Guide to compliance with the Australian Privacy Principles

This guide provides a summary of each of the Australian Privacy Principles (**APPs**) prescribed under the *Privacy Act 1988* (Cth), together with some practical tips on compliance with each APP.

This guide has been prepared by Norton Rose Fulbright Australia, in conjunction with CyberHound Pty Ltd, as a guide to assist schools bound by the *Privacy Act 1988* (Cth) to understand their obligations.

APP 1 – Open and transparent management of personal information

Summary of principle

APP 1 requires APP entities to manage personal information in an open and transparent way. This includes being required to:

- take reasonable steps to implement practices, procedures and systems relating to the organisation's functions or activities that will ensure compliance with the APPs (APP 1.2)
- have a clearly expressed and up-to-date privacy policy about the management of personal information (APP 1.3) that specifies:
    - the kinds of personal information collected
    - how personal information is collected and held
    - how an individual may seek access to personal information held by the entity or seek correction of such information
    - how an individual may complain about a breach of an APP and how the entity will deal with such a complaint
    - whether the entity is likely to disclose personal information to overseas recipients and if so, the countries in which such recipients are likely to be located, if it is practicable to specify those countries (APP 1.4)
- take reasonable steps to make its privacy policy available free of charge and in an appropriate form, such as on the organisation’s website (APP 1.5), and
- take reasonable steps to give a copy of the organisation’s privacy policy in a particular form, if requested by an individual or body (APP 1.6).

How to comply

In order to comply with APP 1, you must implement and publish a privacy policy that contains the mandatory required content listed above.

You must ensure that your privacy policy is readily available (preferably on your website) and you should also review your current internal policies and procedures, including the handling of privacy complaints, to ensure compliance with the APPs.

Where it is "practicable" to do, you must specify the foreign countries where you are likely to disclose personal information. We recommend specifying those countries in your privacy policy (and your collection statement). However, if the list of countries is impracticably long, you could, for example, insert a reference to a separate list of countries on your website.

APP 2 – Anonymity and pseudonymity

Summary of principle

APP 2 provides that individuals must have the option of dealing with an organisation anonymously or through the use of a pseudonym in relation to a particular matter unless:

- the organisation is required or authorised by or under an Australian law or a court/tribunal order to deal with individuals who have identified themselves, or
- it is impracticable for the organisation to deal with individuals who have not identified themselves.

How to comply

You will need to consider the interactions that you have with individuals and identify where these interactions could practically occur anonymously or under a pseudonym.

APP 3 – Collection of solicited personal information

Summary of principle

APP 3 applies to personal information solicited by an organisation. APP 3.2 provides that an organisation must not collect personal information unless the information is reasonably necessary for at least one of the entity's functions or activities.

APP 3.3 provides that an organisation must not collect sensitive information about an individual unless:

- the individual consents to the collection of the information, and
- the information is reasonably necessary for at least one of the entity's functions or activities.

APP 3.5 provides that an organisation must collect personal information only by lawful and fair means.

APP 3.6 states that an organisation must collect personal information about an individual only from the individual unless it is unreasonable or impracticable to do so.

How to comply

An important note here is that APP 3.2 states that an organisation is not to collect personal information unless it is "reasonably necessary". You will need to ensure that you collect the minimum amount of personal information necessary to achieve your purpose.

APP 3 clarifies that an organisation must only collect 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. You will need to carefully consider whether you need to collect sensitive information at all, and if so, how to satisfy the consent requirement.

APP 3.5 states that personal information must be collected "only by lawful and fair means". The Office of the Australian Information Commissioner (OAIC) suggests that the term 'fair' extends to the obligation not to use "unreasonably intrusive" means.

APP 4 – Dealing with unsolicited personal information

Summary of principle

Where an organisation receives personal information which it did not ask for, the entity must, within a reasonable period of time, determine whether it could have collected the information lawfully under APP 3 (if the entity had sought the information).

APP 4.2 allows an entity to use or disclose the personal information for the limited purpose of making this determination.

