Legalwise Seminar

Commercial Law Conference
The Critical Issues

Thursday, 31 March, 2016

Privacy in a Commercial Context

Fred Chilton, Partner, and Sarah Heydon, Research Assistant

Emil Ford Lawyers
Sydney
March 2016

EMIL FORD
Lawyers

Introduction

This paper and the session to which it relates is not intended as an exhaustive treatment of Privacy Law in Australia, but instead attempts to alert practitioners to situations where the Privacy Act and the Australian privacy principles may be relevant.

Privacy Principles

The *Australian Privacy Act 1988* (Cth) (**Privacy Act**) is the pre-eminent Federal statute regulating the collection, storage, use and disclosure of personal and sensitive information concerning individuals. Schedule 1 of the Privacy Act contains the 13 Australian Privacy Principles (**APPs**) which must be complied with in the collection and management of an individual's personal information. They include:

1. Open and transparent management of personal information;
2. Anonymity and pseudonymity;
3. Collection of solicited personal information;
4. Dealing with unsolicited personal information;
5. Notification of the collection of personal information;
6. Use or disclosure of personal information;
7. Direct marketing;
8. Cross-border disclosure of personal information;
9. Adoption, use or disclosure of government related identifiers;
10. Quality of personal information;
11. Security of personal information;
12. Access to personal information; and
13. Correction of personal information.

Each APP in turn has a number of sub-clauses which spell out specific obligations. Attached to this paper as **Annexure A** is a copy of *Privacy Fact Sheet 17* issued by the Office of the Australian Information Commission (**OAIC**) which sets these out.

The APPs apply to both Commonwealth and Norfolk Island government agencies and private sector organisations, with some exceptions such as small business operators (annual turnover less than $3M). However, even small business operators may fall within the scope of the Privacy Act depending on their particular business (such as health care providers or credit reporting bodies).

The APPs commenced on 14 March 2014 as part of an amendment to the Privacy Act. They effectively converge the "Information Privacy Principles" and "National Privacy Principles" (**NPPs**) which were formerly applicable to Government agencies and private organisations respectively.

Privacy Policy

Every entity to which the Privacy Act applies, i.e. most companies and other business structures other than certain small businesses, must have a clearly expressed and up to date privacy policy about how that entity manages personal information. This is mandated by APP 1.3. APP 1.5 requires the policy to be made available free of charge in an appropriate form. For this reason, most entities usually make their privacy policies available on their websites.

As a lawyer, you may be called upon to draft a privacy policy, review a proposed privacy policy before its adoption or, in the context of an M&A transaction, review the privacy policy for any defects as part of due diligence. It is very important to understand the nature of the business and thus what sort of personal information it may need to collect and how it might use that information. Over the years I have seen many clients who simply download a privacy policy that some other entity has adopted on its website, change the names and upload it to their website as their own. This approach is fraught with danger as what might be relevant to one entity, may not be appropriate for another. In reviewing the policy, you should have regard to APP 1.4 to ensure that the policy covers the required information.

Collection of Personal Information

APP 3 requires the relevant entity to ensure that the collection of personal information is reasonably necessary for, or directly related to, its functions or activities and that such collection is undertaken only by lawful and fair processes. Similarly, APP 5 requires notice of the collection of such personal information to be given to the individual concerned. The decision of *'HW' and Freelancer International Pty Ltd* [2015] AlCmr 86 ('*Freelancer*') handed down last year by the OAIC considered collection issues in a commercial context. Since the APPs are still relatively new, this case was decided in the context of the NPPs. But there is a significant degree of overlap between the old NPPs and new APPs in respect of collection, so the case is worth considering.

The Freelancer Group, through its parent company (Freelancer International Pty Limited) and its subsidiaries controls and operates an online marketplace with global reach that operates through a core website, Freelancer.com, and 40 regional websites. The User Agreement for the Freelancer website sets out the terms and conditions on which users are permitted to use the website and Freelancer's services. On the website employers are allowed to post work they need to be done and anybody is able to offer quotes to complete the project. The employer is then able to award the work. Freelancer collects the personal information of buyers and sellers when they register as users of the website. HW had registered with the Freelancer website and was provided with an active user account. However, HW also set up two additional 'dummy' user accounts on the Freelancer website using 'dummy' email addresses (ones which he used for receipt of spam).

Freelancer then suspended HW's account and froze account funds. After issuing proof of his identity, the suspension of his account was lifted and the funds were released. However, when Freelancer was not satisfied with HW's answer as to why he had an operative user account and dummy accounts, his operative user account was suspended again. HW then posted a series of complaints, articles, blogs and comments online disparaging Freelancer. Freelancer responded by posting a series of critical comments online regarding HW, some of which HW argued came close to identifying him.

The findings of the OAIC speak to the importance of having a privacy policy in place. Because Freelancer's User Agreement and Privacy Policy did provide information to put users on notice that access to their accounts and/or funds could be limited in the event of suspected contravention of the Agreement's terms and conditions, the process of collection of this information was not 'unfair' or 'unreasonably intrusive' in terms of NPP 1.2 (which is equivalent to APP 3).

However, Freelancer's User Agreement and Privacy Policy did not specifically address the collection of IP addresses. Because HW was not aware that Freelancer used IP addresses for purposes of cyber security or fraud protection, the OAIC found that Freelancer had an obligation to take reasonable steps to make users of its website aware that other metadata such as IP addresses could be collected for risk management purposes. Consequently, Freelancer breached HW's privacy in this respect.

This decision goes to show just how important it is for entities, and their lawyers, when drafting privacy agreements to consider every process of collection of personal information the entity might undertake.

Use or Disclosure

APP 6 requires that the relevant entity must not use or disclose personal information unless an exception applies. The *Freelancer* case also demonstrates the important role a privacy policy can play in the context of use and disclosure of information. In that case, because the User Agreement and Privacy Policy made clear that Freelancer could close, suspend or limit access to a user's account if they carried out activities which were in contravention of the User Agreement and its associated policies, there was found to be no breach in relation to Freelancer's use of HW's IP address information.

