacy Principles

As technological advancements continue, transfer of personal information and data increases. As a result, privacy reforms are increasingly discussed and considered. It is critical for Australian businesses to keep on top of amendments to this area of law, as they directly impact business practices.

For example, most recently, the Privacy and Other Legislation Amendment Act 2024 updated requirements under the Act regarding overseas entities holding or using personal information. In addition, the amending Act introduced privacy principles and disclosure requirements related to the use of AI.

This is a perfect time for businesses to review and understand the personal information they hold, and the processes that they may need to implement to improve their compliance with the Privacy Act and the APPs. It is particularly important as businesses increase their implementation of AI in their business practices and operations. This will enable them to respond and act more effectively, drawing on their recent and up-to-date knowledge of the business's current practices, when further legislative or regulatory updates are introduced.

Get help from a commercial lawyer

If you require assistance updating your privacy compliance, including considering privacy risks and drafting a privacy policy/statement, then be sure to get in touch with IM Lawyers for an obligation-free discussion with one of our lawyers.

This article is of a general nature and should not be relied upon as legal advice. If you require further information, advice or assistance for your specific circumstances, please contact us.