If the entity determines that the personal information could have been collected lawfully then the rest of the APPs apply as if the information had been collected in that manner. On the other hand, if the entity determines that the information could not have been collected lawfully, it must destroy the information or de-identify it where it is otherwise lawful to do so.

How to comply

You will need to ensure that you have new procedures in place for the handling and evaluation of any unsolicited personal information.

APP 5 – Notification of the collection of personal information

Summary of principle

APP 5.1 provides that either at or before the collection of personal information, an organisation must take reasonable steps to notify the individual, or otherwise ensure the individual is aware, of a number of matters set out at APP 5.2. If that timing is not practicable, the entity must do so as soon as practicable after the collection.

The relevant matters under APP 5.2 are:

- the organisation's identity and contact details
- if the organisation collects personal information from a third party, or the individual may not be aware that the entity has collected their personal information, the fact the entity so collects, or has collected, the information and the circumstances of collection
- the purposes for which the organisation collects the personal information
- the main consequences (if any) for the individual if all or some of the personal information is not collected by the organisation
- any other organisation, body or person, or the types of any other organisations, bodies or persons, to which the organisation usually discloses personal information of the kind collected by the entity
- that the organisation's privacy policy contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information
- that the organisation's privacy policy contains information about how the individual may complain about a breach of the APPs, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint
- whether the organisation is likely to disclose the personal information to overseas recipients, and
- if the organisation is likely to disclose the personal information to overseas recipients, the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

How to comply

You should develop a collection statement that can be readily provided to each individual from whom you collect personal information.

You will then need to implement a procedure for providing a collection statement to individuals when you first collect personal information, such as providing a copy of the collection statement or a link to a website containing the collection statement in the first email that you send to an individual (such as an acknowledgement email confirming that an account has been created or a query submitted via an online form).

APP 6 – Use or disclosure of personal information

Summary of principle

APP 6.1 provides that if an organisation holds personal information about an individual that was collected for the primary purpose, the entity must not use or disclose it for a secondary purpose unless:

- the individual has consented to the use or disclosure, or
- the use or disclosure of the information falls within the exceptions in APP 6.2.

APP 6.2(a) applies if the individual would reasonably expect the organisation to use or disclose the personal information for the secondary purpose and the secondary purpose is related to the primary purpose. APP 6.2(b) permits the use or disclosure of personal information if it is required or authorised by or under an Australian law or a court/tribunal order.

How to comply

You will need to review your privacy policies and procedures relating to the use of personal information to ensure you comply with the requirements of APP 6.

The Privacy Act contains an exemption which allows related bodies corporate to disclose personal information to each other. Section 13B of the Privacy Act permits the sharing of personal information (but not sensitive information) between related bodies corporate. Organisations sometimes share personal information and other data for a variety of reasons including central storage and processing of data for the company group. However, APP 6.6 provides that if an organisation receives personal information from a related body corporate, the primary purpose for which the information is collected is the same as the primary purpose for which the personal information was collected by the organisation that originally collected it. That is, the primary purpose is fixed and remains in place even after the disclosure of the personal information to the related body corporate.

APP 7 – Direct marketing

Summary of principle

APP 7 provides a regime for permitting use or disclosure of personal information for direct marketing purposes only if certain requirements are met. An organisation may not use or disclose personal information for the purpose of direct marketing unless APP 7.2 or APP 7.3 applies. If an organisation is permitted to use or disclose personal information under those APPs, the organisation must also comply with APPs 7.6, 7.7 and 7.8.

APP 7.2 provides that an organisation that holds personal information (other than sensitive information) about an individual must **not** use or disclose the information for the purpose of direct marketing unless each of the following applies:

- the organisation collected the information from the individual
- the individual would **reasonably expect** the organisation to use or disclose the information for that purpose
- the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications, and
- the individual has not made such a request to the organisation.

