LPA Guide

Australian Privacy Principles

07 July 2016

LIVE PERFORMANCE AUSTRALIA

Australian Privacy Principles

Australian Privacy Principles

Key Points

- The Australian Privacy Principles (APPs) apply to all private sector and not-for-profit organisations with an annual turnover of more than $3 million, and most Australian Government agencies. The APPs do not apply to state, territory and local government entities. Most of these jurisdictions have privacy principles in place for government entities which are similar to the APPs.

- The APPs do not apply to small businesses with an annual turnover of less than $3 million, unless they trade in personal information. LPA recommends that organisations not bound to comply with the APPs should use the APPs as a best practice guide for managing personal information.

- The only person who 'owns' personal information is the individual to whom the information belongs. No organisation (producer, venue, ticketing company etc.) owns the personal data of consumers.

- Personal information can only be collected by organisations where it is reasonably necessary for one or more of the organisation's functions or activities. Personal information can only be provided by the individual it relates to (and not a third party), unless it is unreasonable or impracticable to do so.

- Individuals can choose to deal with organisations anonymously or under a pseudonym, except in instances where it is impractical for the organisation to deal with individuals who have not identified themselves.

- Organisations must inform individuals of their privacy and data collection practices, such as what information is collected, how the information is used, and whether information is likely to be disclosed to overseas recipients. This may be partially or wholly covered by developing a privacy policy made available to individuals free of charge (e.g. online).

- Personal information can only be used or disclosed for the specific purpose it was collected, except when the individual has consented to or would reasonably expect that the personal information would be used for a secondary use or disclosure.

- Organisations must take reasonable steps to protect personal information from a range of risks, such as but not limited to misuse, interference or loss.

- Organisations may use personal information (other than sensitive information) about an individual for direct marketing purposes if the individual has consented to or would reasonably expect that their personal information would be used for direct marketing, and the organisation has provided a simple means for the individual to opt-out of receiving direct marketing communications.

- Organisations can use personal information collected by third parties (e.g. venue or ticketing company) or share personal information with third parties (e.g. promoter) for direct marketing where consent to use or disclose the information for this purpose has been provided by the individual.

- Organisations must only collect sensitive information (e.g. racial or ethnic origin) about an individual if the individual consents to the collection and the information is reasonably necessary for the organisation's functions or activities, or an exception applies.

Introduction

The *Privacy Act 1988* (Cth) contains 13 Australian Privacy Principles (APPs) which outline how applicable entities must handle, use and manage personal information. These principles are legislative requirements and hold legal force.

The *LPA Guide to the Australian Privacy Principles* provides guidance on how the APPs generally apply to LPA Members. It is important to note that the law is 'principle based', and therefore does not provide prescriptive directions or details about how the principles should be implemented.

1. Application

The APPs apply to all private sector and not-for-profit organisations with an annual turnover of more than $3 million, and most Australian Government agencies ("APP entities"). The APPs outline how these entities must handle, use and manage both paper-based and digital personal information.

Personal information is information or an opinion (including within a database) about an individual with an apparent identity, or an identity that can be reasonably ascertained from the information or opinion. Common examples of personal information include name, signature, address, telephone number, bank account details and opinion or commentary. Information that has been successfully de-identified is not personal information. Successful de-identification means that the personal is not identifiable or cannot be reasonably identified.

The APPs do not apply to small businesses with an annual turnover of less than $3 million, unless they trade in personal information. LPA recommends that organisations not bound to comply with the APPs should use the APPs as a best practice guide for managing personal information.

1.1 Trading in personal information

Trading is considered buying, selling, bartering or gaining a commercial benefit in return for providing personal information about individuals. A business is not trading in personal information if it gives or receives personal information for a benefit, service or advantage and it always has the consent of all the individuals concerned; or only does so when authorised or required by law.

Example: Trading in personal information

A local venue is a not-for-profit. It does not have an annual turnover of more than $3 million. However, the venue begins selling mailing lists to promoters. Now that the venue trades in personal information, the APPs apply.

1.2 State, territory and local government entities

The APPs do not apply to state, territory and local government entities. Most of these jurisdictions have privacy principles in place for government entities which are similar to the APPs. They cover use, collection, disclosure and management of information. Many jurisdictions also have mechanisms that allow organisations to modify their obligations.

Western Australia does not have a privacy regime, and there is no applicable legislation for South Australian local government authorities. Government entities that fall within these jurisdictions are governed by their own privacy policies, but should use the APPs as a best practice guide.