With regard to disclosure, the *Freelancer* case is also instructive. Because Freelancer's User Agreement and Privacy Policy did not state that Freelancer customers should reasonably expect the personal information they provide or the personal information which Freelancer collects from publicly available sites to be published, Freelancer's disclosure was a breach of privacy. Many other disclosures made by Freelancer were also a breach of HW's privacy.

As previously mentioned, there are however exceptions to this principle. Interestingly, in the case of *'EZ' and 'EY'* [2015] AlCmr 23, none of the use or disclosure exceptions applied. In this case, the complainant contacted his local police station about a property dispute he was having with his neighbours. When a police officer arrived at the complainant's home, he found him in an overly excited and paranoid state. He admitted to suffering from various medical conditions. The police officer subsequently contacted the complainant's doctor and asked whether he was psychotic. The doctor responded that 'it was possible but further assessment was needed.' The complainant lodged a privacy complaint, alleging improper disclosure of his personal information, amongst other things.

Under one of the old NPPs exceptions, an organisation was allowed to disclose personal information to an enforcement body if they reasonably believed it was necessary for the purposes of preventing, detecting or investigating criminal or improper conduct. In this case it was held that although the doctor had been contacted by the police officer, a warrant had not been issued and the doctor had no reason to believe that the complainant had been involved in criminal or improper activity. Consequently, the doctor's disclosure was a breach of the complainant's privacy.

Although this is not a commercial case, it is worth considering what issues might arise if a lawyer disclosed personal information to a police officer in similar circumstances but in the context of the new APPs. APP 6.2(e) is closest to NPP 2.1(h). Although the new principle is less prescriptive than the old principle, in that it does not explicitly require a reasonable belief that criminal or improper behaviour is occurring, such a belief is still implicit in the new principle. No relevant health exceptions applied in the case either. It is therefore likely that this case would be decided in the same way if it concerned a lawyer, rather than a doctor.

A few principles can be distilled from the determination by the OAIC which would be helpful for lawyers, should they find themselves in a situation like this. Firstly, they should make enquiries with the police officer as to the nature of the circumstances that have led them to get in contact. Ask them why they want the information. Secondly, consider whether there is a warrant or whether there are legislative provisions that require the disclosure of personal information. Do not assume that the police have the authority to request the information. The Privacy Commissioner in this case said it was unfortunate that the police officer had put the doctor in this position in the first place, but this did not change the fact that the doctor had breached the complainant's privacy.

Privacy Due Diligence

As pointed out above, the first step in due diligence is to understand the nature of the target's business and, in particular, what information it might collect in the course of that business and how it might be used. The nature of the business will also dictate the extent to which compliance with the APPs may

be a major issue. For example, if the target is an e-commerce site marketing to individuals much like Freelancer, using personal information to undertake marketing, then it must make that clear to potential customers. If the target is part of an international group, then it is possible that information will be passed to related parties off-shore and may be processed off-shore. You will then need to ensure that there are contractual safeguards in place or the location of processing has equivalent standards of privacy protection (*see APP 8, in particular 8.1 and 8.2*). Even if the target is not an international group, it may well have entered into outsourcing arrangements, which involve processing of information off-shore.

If the target is involved in any way with health, then additional obligations will apply. If the target is a financial institution, there will be additional obligations relating to the provision of credit.

As part of due diligence, a lawyer would also need to review any compliance and monitoring policies and processes, whether there have been any releases of anonymised data and to whom, whether there has been compliance with the Spam Act and Do Not Call register and whether there have been any breaches of privacy and how have they been handled.

Terms and Conditions of Trade

Obligations under the Privacy Act will be relevant to many agreements which involve the provision of services. You would normally impose explicit obligations on the service provider to comply with the APPs, as well as other related Australian legislation, such as the Spam Act, the Credit Reporting Act and the Do Not Call Register, if applicable.

Protection

APP 11 requires the relevant entity to take reasonable steps to protect personal information from misuse, interference and loss and unauthorised access, modification or disclosure. In an age where data and personal information reside on computer systems, cyber security becomes extremely important. Most would have read of examples in recent times of success by hackers in penetrating an entity's systems and obtaining information. A more sinister use involves an on-sale of information in connection with identity theft. Sometimes it is simply a hacker obtaining access to passwords for credit cards, which can result in unauthorised use of an individual's credit card and potential financial exposure of the individual customer or, if covered by the card issuing entity, a cost to the entity as well as the inconvenience caused to customers in having to change passwords.

Cyber security is becoming more and more of an issue and an obligation of companies not just under the APPs, but more generally to protect customer information, as well as to notify customers when a breach of data security occurs. Many countries have legislated or are considering legislating, to deal with obligations of companies in relation to breaches of data security.

Increased Protection in the Future?

Despite the protections offered by APP 11, businesses that are subject to that principle are not subject to a mandatory data breach notification requirement under the Privacy Act. Against this background, on 30 November 2015, the Federal Government released an exposure draft of the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015* for public consultation. Under the provisions of the Bill, if an entity is aware, or ought reasonably to be aware, that there has been a serious data breach, the entity must notify each of the affected individuals and the Australian Information Commissioner. If it is not practicable to notify each of the affected individuals, the entity is required to publish a notice about the data breach on their website and take reasonable steps to publicise its contents. For the purposes of the Bill, a serious data breach occurs if there is unauthorised access to or disclosure of information and it results in a real risk of serious harm to the individuals concerned. Submissions closed on 4 March 2016.

Australia – Cloud Computing

The rapid spread and adoption of cloud computing raises a number of issues in the privacy context:

(a) Data including personal information about customers may be stored in the "cloud". The entity involved must ascertain the location of that storage and ensure that, if the cloud storage is located outside Australia, there has been compliance with APP 8, among others.