APP 7.3 provides that where an organisation collects personal information from an individual who would **not reasonably expect** the organisation to use or disclose the information for the purpose of direct marketing, or from someone other than the individual, the organisation may use that information for the purposes of direct marketing if each of the following applies:

- the individual has consented to the use or disclosure of the information for that purpose or it is impracticable to obtain this consent
- the organisation provides a simple way by which the individual may easily request not to receive the direct marketing communication
- in each direct marketing communication, the organisation includes a prominent statement that the individual may make a request not to receive the direct marketing communication or otherwise draws the individual's attention to the fact that he/she may make such a request, and
- the individual has not made such a request.

Under APP 7.6, if an organisation uses or discloses personal information about an individual:

- for the purpose of direct marketing by that organisation, the individual may request not to receive such communications from the first organisation, or
- for the purpose of facilitating direct marketing by other organisations, the individual may request the first organisation not to use or disclose their personal information for this purpose, and
- in either case, the individual may request the first organisation to provide its source of the information.

Under APP 7.7(a), if an individual makes a request under APP 7.6 in the circumstances above, the first organisation must give effect to the request without any charge and within a reasonable period of time. APP 7.7(b) also provides that for any request made by an individual relating to the source of the information, the first organisation must notify the individual of its source without any charge within a reasonable period of time, unless it is impracticable or unreasonable to do so.

How to comply

APP 7 prohibits direct marketing unless an exception applies.

APP 7 is subject to the operation of other direct marketing legislation, including the *Do Not Call Register Act 2006* (Cth) and the *Spam Act 2003* (Cth). As a result, APP 7 mostly relates to hard copy direct marketing materials.

Some organisations may find it impracticable to divide their customers and contacts into the two categories established by each of APP 7.2 and 7.3 and to then produce two different forms of direct marketing materials. If so, a simpler (if less desirable) solution may be to ensure that all direct marketing materials contain the opt-out statement required under APP 7.3.

APP 8 – Cross-border disclosure of personal information

Summary of principle

Under APP 8.1, before an organisation **discloses** personal information about an individual to an overseas recipient, it must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs in relation to the information.

However, APP 8.2 provides certain exceptions. APP 8.2 states that APP 8.1 will not apply to cross-border disclosures of personal information in the following circumstances:

- where the organisation reasonably believes that the overseas recipient of the information is subject to a law or binding scheme that has the effect of protecting the information in a substantially similar way in which the APPs protect the information, and there are mechanisms that the individuals can access to take action to enforce the law or binding scheme (**Substantially Similar Law Exception**), or

- where the individual consents to the disclosure after the organisation expressly informs the individual that, if the individual consents to the disclosure of information, APP 8.1 will not apply to the disclosure (**Informed Consent Exception**).

APP 8.1 permits cross-border disclosure of personal information, ensuring that any personal information disclosed is still treated in accordance with the Act.

How to comply

APP 8.1 and section 16C of the Privacy Act make an organisation accountable for the personal information it collects and stores, even if that information is stored by a third party outside Australia. Indeed, section 16C deems the organisation to be liable for acts and omissions of any overseas recipient to whom the organisation has disclosed personal information that would breach the APPs.

An important early consideration is whether the overseas recipient has an "Australian link" and is therefore independently subject to the Privacy Act. An overseas recipient will have an Australian link, and the APPs will apply to acts carried out outside Australia by it:

- if the person has Australian citizenship or permanent residence
- if the organisation is formed, created, or incorporated in Australia, or
- if the organisation was not formed, created or incorporated in Australia, it carries on business in Australia and the relevant personal information was collected or at any time held in Australia.

In many cases this may not be the case. It will therefore be necessary to systematically review the circumstances in which you disclose personal information to overseas recipients.

We recommend that you:

- review your privacy policy and your collection statement to ensure they cover the proposed disclosure and use of personal information by the overseas recipient (e.g. your overseas outsourcing service provider or cloud service provider). Amongst other things, your privacy policy and collection statement must specify (if practicable) the countries in which the personal information will be disclosed; and
- review the privacy provisions in your contract with the recipient to ensure that the provisions are not merely general but itemise key privacy obligations and contain appropriate warranties, audit rights and indemnities (particularly in respect of liability arising under section 16C of the Act).