2. Collecting personal information

2.1 Solicited information

APP 3 governs the collection of personal information where it has been requested by organisations from individuals.

Personal information can only be collected by organisations where it is reasonably necessary for one or more of the organisation's functions or activities. Personal information can only be provided by the individual it relates to (and not a third party), unless it is unreasonable or impracticable to do so.

Example: Soliciting information

A promoter collects feedback forms at the end of the show. The feedback is not anonymous and so the opinions are considered personal information. The opinions are reasonably necessary for the organisation's functions; therefore it is permissible to collect this information.

2.2 Unsolicited information

APP 4 governs the collection of unrequested personal information. Personal information is considered unsolicited when it is received without active steps being taken to collect the information.

If unsolicited personal information is received, organisations must determine within a reasonable time if it could have lawfully collected the information under APP 3 (see above). If this is the case, organisations may keep the information and deal with it as if it had been solicited. If this is not the case, the information must be destroyed or de-identified as soon as is lawful and practical to do so.

Example: Unsolicited information

A venue mistakenly received an email from an audience member. The email was addressed to the artist and contained a range of personal information. The majority of the information received is not relevant to the venue's operation; therefore the venue should destroy or de-identify the personal information.

2.3 Anonymous dealings

APP 2 requires that individuals be provided with the option of dealing with organisations anonymously or under a pseudonym.

Anonymity requires that a person can deal with an organisation without providing personal information or identifiers. Pseudonymity allows for individuals to deal with organisations using a name, term or descriptor that is different to their actual name. This does not apply where it is impractical for the organisation to deal with individuals who have not identified themselves.

Example: Using pseudonyms

A theatre company posts a media release online and enables comments to be posted in response to the release. A commenter can use a 'screen-name' so that his/her personal information is not identifiable. At a later stage, the commenter may purchase tickets and provide credit card information to the theatre company. The individual has chosen to divulge his/her identity to be able to purchase tickets. However, the theatre company has allowed for pseudonymity where possible.

2.4 Notification of the collection of personal information

APP 5 requires that organisations take reasonable steps to notify individuals or ensure they are aware of particular privacy and information collection practices of the organisation. Ideally, this should be done prior to, or at the time of collection. If this is not possible, individuals must be notified as soon as practicable.

The matters that individuals must be notified about include:

- the organisation's identity and contact details;
- the facts and circumstances of collection;
- whether the collection is required or authorised by law;
- the purposes of collection;
- the consequences if personal information is not collected;
- the organisation's usual disclosures of personal information of the kind collected by the entity;
- information about the organisation's privacy policy; and
- whether the organisation is likely to disclose personal information to overseas recipients, and if practicable, the countries where the overseas recipients are located.

3. Using personal information

APP 6 outlines when organisations can use and disclose personal information (not applicable to direct marketing). Further information on direct marketing can be found on p.7.

Personal information can only be used or disclosed for the specific purpose it was collected. Generally, it cannot be used for any other purpose. However, there are a few exceptions that may be relevant to LPA Members, such as the individual:

- has consented to a secondary use or disclosure; or
- would reasonably expect that the personal information would be used for the secondary purpose. The secondary purpose must be related to the primary purpose of collection.

Example: Using personal information for a secondary purpose

A ticketing company collects the personal information of consumers to process the purchase of tickets to a music festival.

- The ticketing company is running a prize draw competition for consumers that purchase tickets to the festival, and sought consent from consumers to use the personal details for the purpose of entering ticket holders into the competition.
- The ticketing company needs to inform consumers that a band scheduled to perform at the festival has cancelled. Consumers would reasonably expect that the ticketing company would use their contact details to inform them of this change.

3.1 Sharing data for reporting or data analysis purposes

Organisations may wish to access information relating to attendees for reporting or data analysis purposes. Information such as age, home address, or attendance rates may prove useful for reporting purposes and gaining a deeper understanding of a client-base.

There are three instances whereby data sharing is legal. Specifically if reporting purposes:

- fall under the ‘primary purpose’ of collecting the information;
- are a ‘secondary purpose,’ but the individual has consented; or
- are considered a ‘secondary purpose’ and the individual would reasonably expect the use or disclosure of their information as it is related to the primary purpose.