(b) Whilst data might be retained on an entity's own servers located in Australia, the entity may use SaaS (Software as a Service) where the software resides on a server outside Australia. This may involve the relevant software interacting with the entity's database to obtain and process personal information. Careful analysis will be required to understand the nature of the processing transaction and thus what, if any, additional steps need to be taken to comply with the APPs.

(c) Many cloud providers will provide backup services which may involve the data being replicated in a number of data centres, which may be located in different countries or even, for security, split and reassembled when access or processing occurs. Again, analysis of exactly what is happening with this data is required to ensure compliance.

(d) Most social media services are provided through a cloud based system. While the APPs will not apply to an individual uploading personal information such as family photos or videos on You-tube or similar, if a commercial entity takes and re-uses any of that personal information, then care must be taken that the relevant individual's consent has been obtained.

For example, there are a number of services that provide automated reviews of twitter strings. There could be circumstances where that service provides to a commercial customer details of negative tweets, for example.

Also, retweeting may involve the dissemination of personal information contained in the original tweet.

Big Data

New risks to privacy compliance arise with the use of advanced data mining and data analysis tools in connection with "Big Data". Examples have already arisen where supposedly anonymous de-identified data has been released by a government health department and subsequently re-identified so that it became personal information.

Privacy Governance

Boards of Directors of all companies (but especially publicly listed ones) are increasingly focussed on risk management and governance, which are important aspects of a Board's role.

Drafting and promulgation of appropriate policies and processes are only the first step. An appropriate privacy governance structure and adoption and application of review mechanisms are also necessary.

The Australian Information Commissioner, Timothy Pilgrim, is firmly of the view that "responsibility for privacy governance sits firmly with the CEO and the Board". (*Speech to IAPP ANZ, Sydney – 11 February, 2015*).

A number of high profile IT security incidents (e.g. in early February last year, it was reported that the Anthem health insurance data breach in the US resulted in the personal information of 80 million customers being unencrypted and vulnerable to unauthorised access), which can have a great impact on business continuity and a company's reputation, have led to c-suite executives being held accountable for IT and data security.

Mr Pilgrim calls for "a robust culture of accountability and governance". To assist companies to achieve this and to comply with APP 1.2, the OAIC has launched a Privacy Management Framework (**Framework**). The Framework has four steps. These are the steps an entity should take to ensure it practises good privacy governance and meets its ongoing compliance obligations. Which commitments are implemented at each step, and who takes on these roles, will depend upon the particular circumstances of the relevant entity, including its size, resources and business model.

The first step is to **embed** a culture of privacy that enables compliance. The Framework lists seven practical examples to show what embedding a culture of privacy might look like. This might involve:

- employing staff specifically for the purpose of privacy management. This will be more applicable to entities of a larger size.

- adopting a 'privacy by design' approach.[1] This involves considering the foundational principles of privacy by design during every stage of a business project or whenever making a decision that involves personal information.

- introducing reporting processes that ensure senior management are regularly informed about privacy issues. Again, this commitment will be more fitting for a larger sized entity.

The second step is to **establish** robust and effective privacy processes. Again, the Framework lists nine practical examples to show what establishing robust and effective privacy practices, procedures and systems might look like. This might involve:

- developing and maintaining processes for the handling of personal information throughout its 'lifecycle' – that is, before collection, once it has been collected, while it is being held and once it is no longer required.

- integrating privacy into induction procedures and regular staff training programs.

- undertaking privacy impact assessments for business projects or decisions that involve new or changed personal information handling practices. This might occur when a new technology or management system is introduced.

The third step is for entities to **evaluate** their privacy processes to ensure continued effectiveness. This might involve:

- monitoring and reviewing privacy processes on a regular basis.

- documenting an entity's compliance with its privacy obligations by keeping records on privacy process reviews, breaches and complaints.

- creating avenues for both staff and customers to provide feedback on their experiences with the entity's privacy processes, such as a feedback form.

[1] https://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/

The last step is for entities to **enhance** their response to privacy issues. This might involve:

- using the results from the Step 3 evaluations to make changes in practices, procedures and systems to improve the privacy processes.

- monitoring and addressing new security risks and threats. An entity could sign up to the *Stay Smart Online Alert Service* and follow the processes it suggests for ensuring online security, such as implementing software updates and patches. This commitment has the added bonus of being suitable for an entity of any size.

Further practical examples are given in the Framework, which enable compliance and encourage good practice.

ECJ Safe Harbour Privacy Decision

On 6 October last year, the Court of Justice of the European Union (ECJ) handed down a decision concerning the transfer of personal information from the EU to the US.

By way of background, the EU Data Protection Directive provided that personal data could only be transferred to a non-EU country if the third country guaranteed a sufficient level of protection of the data. However, the US did not have a general data protection law that ensured such a level of protection of personal data transferred from the EU. Consequently, in 2000 the European Commission decided that personal data could be transferred to the US on the proviso that entities complied with specific safe harbour privacy principles. This was known as the US Safe Harbour Decision. This allowed US entities to self-certify that the implementation of their privacy principles was sufficient for EU purposes. The process of self-certification was readily adopted by over 4000 US companies, many of them global corporations such as Google and Amazon. The validity of this decision was brought into question in *Schrems v Facebook.* A user of Facebook (also one of the self-certified companies) argued that, as a result of the disclosures made in 2013 by Edward Snowden, US law and processes did not offer adequate protection against monitoring by law enforcement agencies of personal data transferred to the US.

The US Safe Harbour Decision was overturned by the ECJ. The surveillance conducted by US public authorities, especially the National Security Agency, influenced the ECJ's decision. Other factors which influenced the decision included the fact that:

- self-certification did not apply to US public authorities.

- domestic US law, as well the country's national security and public interest, was more important. Entities were obliged in the face of conflict between the EU and US requirements to disregard those of the EU.

- US public authorities were allowed to access personal data transferred from the EU in a way that went beyond what was actually necessary and proportionate to safeguard national security

- there were no administrative or judicial means of redress to ensure that those who had their personal data unfairly accessed could obtain rectification or other remedies.

