The Australian Privacy Act

An overview of the Australian Privacy Principles (APPs)

Author: Paul Green

A Fresh Perspective

INTRODUCTION

If you are collecting or processing personal information then you are likely to be required to be compliant to the Australian Privacy Act. Even if you are not required to be compliant, it is best practice to ensure that you are following the principles of the act.

All Australian Government and ACT agencies and most business and not for profit organisations with an annual turnover in excess of $3 million, are required to comply with the Australian Privacy Act, as well as most health providers, credit reporting agencies, personal information brokers and employee associations. State Government agencies have to comply with the state's privacy laws.

The Australian Privacy Act constitutes thirteen Australian Privacy Principles (APPs). The following sections identify the APPs and discuss how you might consider them within your organisation.

APP 1 — OPEN AND TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION

It is best practice and a requirement under APP1 of the Privacy Act to have in place an Information Security Management System (ISMS). At the very least this should consist of set of policies and procedures that detail how the organisation's sensitive data is managed. The goal of an ISMS is to minimise the risk to the organisation and ensure business continuity by pro-actively mitigating the impact of a data breach.

If the organisation is collecting, storing or processing personal information then the ISMS must also include a Privacy Policy, which should detail how the organisation manages the personal information it collects, and the information flows associated with that personal information.

APP 2 — ANONYMITY AND PSEUDONYMITY

The organisation should not collect personal information from an individual when it is not required to perform the action they request. In doing so the organisation is providing the individual with the opportunity to transact anonymously. An example of this would be an enquiry about products and services made in person by the individual.

If the transaction does not need the individual's identity, but there are requirements to tie future transactions from the same individual together, then it may be appropriate to allow the individual to use a pseudonym. An example of this could be a screen name in a chat room.

Information systems used by the organisation should consider these before collecting personal information, unless the organisation is able to demonstrate that anonymity and pseudonymity would not enable the provision of the service, or that there are other laws or regulations that require the individual's identity to be known and recorded.

APP 3 — COLLECTION OF SOLICITED PERSONAL INFORMATION

Any privacy information collected should be identified and your organisation must be able to demonstrate that it is required for the provision of services to the individual concerned. Examples of solicited personal information could include application forms, competition entries, business cards exchanged at a meeting and credit card payments.

Some personal information is defined as sensitive under the Australian Privacy Act. Sensitive information can only be collected by authorised organisations and only for specific purposes. Additional safeguards must be in place to secure sensitive personal information. Examples of sensitive information include health records, racial/ethnic origin, religious affiliations, sexual orientation, criminal records and biometric information that is used for identification (e.g. fingerprints).

Any organisation collecting personal information must consider the following:

- Understand what information they are collecting.
- How it is being collected?
- Why it is required?

APP 4 — DEALING WITH UNSOLICITED PERSONAL INFORMATION

If personal information is received by the organisation that was not requested then the organisation should have a process to determine what to do. An example of unsolicited personal information could

be a job applicant completing the required application form and voluntarily attaching a copy of their passport, which was not requested.

The process to deal with unsolicited personal information should detail how the organisation determines that the information is unsolicited, what (if any) laws and regulations mat apply to the retention of the data, and how the data is to be destroyed or permanently deleted.

APP 5 — NOTIFICATION OF THE COLLECTION OF PERSONAL INFORMATION

The individual concerned must provide informed consent and this should be recorded in your systems. The individual must be informed of why your organisation is collecting the information and what you intend to do with it, referred to as the "Primary Purpose". This includes whether your organisation will transmit the personal information to another entity, particularly if that entity is overseas; and if practical should list the destinations. The notification must also direct the individual to where they can get a copy of your organisations privacy policy.

The organisation may also request the individual to authorise the use of the information for a "secondary purpose", but this would normally be optional. An example of a secondary purpose would be to use an individual's contact details to send them marketing information in addition to sending them the item they have purchased, which would be the primary purpose.

There are some exceptions to the notification but generally the organisation would need to demonstrate that the individual should have known previously, e.g. a doctor referring a patient to a specialist for treatment would include details of the individual's medical history relating to the episode of care.

Notification must be clearly visible prior (or at the same time) as the collection of the information. For example, on the top of the web page or printed at the top of the form. It is also good practice to ask the individual to acknowledge that they understand the notification by requesting them to tick a box.