Privacy notices (refer to 2.4, p.5) can assist in these instances by establishing:

- express or implied consent to using personal information for a secondary purpose; or
- that an individual would reasonably expect their data to be used in this way by setting out a range of likely secondary uses.

Further to this, information that is not ‘personal’ (i.e. does not identify an individual) can be shared (e.g. postcodes of attendees).

4. Obligations when holding personal information

4.1 Maintaining quality of personal information

APP 10 requires that reasonable steps be taken to ensure that the collection, use and disclosure of personal information is accurate, up-to-date and complete.

Reasonable steps depend on the circumstances (e.g. sensitivity of information, size of the organisation, risk of adversity). In some circumstances, it is reasonable that an organisation will take no steps to ensure the quality of personal information.

4.2 Securing personal information

APP 11 requires that steps be taken to protect personal information from the following:

- misuse
- interference
- loss
- unauthorised access
- unauthorised modification
- unauthorised disclosure

Once information is no longer needed for the purpose it was collected, it must be destroyed or de-identified.

4.3 Providing access to personal information

APP 12 requires that an individual must be able to access his/her personal information on request.

If such a request is made, organisations must take steps to verify the individual's identity. Organisations must give access in the manner requested by the individual if it is reasonable to do so and within a reasonable period. If an organisation decides not to give an individual access, the organisation must generally provide written reasons for the refusal and the mechanisms available to lodge a complaint. If an organisation intends to charge a fee for giving access to the individual's personal information, the charge must not be excessive and must not apply to the making of the request.

4.4 Correction of personal information

APP 13 requires that steps be taken to correct personal information in order to ensure its accuracy.

Personal information must be corrected where:

- an organisation is satisfied that it is inaccurate or;
- if an individual requests a correction.

Where an individual makes a request for correction, the organisation should respond in a reasonable time. Organisations cannot charge individuals for making this request.

If the information has been passed onto third parties, organisations must take steps to notify them of the correction, as requested by the individual.

Whether information is accurate, up-to-date, relevant and not misleading is dependent upon the purpose for which the information was collected.

4.5 Disclosing personal information to overseas entities

APP 8 requires that organisations take reasonable steps to ensure overseas recipients do not breach the APPs.

Organisations that disclose personal information to overseas recipients may be accountable for how the information is handled. This does not apply if relevant individuals are expressly informed and consent to both the disclosure and non-application of APP 8.

When an organisation collects information they must take steps to inform the individual as to whether the information is likely to be disclosed to overseas recipients, and if it is practicable, where those recipients are located. This is particularly important for organisations that use ticketing and CRM systems that may store information overseas.

5. Direct Marketing

APP 7 stipulates specific conditions under which the use and disclosure of personal information for direct marketing is permitted.

An organisation may use or disclose personal information (other than sensitive information) about an individual for direct marketing purposes if:

- it collected the information from the individual;
- the individual would reasonably expect (usually by notification) that his/her personal information would be used or disclosed for direct marketing;
- the organisation has provided a simple means for the individual to opt out of receiving direct marketing; and
- the individual has not made a request to opt-out of receiving direct marketing.

5.1 Third parties and direct marketing

Organisations can use personal information collected by third parties, such as venues or ticketing companies, where consent to use or disclose the information for this purpose has been provided by the individual.

Similarly, personal information can be shared with third parties, such as a promoter, for the purposes of direct marketing when the following conditions are satisfied:

- the individual consents to their personal information being used or disclosed in this way (unless it is impractical to seek consent);
- the organisation provides a simple means to opt-out and a prominent statement in each direct marketing communication informs the individual that they can do so; and
- the individual has not requested to opt-out.

In the interests of industry best practice organisations may give consumers the option of being contacted in the future by all relevant stakeholders (e.g. venue, ticketing company and promoter/producer). It is important to gain consent at the outset to ensure that any direct marketing and data sharing complies with the APPs.

To facilitate consent for directing marketing and data sharing consumers should be asked the following questions:

- Do they wish to be contacted in the future by the ticketing company or venue about events or news that may interest them?
- Do they wish for their contact information to be shared with the event promoter/producer, so that the event promoter/producer can contact the customer directly about future events or news that may interest them?

Consent need only be sought once, such as when the consumer sets up an online account with the organisation and discloses their contact details, providing that the consumer can opt-out of receiving direct marketing communication at any time.