Replacement System

This decision raised concerns in the business community particularly. Tech firms, for instance, were worried that new rules might restrict their ability to operate in both the EU and the US. As a result of such concerns, on 2 February 2016 a broad agreement for protecting personal information was reached between EU and US officials. The new framework is called the EU-US Privacy Shield. The agreement requires:

- companies handling and processing personal data from the EU to comply with stronger obligations. If companies fail to comply with privacy safeguards, they may be prohibited from making use of the data transfer agreement altogether.
- subjecting US authorities to strict safeguards and specific restrictions when they are accessing personal data for law enforcement and national security purposes. The US Office of the Director of National Intelligence must state in writing that the data of EU citizens will not be part of mass surveillance.
- heightened protection for EU citizens. If they think that their personal data has been misused or needs to be corrected or deleted, they will be able to challenge the US Department of Commerce and Federal Trade Commission by lodging a complaint with their local data protection agency. In addition, alternative dispute resolution processes will be available free of charge.
- a joint review of the terms of the agreement on an annual basis, with particular regard to national security. It will be undertaken by the European Commission and the US Department of Commerce with the help of other data protection authorities from both parties.

This agreement has been met with criticism from privacy advocates. Most have stated that a written guarantee from government officials that the data of EU citizens will not be part of mass surveillance is a weak safeguard. Others take issue with the fact that the agreement allows US companies to continue to store personal data on their servers in compliance with US rather than EU law.

However, the agreement has also been praised for allowing businesses to continue their work with the addition of a few more checks and balances.

Are there any implications for Australia?

The question remains whether the ECJ decision and the subsequent EU-US Privacy Shield agreement create any issues for data transfers to and from Australia? Neither creates any new issues, although they do highlight two issues that continue to pose a problem in Australian privacy law.

Firstly, the Privacy Act makes concessions for small businesses and with regard to employee records, as mentioned earlier. In this respect, Australian privacy laws may not ensure a sufficient level of protection of personal data transferred from the EU.

Secondly, although the problems arising from cloud-based data storage operations were previously discussed, the decision and agreement raise further questions here. For example, an Australian entity might rely on a US service provider that was self-certified under the Safe Harbour Decision and is not yet compliant with the EU-US Privacy Shield agreement. An organisation storing patient data files externally in the US would be an example. Such organisations may be impacted if the service provider makes use of US and EU servers.

Other than these two issues, the decision and agreement are unlikely to have an impact on the direct transfer of personal data from the EU to Australia. Transfers of data from Australia to foreign countries will continue to be regulated by APP 8 as previously mentioned.

Annexure A – Detailed Principles

Australian Government
Office of the Australian Information Commissioner

Privacy fact sheet 17

Australian Privacy Principles

January 2014

From 12 March 2014, the Australian Privacy Principles (APPs) will replace the National Privacy Principles and Information Privacy Principles and will apply to organisations, and Australian Government (and Norfolk Island Government) agencies.

This privacy fact sheet provides the text of the 13 APPs from Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, which amends the *Privacy Act 1988*. For the latest versions of these Acts visit the ComLaw website: www.comlaw.gov.au.

Part 1—Consideration of personal information privacy

Australian Privacy Principle 1—open and transparent management of personal information

1.1 The object of this principle is to ensure that APP entities manage personal information in an open and transparent way.

Compliance with the Australian Privacy Principles etc.

1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:

(a) will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and

(b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles or such a code.

APP Privacy policy

1.3 An APP entity must have a clearly expressed and up to date policy (the *APP privacy policy*) about the management of personal information by the entity.

1.4 Without limiting subclause 1.3, the APP privacy policy of the APP entity must contain the following information:

(a) the kinds of personal information that the entity collects and holds;

(b) how the entity collects and holds personal information;

(c) the purposes for which the entity collects, holds, uses and discloses personal information;

(d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;

(e) how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(f) whether the entity is likely to disclose personal information to overseas recipients;

(g) if the entity is likely to disclose 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 policy.

Availability of APP privacy policy etc.

1.5 An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available:

(a) free of charge; and

(b) in such form as is appropriate.

Note: An APP entity will usually make its APP privacy policy available on the entity's website.

1.6 If a person or body requests a copy of the APP privacy policy of an APP entity in a particular form, the entity must take such steps as are reasonable in the circumstances to give the person or body a copy in that form.

Australian Privacy Principle 2—anonymity and pseudonymity

2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

2.2 Subclause 2.1 does not apply if, in relation to that matter:

(a) the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or

(b) it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.

Part 2—Collection of personal information

Australian Privacy Principle 3—collection of solicited personal information

Personal information other than sensitive information

3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

3.2 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

Sensitive information

3.3 An APP entity must not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information and:

(i) if the entity is an agency—the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(ii) if the entity is an organisation—the information is reasonably necessary for one or more of the entity's functions or activities; or

(b) subclause 3.4 applies in relation to the information.

3.4 This subclause applies in relation to sensitive information about an individual if:

(a) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(b) a permitted general situation exists in relation to the collection of the information by the APP entity; or

(c) the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; or

(d) the APP entity is an enforcement body and the entity reasonably believes that:

(i) if the entity is the Immigration Department—the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or

(ii) otherwise—the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(e) the APP entity is a non-profit organisation and both of the following apply:

(i) the information relates to the activities of the organisation;

(ii) the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

Note: For *permitted general situation*, see section 16A. For *permitted health situation*, see section 16B.

Means of collection

3.5 An APP entity must collect personal information only by lawful and fair means.

3.6 An APP entity must collect personal information about an individual only from the individual unless:

(a) if the entity is an agency:

(i) the individual consents to the collection of the information from someone other than the individual; or

(ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or

(b) it is unreasonable or impracticable to do so.

Solicited personal information

3.7 This principle applies to the collection of personal information that is solicited by an APP entity.

Australian Privacy Principle 4—dealing with unsolicited personal information

4.1 If:

(a) an APP entity receives personal information; and

(b) the entity did not solicit the information;

the entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information.