APP 6 — USE OR DISCLOSURE OF PERSONAL INFORMATION

An organisation can only use the personal information collected for the primary purpose and if applicable any secondary purposes, as notified during collection. If the organisation is required to disclose the personal information, either as part of its business function or as required by law, then the individual must be notified in the notification about who and when the information will be disclosed.

The organisation must also identify what will happen in the event that there is an unauthorised disclosure. This would be part of the organisation's Data Breach Notification process.

APP 7 — DIRECT MARKETING

Direct marketing is when an organisation uses an individual's personal information to send communications with the sole purpose of promoting goods or services. Some examples of direct marketing by an organisation include a catalogue in the mail addressed to them by name, displaying a personalised advertisement on a social media site that an individual is logged onto, sending an email to an individual.

Marketing is not direct, if personal information is not used or disclosed to identify the particular individual.

The organisation must provide and clearly advertise a facility that enables an individual to remove themselves from such a list, and must ensure that valid requests are honoured. If the organisation uses a third-party for the provision of direct marketing lists then this facility is often provided by that party.

APP 8 — CROSS-BORDER DISCLOSURE OF PERSONAL INFORMATION

If an organisation is required to provide the personal information to a third-party outside of Australia so that third-party can perform functions on behalf of the organisation then this is classed as “cross-border disclosure”. The individual must have been notified that their personal information is required to be sent outside of Australia, but they do not need to explicitly consent.

The organisation remains accountable for any breaches of the Australian Privacy Act, even if these breaches occur at the third-party or within the third-party systems. The organisation is also accountable for any data breach notification requirements.

If the third-party is only storing the information, and is not processing it; e.g. offshore cloud storage; then this requirement may not apply.

APP 9 — ADOPTION, USE OR DISCLOSURE OF GOVERNMENT RELATED IDENTIFIERS

Government related identifiers are restricted in how organisations can use them. They must never be used by an organisation as a unique identifier and must only be collected if required by the organisation to perform the service or function.

Some examples of government related identifiers include Medicare numbers, Centrelink Reference numbers, Drivers Licence numbers issued by State and Territory authorities, Tax File numbers and Australian Passport numbers. Some government related identifiers are regulated and are restricted in how organisations can collect, use or disclose the particular identifier and related personal information.

APP 10 — QUALITY OF PERSONAL INFORMATION

It is the responsibility of the organisation to ensure that the personal information that it holds is correct and up to date. This could be as simple as refreshing from a known and trusted source at regular intervals, or prompting the individual to validate and update their personal information at regular intervals, or implementing processes that catch returned mail and email; undelivered SMS; incorrect phone numbers; and unused accounts, to update the information or mark it as not being reliable.

If an individual requests that their personal information be updated or corrected then the organisation must have a process to ensure that these requests are actioned in a timely manner, see APP 13.

APP 11 — SECURITY OF PERSONAL INFORMATION

The organisation is required to ensure the security of the personal information that it holds. The organisation should ensure that they have a privacy impact assessment for the information systems that process this data. This assessment should identify any impacts (or risks) to the privacy of the individual and make recommendations on how to mitigate them. Your organisation should also document the processes and systems that are in place to secure the personal information, including monitoring and reporting processes and systems. These documents are your organisations first line of defence as they demonstrate that you have considered the security of the information.

Once personal information is identified as no longer required then it should be securely destroyed or deleted, unless there is a legal requirement to retain it for audit or archival purposes (e.g.Commonwealth record).

APP 12 — ACCESS TO PERSONAL INFORMATION

An organisation must provide access to an individual of all the information that they hold on said individual. There are some limited cases where an organisation may refuse access, most notably where personal information is shared and could lead to an impact of the other individual.

The requesting individual must be authenticated to ensure that they are the individual, or in some circumstances an authorised proxy for the individual. There may be other legal avenues for the individual to access the personal information for example Freedom of Information request (FOI).

APP 13 — CORRECTION OF PERSONAL INFORMATION

An organisation is required to correct 'incorrect personal information' as quickly as is practical after a request from the individual or when the information is identified as being incorrect. The organisation must provide a process and/or facility for the individual to correct their information or make a request for their information to be corrected.

There are some limited cases where changing the personal record is restricted, e.g. Commonwealth record.

CONTACT US

We are always happy to talk to organisations about tackling their data privacy and security challenges:

1300 06 06 42 / info@businessaspect.com.au