5.2 Application of The Spam Act 2003 (Vic) ('The Act')

The Act includes provisions related to direct marketing and sets out the following requirements for permissible electronic messages (s. 15-18):

- express or implied consent (e.g. ticking a box on a website) of recipient must be attained (a one-off purchase cannot be inferred as consent);
- the message must identify the organisation that authorised sending the message; and
- there must be a functional 'unsubscribe' facility.

Example: Direct Marketing

As part of the ticket purchase process, a ticketing company asks consumers to opt-in to receiving monthly e-newsletters. Consumers provide consent when they do not opt-out. The ticketing company identifies itself clearly in the monthly e-newsletter (not just the artists) and clearly displays an 'unsubscribe' facility.

6. Sensitive Information

APP 3 clarifies that an organisation must only collect and use sensitive information about an individual if the individual consents to the collection and the information is reasonably necessary for the organisation's functions or activities, or an exception applies.

Sensitive information includes information or an opinion about an individual's:

- racial or ethnic origin;
- political opinions;
- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;
- sexual orientation or practices; or
- criminal record.

Collecting an individual's sensitive information is permitted by non-profit organisations if the information relates:

- to the activities of the organisation; and
- solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

Section 6 of the Privacy Act states that a 'non-profit organisation' is an organisation that engages in activities for cultural, recreational, political, religious, philosophical, professional, trade or trade union purposes, and does not earn a profit.

7. Privacy Policies

APP 1 stipulates that organisations must have a privacy policy that contains specified information about the privacy and information collection practices of the organisation, including the kinds of personal information it collects, how an individual may complain about a breach of the APPs, and whether the organisation is likely to disclose information to overseas recipients.

Organisations must take reasonable steps to make their privacy policy available free of charge (e.g. online) and in an appropriate form. Reasonable steps must also be taken to make the policy available in a particular form that an individual requests.

As a best practice guide, your privacy policy should address the following questions:

Collection:

- What information do we collect? Names and contact details? Other information?
- How do we collect this information? Is it automatic?
- Why do we collect this information? Why do we need this information?
- Do we use cookies or web bugs?
- Does our internet server collect information of the individuals that browse our website? If so, what do we use this information for?

Use:

- How do we use this information?
- How and where do we store this information? Is any information stored overseas?
- Who has access to this information?

Disclosure:

- To whom do we disclose this information?
- Is it likely to be disclosed to anyone overseas and if so, in which countries?
- How will the information be used once it is disclosed?
- Will the people to whom we disclose the information use it in accordance with the principles of the Act? How do we ensure this?

Accessing and Correcting Information

- How can the Privacy Officer in our organisation be contacted (provide contact details)?
- What does a person do if they want to access or correct their personal information?
- What does a person do if they wish to complain that their privacy has been interfered with?
- How will we deal with such a complaint?

7.1 Privacy Officers

A Privacy Officer is someone in an organisation who has an understanding of the Privacy Act, the organisation's privacy policy and how it is implemented.

The Privacy Officer should:

- be contactable directly by anyone dealing with the organisation;
- provide contact details in the organisation's privacy policy;
- be responsible for ensuring that the organisation complies with the Privacy Act, which may involve the Privacy Officer reviewing customer databases and being involved in discussions with information technology service providers to ensure compliance; and
- be equipped to manage 'unsubscribe' requests from customers and respond to any complaints.

8. Complaints

If an individual considers that there has been a breach to his/her privacy, he/she has the right to complain to the Office of the Australian Information Commissioner. Most complaints are resolved by conciliation and the complainant must generally complain directly to the organisation first.

If conciliation is not successful, the Commissioner may order:

- enforceable undertakings;
- determinations – the Commissioner decides whether there has been a breach and can make an order accordingly; or
- injunctions and civil penalty orders if the Commissioner applies to the court.

The Information Commissioner also has the power to investigate an organisation of his/her own accord.

9. Further information

The Office of the Australian Information Commissioner (OIAC) provides a range of resources that give detailed guidance on the application of the *Privacy Act 1988* and Australian Privacy Principles:

- Guides for agencies and organisations on application of the *Privacy Act 1988*
- Quick guide to the APPs
- Extended APPs Guidelines

Further information on specific issues relevant to LPA Members:

- Organisations bound by the APPs
- Privacy law applicable in each state and territory jurisdiction
- Tips on protecting personal information
- Sending personal information overseas
- De-identification of data and information
- Dealing with requests for access to personal information
- Dealing with requests for correction of personal information
- Developing a Privacy Policy