4.2 The APP entity may use or disclose the personal information for the purposes of making the determination under subclause 4.1.

4.3 If:

(a) the APP entity determines that the entity could not have collected the personal information; and

(b) the information is not contained in a Commonwealth record;

the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

4.4 If subclause 4.3 does not apply in relation to the personal information, Australian Privacy Principles 5 to 13 apply in relation to the information as if the entity had collected the information under Australian Privacy Principle 3.

Australian Privacy Principle 5—notification of the collection of personal information

5.1 At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

(a) to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or

(b) to otherwise ensure that the individual is aware of any such matters.

5.2 The matters for the purposes of subclause 5.1 are as follows:

(a) the identity and contact details of the APP entity;

(b) if:

(i) the APP entity collects the personal information from someone other than the individual; or

(ii) the individual may not be aware that the APP entity has collected the personal information;

the fact that the entity so collects, or has collected, the information and the circumstances of that collection;

(c) if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order—the fact that the collection is so required

or authorised (including the name of the Australian law, or details of the court/ tribunal order, that requires or authorises the collection);

(d) the purposes for which the APP entity collects the personal information;

(e) the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;

(f) any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity;

(g) that the APP privacy policy of the APP entity 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;

(h) that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(i) whether the APP entity is likely to disclose the personal information to overseas recipients;

(j) if the APP entity 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.

Part 3—Dealing with personal information

Australian Privacy Principle 6—use or disclosure of personal information

Use or disclosure

6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless:

(a) the individual has consented to the use or disclosure of the information; or

(b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.

Note: Australian Privacy Principle 8 sets out requirements for the disclosure of personal information to a person who is not in Australia or an external Territory.

6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:

(a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:

(i) if the information is sensitive information—directly related to the primary purpose; or

(ii) if the information is not sensitive information—related to the primary purpose; or

(b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or

(d) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or

(e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Note: For *permitted general situation*, see section 16A. For *permitted health situation*, see section 16B.

6.3 This subclause applies in relation to the disclosure of personal information about an individual by an APP entity that is an agency if:

(a) the agency is not an enforcement body; and

(b) the information is biometric information or biometric templates; and

(c) the recipient of the information is an enforcement body; and

(d) the disclosure is conducted in accordance with the guidelines made by the Commissioner for the purposes of this paragraph.

6.4 If:

(a) the APP entity is an organisation; and

(b) subsection 16B(2) applied in relation to the collection of the personal information by the entity;

the entity must take such steps as are reasonable in the circumstances to ensure that the information is de-identified before the entity discloses it in accordance with subclause 6.1 or 6.2.

Written note of use or disclosure

6.5 If an APP entity uses or discloses personal information in accordance with paragraph 6.2(e), the entity must make a written note of the use or disclosure.

Related bodies corporate

6.6 If:

(a) an APP entity is a body corporate; and

(b) the entity collects personal information from a related body corporate;

this principle applies as if the entity's primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.

Exceptions

6.7 This principle does not apply to the use or disclosure by an organisation of:

(a) personal information for the purpose of direct marketing; or

(b) government related identifiers.

Australian Privacy Principle 7—direct marketing

Direct marketing

7.1 If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Exceptions—personal information other than sensitive information

7.2 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

(a) the organisation collected the information from the individual; and

(b) the individual would reasonably expect the organisation to use or disclose the information for that purpose; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) the individual has not made such a request to the organisation.

7.3 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

(a) the organisation collected the information from:

(i) the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or

(ii) someone other than the individual; and

(b) either:

(i) the individual has consented to the use or disclosure of the information for that purpose; or

(ii) it is impracticable to obtain that consent; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) in each direct marketing communication with the individual:

(i) the organisation includes a prominent statement that the individual may make such a request; or

(ii) the organisation otherwise draws the individual's attention to the fact that the individual may make such a request; and

(e) the individual has not made such a request to the organisation.

Exception—sensitive information

7.4 Despite subclause 7.1, an organisation may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

Exception—contracted service providers

7.5 Despite subclause 7.1, an organisation may use or disclose personal information for the purpose of direct marketing if:

(a) the organisation is a contracted service provider for a Commonwealth contract; and

(b) the organisation collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract; and

(c) the use or disclosure is necessary to meet (directly or indirectly) such an obligation.

Individual may request not to receive direct marketing communications etc.

7.6 If an organisation (the first organisation) uses or discloses personal information about an individual:

(a) for the purpose of direct marketing by the first organisation; or

(b) for the purpose of facilitating direct marketing by other organisations;

the individual may:

(c) if paragraph (a) applies—request not to receive direct marketing communications from the first organisation; and

(d) if paragraph (b) applies—request the organisation not to use or disclose the information for the purpose referred to in that paragraph; and

(e) request the first organisation to provide its source of the information.

7.7 If an individual makes a request under subclause 7.6, the first organisation must not charge the individual for the making of, or to give effect to, the request and:

(a) if the request is of a kind referred to in paragraph 7.6(c) or (d)—the first organisation must give effect to the request within a reasonable period after the request is made; and

(b) if the request is of a kind referred to in paragraph 7.6(e)—the organisation must, within a reasonable period after the request is made, notify the individual of its source unless it is impracticable or unreasonable to do so.

Interaction with other legislation

7.8 This principle does not apply to the extent that any of the following apply:

(a) the *Do Not Call Register Act 2006*;

(b) the *Spam Act 2003*;

(c) any other Act of the Commonwealth, or a Norfolk Island enactment, prescribed by the regulations.

Australian Privacy Principle 8—cross-border disclosure of personal information

8.1 Before an APP entity discloses personal information about an individual to a person (the overseas recipient):

(a) who is not in Australia or an external Territory; and

(b) who is not the entity or the individual;

the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.

8.2 Subclause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:

(a) the entity reasonably believes that:

(i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and

(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

(b) both of the following apply:

(i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure;

(ii) after being so informed, the individual consents to the disclosure; or

(c) the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or

(e) the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or

(f) the entity is an agency and both of the following apply:

(i) the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;

(ii) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

Note: For *permitted general situation*, see section 16A.

Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers

Adoption of government related identifiers

9.1 An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless:

(a) the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(b) subclause 9.3 applies in relation to the adoption.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Use or disclosure of government related identifiers

9.2 An organisation must not use or disclose a government related identifier of an individual unless:

(a) the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions; or

(b) the use or disclosure of the identifier is reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or

(c) the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the identifier; or

(e) the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(f) subclause 9.3 applies in relation to the use or disclosure.

Note 1: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Note 2: For *permitted general situation*, see section 16A.

Regulations about adoption, use or disclosure

9.3 This subclause applies in relation to the adoption, use or disclosure by an organisation of a government related identifier of an individual if:

(a) the identifier is prescribed by the regulations; and

(b) the organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations; and

(c) the adoption, use or disclosure occurs in the circumstances prescribed by the regulations.

Note: There are prerequisites that must be satisfied before the matters mentioned in this subclause are prescribed, see subsections 100(2) and (3).

Part 4—Integrity of personal information

Australian Privacy Principle 10—quality of personal information

10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up to date and complete.

10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant.

Australian Privacy Principle 11—security of personal information

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

11.2 If:

(a) an APP entity holds personal information about an individual; and

(b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and

(c) the information is not contained in a Commonwealth record; and

(d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

Part 5—Access to, and correction of, personal information

Australian Privacy Principle 12—access to personal information

Access

12.1 If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

Exception to access—agency

12.2 If:

(a) the APP entity is an agency; and

(b) the entity is required or authorised to refuse to give the individual access to the personal information by or under:

(i) the Freedom of Information Act; or

(ii) any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents;

then, despite subclause 12.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access.

Exception to access—organisation

12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:

(a) the entity 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; or

(b) giving access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access is frivolous or vexatious; or

(d) 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; or

(e) 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; or

(f) giving access would be unlawful; or

(g) denying access is required or authorised by or under an Australian law or a court/tribunal order; or

(h) both of the following apply:

(i) 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;

(ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or

(i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(j) giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

Dealing with requests for access

12.4 The APP entity must:

(a) respond to the request for access to the personal information:

(i) if the entity is an agency—within 30 days after the request is made; or

(ii) if the entity is an organisation—within a reasonable period after the request is made; and

(b) give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

Other means of access

12.5 If the APP entity refuses:

(a) to give access to the personal information because of subclause 12.2 or 12.3; or

(b) to give access in the manner requested by the individual;

the entity must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the entity and the individual.

12.6 Without limiting subclause 12.5, access may be given through the use of a mutually agreed intermediary.

Access charges

12.7 If the APP entity is an agency, the entity must not charge the individual for the making of the request or for giving access to the personal information.

12.8 If:

(a) the APP entity is an organisation; and

(b) the entity charges the individual for giving access to the personal information;

the charge must not be excessive and must not apply to the making of the request.

Refusal to give access

12.9 If the APP entity refuses to give access to the personal information because of subclause 12.2 or 12.3, or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

12.10 If the APP entity refuses to give access to the personal information because of paragraph 12.3(j), the reasons for the refusal may include an explanation for the commercially sensitive decision.

Australian Privacy Principle 13—correction of personal information

Correction

13.1 If:

(a) an APP entity holds personal information about an individual; and

(b) either:

(i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or

(ii) the individual requests the entity to correct the information;

the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

Notification of correction to third parties

13.2 If:

(a) the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and

(b) the individual requests the entity to notify the other APP entity of the correction;

the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

Refusal to correct information

13.3 If the APP entity refuses to correct the personal information as requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

Request to associate a statement

13.4 If:

(a) the APP entity refuses to correct the personal information as requested by the individual; and

(b) the individual requests the entity to associate with the information a statement that the information is inaccurate, out of date, incomplete, irrelevant or misleading;

the entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

Dealing with requests

13.5 If a request is made under subclause 13.1 or 13.4, the APP entity:

(a) must respond to the request:

(i) if the entity is an agency—within 30 days after the request is made; or

(ii) if the entity is an organisation—within a reasonable period after the request is made; and

(b) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be).

The information provided in this fact sheet is of a general nature. It is not a substitute for legal advice.