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

Summary of principle

Organisations must not adopt a government related identifier (e.g. Medicare numbers or driver licence numbers) of an individual as its own identifier unless authorised under Australian law or court order.

The exceptions to this are set out in APP 9.2. The main exceptions where an organisation may adopt or use a government identifier are:

- where the use or disclosure of the identifier is reasonably necessary for an organisation to verify the identity of an individual for the purposes of its activities or functions
- to fulfil its obligations to an agency or a State or Territory organisation, or
- the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for enforcement related activities.

How to comply

The term 'government related identifier' includes State and Territory authorities to the list of entities that can assign government identifiers. The definition of identifier has also been expanded to include any combination of numbers, letters or symbols that can be used to identify an individual.

APP 9.1 contains an exception to permit the use of a government related identifier if permitted under an Australian law or court/tribunal order.

APP 9.2 also states that:

- a government identifier under the APPs can be used if it is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisations activities (APP 9.2(a))
- where the use or disclosure is required or authorised by a court/tribunal order (APP 9.2(c)), and
- where the use or disclosure is reasonably necessary for an enforcement related activity being conducted by or on behalf of an enforcement body (APP 9.2(e)).

APP 10 – Quality of personal information

Summary of principle

Organisations are required to take **reasonable steps** to ensure that any personal information that is held by them is kept accurate, up-to-date, complete and relevant.

APP 10 imposes slightly different obligations in respect of the quality of personal information for information that is collected, as opposed to information that is used or disclosed:

- APP 10.1 requires organisations to take reasonable steps to ensure that any personal information collected is accurate, up-to-date and complete, and
- APP 10.2 requires organisations to take reasonable steps to ensure that personal information that it uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

How to comply

APP 10 requires an organisation to take reasonable steps to ensure that the personal information it stores is accurate, up-to-date, complete (and relevant), so organisations will have to consider the quality of the personal information it has both at the time of collection and at the time of use of that information.

APP 11 – Security of personal information

Summary of principle

APP 11.1 requires organisations to take **reasonable steps** to protect personal information that they hold from misuse, interference, loss and unauthorised access, modification or disclosure.

Under APP 11.2, organisations must take reasonable steps to destroy or de-identify personal information if:

- the organisation no longer needs the information for any purpose for which the information may be lawfully used or disclosed, or
- the information is not otherwise required to be kept under an Australian law or court order.

APP 11 applies to any personal information held by an organisation, regardless of whether it collected that information.

How to comply

You need to ensure you review your data and document retention policies to ensure that you have steps in place to ensure that personal information that is no longer needed is either deleted or de-identified.

Personal information may be incorporated into various types of records and you should ensure that you comply with the record-keeping requirements for each type of record. Record-keeping requirements, also known as document retention requirements, usually set out a minimum period during which a type of record must be retained.

In April 2013, the OAIC released the *Guide to Information Security: Reasonable Steps to Protect Personal Information.* The Guide sets out what the OAIC considers to be "reasonable steps" in the protection of personal information as required under APP 11 and the Privacy Act in general. The Guide serves as a good starting point for considering your own organisation's security requirements.

According to the Guide, "reasonable steps" will vary depending on the particular circumstances surrounding the storage of personal information. However, the Guide sets out steps and strategies that the OAIC considers to be the minimum requirements for meeting a business' security obligations under the Privacy Act. The Guide can be found on the OAIC's website at oaic.gov.au.

In brief, the reasonable steps that organisations must take depend on circumstances including:

- the nature of the entity holding the personal information
- the nature and quantity of personal information held
- the risk to the individuals concerned if the personal information is not secured
- the data handling practices of the entity holding the information, and

- the ease with which a security measure can be implemented.

The actual reasonable steps to be taken can encompass all or any combination of matters such as governance (including security and breach response plans), ICT security (including software security, whitelisting and blacklisting entities, content or applications, access protocols, encryption, network security, testing and backups), physical security, personnel security and training, workplace policies, the information life cycle, complying with relevant standards and regular monitoring and review.