For further information

telephone: 1300 363 992

email: enquiries@oaic.gov.au

write: GPO Box 5218, Sydney NSW 2001

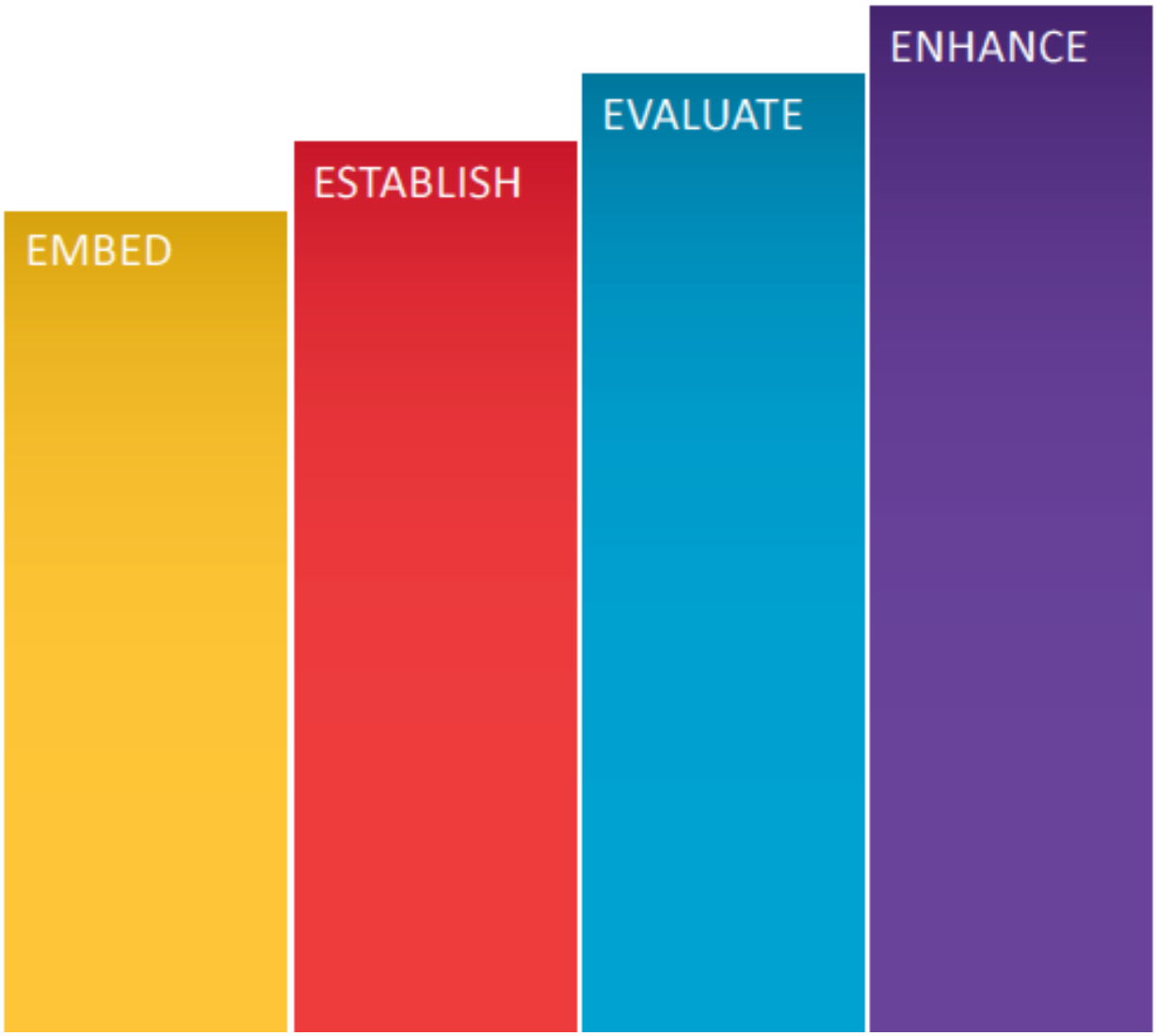
GPO Box 2999, Canberra ACT 2601

or visit our website at **www.oaic.gov.au**

Australian Government
Office of the Australian Information Commissioner

Privacy management framework:

enabling compliance and encouraging good practice



INTRODUCTION

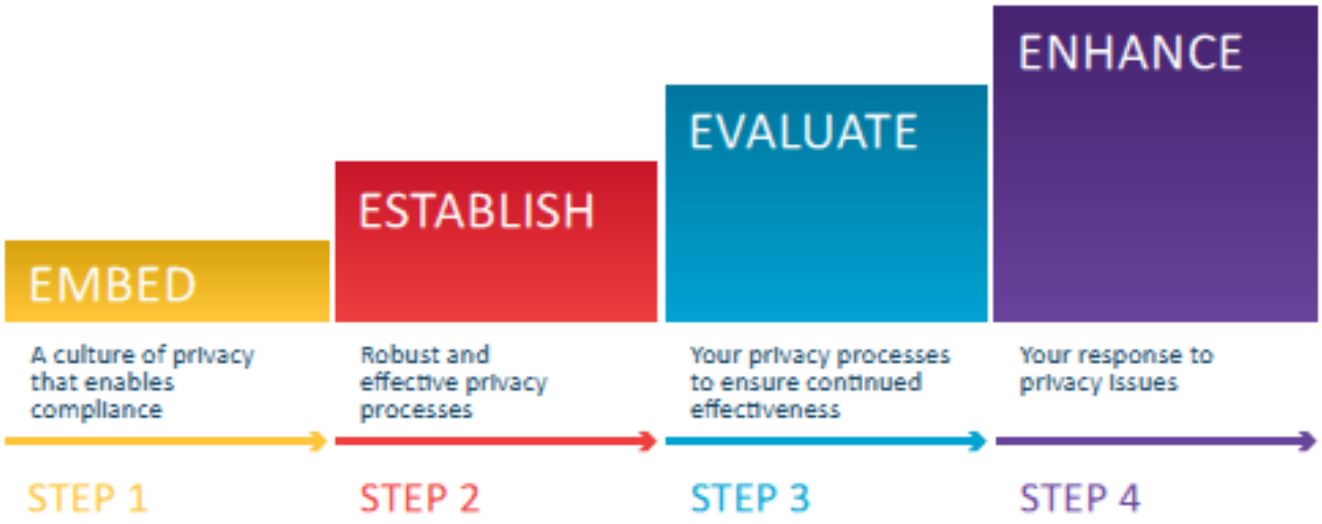
This *Privacy management framework* (Framework) provides steps the Office of the Australian Information Commissioner (OAIC) expects you to take to meet your ongoing compliance obligations under Australian Privacy Principle (APP) 1.2.

APP 1 ensures that personal information is managed in an open and transparent way. APP 1.2 requires you to take reasonable steps to implement practices, procedures and systems that ensure compliance with the APPs. This means that you must be proactive in establishing, implementing and maintaining privacy processes. Compliance with APP 1.2 should be understood as a matter of good governance.

A leadership commitment to a culture of privacy is a foundation for good privacy governance. Good privacy governance can improve business productivity and help to develop more efficient business processes. Good privacy governance will also help you manage both the risk of a privacy breach and your response should one occur.

Personal information is one of your most valuable business assets. By embedding a culture that respects privacy, you will build a reputation for strong and effective privacy management that will inspire trust and confidence in your entity.

The Framework has four steps. These are the steps you should take to ensure you practice good privacy governance and meet your ongoing compliance obligations. Which commitments you implement within each step, and who performs these, will depend upon your particular circumstances, including your entity's size, resources and business model.



STEP 1: EMBED

A culture of privacy that enables compliance

Good privacy management stems from good privacy governance. Ensure your leadership and governance arrangements create a culture of privacy that values personal information.

To embed a culture of privacy, make a commitment to:

- treat personal information as a valuable business asset to be respected, managed and protected. Outline how protecting personal information is important for your business
- appoint key roles and responsibilities for privacy management, including a senior member of staff with overall accountability for privacy. Also have staff responsible for managing privacy, including a key privacy officer, who are responsible for handling internal and external privacy enquiries, complaints, and access and correction requests
- adopt a 'privacy by design' approach. Ensure you consider the seven foundational principles of privacy by design in all your business projects and decisions that involve personal information
- allocate resources to support the development and implementation of a privacy management plan that aligns your business processes with your privacy obligations. Your plan should outline how you will implement and monitor the steps outlined in this Framework, and meet your goals or objectives for managing privacy
- implement reporting mechanisms that ensure senior management are routinely informed about privacy issues
- understand your privacy obligations. The *APP guidelines* provide guidance on how the OAIC will interpret the APPs and what matters it may take into account when exercising its functions and powers
- understand the role of the OAIC. The *Privacy regulatory action policy* explains the OAIC's approach to using its privacy regulatory powers and how it will communicate information.

STEP 2: ESTABLISH

Robust and effective privacy practices, procedures and systems

Good privacy management requires the development and implementation of robust and effective practices, procedures and systems.

To establish good privacy practices, procedures and systems, make a commitment to:

- keep information about your business's personal information holdings (including the type of information you hold and where it is held) up to date. This includes information held off-shore, or that is in the physical possession of a third party
- develop and maintain processes to ensure you're handling personal information in accordance with your privacy obligations. Ensure these processes:
  - address the handling of information throughout the information lifecycle — prior to collection, once personal information has been collected, while you hold it and once it is no longer needed. Ensure additional consideration is given to areas you assess as having greater risk, including sensitive information and use of service providers, contractors, outsourcing arrangements and off shore storage
  - clearly outline how staff are expected to handle personal information in their everyday duties. Tailor these processes to align with the different needs of different parts of your business, and how they use personal information
- promote privacy awareness within your entity by integrating privacy into your induction and regular staff training programs (including short term staff, service providers and contractors). This should include training staff on their privacy obligations and your processes. The OAIC has a number of training resources to help you with this
- develop and implement a clearly expressed and up to date privacy policy. Ensure your privacy notices are also up to date and consistent with your privacy policy. The *Guide to developing an APP privacy policy* provides tips and a checklist to help you develop and assess your privacy policy
- implement risk management processes that allow you to identify, assess and manage privacy risks across your business, including personal information security risks. The *Guide to securing personal information* provides steps and strategies you should consider taking to protect personal information, including privacy impact assessments, information security risk assessments and regular reviews of your personal information security controls
- undertake privacy impact assessments for business projects or decisions that involve new or changed personal information handling practices (including implementing new technologies). The *Guide to undertaking privacy impact assessments* includes information on threshold assessments, which will help you determine whether a privacy impact assessment is necessary
- establish processes for receiving and responding to privacy enquiries and complaints. The *Handling privacy complaints* resource provides information to help you address a privacy complaint
- establish processes that allow individuals to promptly and easily access and correct their personal information
- develop a data breach response plan. The *Data breach notification — A guide to handling personal information security breaches* provides guidance to assist you respond effectively to data breaches.

STEP 3: EVALUATE

Your privacy practices, procedures and systems to ensure continued effectiveness

Systematically examine the effectiveness and appropriateness of your privacy practices, procedures and systems to ensure they remain effective and appropriate.

To evaluate your privacy practices, procedures and systems, make a commitment to:

- monitor and review your privacy processes regularly. This could include assessing the adequacy and currency of your practices, procedures and systems, including your privacy policy and privacy notices, to ensure they are up to date and being adhered to
- document your compliance with your privacy obligations, including keeping records on privacy process reviews, breaches and complaints. Ensure senior management and those with responsibility for privacy management are briefed on risks or issues identified
- measure your performance against your privacy management plan. Regularly review your implementation of this Framework and your progress towards your objectives or goals
- create channels for both your staff and customers to provide feedback on your privacy processes, such as a suggestion box and feedback form.

STEP 4: ENHANCE

Your response to privacy issues

Good privacy management requires you to be proactive, forward thinking and to anticipate future challenges. By continually improving your privacy processes, you will ensure you are responsive to new privacy issues and that implementation will not be a burden.

To enhance your response to privacy issues, make a commitment to:

- use the results of your Step 3 evaluations to make changes to your practices, procedures and systems that improve your privacy processes. Track the performance of any new measures you implement
- consider having your privacy processes externally assessed to identify areas for improvement
- consider adopting good privacy practices that go beyond the requirements of the APPs, where appropriate. The *APP guidelines* and other OAIC resources provide examples of good privacy practices
- keep informed of issues and developments in privacy law and changing legal obligations. Subscribe to the OAIC's news email list OAICnet for updates and participate in privacy seminars, including the OAIC's webinars
- monitor and address new security risks and threats. Subscribe to Stay Smart Online Alert Service and follow the steps it suggests for ensuring online security, including implementing software updates and patches. The Australian Cyber Security Centre and CERT Australia provide guidance on cyber security issues
- examine and address the privacy implications, risks and benefits of new technologies. Consider implementing privacy enhancing technologies that allow you to minimise and better manage the personal information you handle
- introduce initiatives that promote good privacy standards in your business practices. Highlight examples of good personal information handling so that your staff know what is expected of them
- participate in Privacy Awareness Week and other privacy events. By bringing privacy into the spotlight, you will ensure your staff remain privacy aware.

Office of the Australian Information Commissioner

GPO Box 5218 Sydney NSW 2001
enquiries line: 1300 363 992
email: enquiries@oaic.gov.au

www.oaic.gov.au