APP 11 relates to security of personal information. It is therefore appropriate to consider the legal requirements arising from any breach of security. In February 2018, new mandatory data breach notification provisions in the Privacy Act came into force. The provisions apply to data breaches regardless of whether the data breach arises from a failure to secure personal information in accordance with APP 11.1, or whether the breach was accidental or through intentional means such as hacking.

Organisations that suffer a data breach must quickly investigate the breach to determine whether there a risk of serious harm being caused to any individuals. If so, the organisation is likely to be required to notify affected individuals and the Privacy Commissioner.

APP 12 – Access to personal information

Summary of principle

APP 12.1 requires organisations that hold personal information about an individual to give the individual access to that information on request by that individual, unless an exception applies.

APP 12.3 sets out the relevant circumstances in which an organisation may refuse to give access to an individual to personal information that is held by it, including:

- the organisation reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety
- giving access would have an unreasonable impact on the privacy of other individuals
- the request for access is frivolous or vexatious
- the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings
- giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations
- giving access would be unlawful
- denying access is required or authorised by or under an Australian law or a court/tribunal order

- the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter
- giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body, or
- giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

APP 12.4 requires the organisation to respond to requests for access to personal information within a reasonable period and to give access to the information in the manner requested by the individual, if reasonable and practicable to do so. Even if the organisation refuses access on the basis of APP 12.3 or refuses to give access in the manner requested, APP 12.5 requires the organisation to take reasonable steps to give access in a way that meets the needs of the entity and the individual. APP 12.6 specifically provides that access may be given through the use of a mutually agreed intermediary.

APP 12.8 provides that an organisation may not impose any excessive charges for access and no charge may be applied to the making of the request for access.

APP 12.9 provides that where an individual's request for personal information is refused, the individual must be given written reasons for the refusal unless it would be unreasonable to do so and the individual must also be advised of the mechanisms available to complain about the refusal.

How to comply

You will need to put in place procedures to ensure that you can assess and respond to access requests in a timely manner. Receiving and responding to access requests is one of the typical tasks of an organisation's privacy officer, so you should consider appointing a dedicated privacy officer or allocating responsibilities for privacy-related queries to a particular person.

APP 13 – Correction of personal information

Summary of principle

An organisation must take reasonable steps to ensure that the personal information it collects and holds is correct.

APP 13.1 provides that an organisation must take reasonable steps to correct personal information that it holds to ensure that, having regard to the purpose for which the information is held, it is accurate, up-to-date, complete, relevant and not misleading where:

- the organisation is satisfied that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, or

- the individual whom the information is about requests the organisation to correct the information.

Under APP 13.2, if an organisation corrects an individual's personal information that it previously disclosed to another organisation and the individual requests the entity to notify the other organisation of the correction, the first organisation must take reasonable steps to notify the other organisation unless it is impracticable or unlawful to do so.

APP 13.3 provides that if an individual's amendment request is refused, the individual must be given written reasons for the refusal unless it would be unreasonable to do so. The individual must also be advised of the mechanisms available to complain about the refusal.

APP 13.4 provides that if an organisation refuses to correct an individual's personal information as requested by the individual and the individual requests the entity to associate the information with a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, the entity must take reasonable steps to associate the statement in a way that is apparent to users of the information.

APP 13.5 requires the organisation to respond to requests under APP 13.1 or 13.4 within a reasonable period and to not charge for making the request, correcting the personal information or associating the statement with the personal information.

How to comply

APP 13 does not require that an individual has to establish that their personal information is incorrect in order to have it corrected.

You need to review your privacy policy and procedures in order to ensure that you comply with the requirements of APP 13. In particular, you need to ensure that there is an established and documented procedure about how you will deal with requests for corrections (as well as access) and that you will take reasonable steps to notify third parties of any corrections to the personal information you collect and store. Again, this can be one of the responsibilities of a dedicated privacy officer or other nominated person.

