Chapter 1: Australian Privacy Principle 1 — Open and transparent management of personal information

Version 1.0, February 2014

Key points

- APP 1 outlines the requirements for an APP entity to manage personal information in an open and transparent way.
- An APP entity must take reasonable steps to implement practices, procedures and systems that will ensure it complies with the APPs and any binding registered APP code, and is able to deal with related inquiries and complaints.
- An APP entity must have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information.
- An APP entity must take reasonable steps to make its APP Privacy Policy available free of charge and in an appropriate form (usually on its website).
- An APP entity must, upon request, take reasonable steps to provide a person or body with a copy of its APP Privacy Policy in the particular form requested.

What does APP 1 say?

1.1 The declared object of APP 1 is 'to ensure that APP entities manage personal information in an open and transparent way' (APP 1.1). This enhances the accountability of APP entities for their personal information handling practices and can build community trust and confidence in those practices.

1.2 APP 1 imposes three separate obligations upon an APP entity to:

- take reasonable steps to implement practices, procedures and systems that will ensure the entity complies with the APPs and any binding registered APP code, and is able to deal with related inquiries and complaints (APP 1.2)
- have a clearly expressed and up-to-date APP Privacy Policy about how the entity manages personal information (APP 1.3 and 1.4)
- take reasonable steps to make its APP Privacy Policy available free of charge in an appropriate form (APP 1.5) and, upon request, in a particular form (APP 1.6).

1.3 APP 1 lays down the first step in the information lifecycle – planning and explaining how personal information will be handled before it is collected. APP entities will be better placed to meet their privacy obligations under the Privacy Act if they embed privacy protections in the design of their information handling practices.

Implementing practices, procedures and systems to ensure APP compliance

1.4 APP 1.2 requires an APP entity to take reasonable steps to implement practices, procedures and systems relating to the entity's functions or activities that will:

- ensure the entity complies with the APPs and any binding registered APP code (see Part IIIB), and

- enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the APPs or such a code.

1.5 APP 1.2 imposes a distinct and separate obligation upon an APP entity, in addition to being a general statement of its obligation to comply with other APPs. The purpose of APP 1.2 is to require an entity to take proactive steps to establish and maintain internal practices, procedures and systems that ensure compliance with the APPs. The obligation is a constant one. An entity could consider keeping a record of the steps taken to comply with APP 1.2, to demonstrate that personal information is managed in an open and transparent way.

1.6 The requirement to implement practices, procedures and systems is qualified by a 'reasonable steps' test. The reasonable steps that an APP entity should take will depend upon circumstances that include:

- the nature of the personal information held. More rigorous steps may be required as the amount and sensitivity of personal information handled by an APP entity increases
- the possible adverse consequences for an individual if their personal information is not handled as required by the APPs. More rigorous steps may be required as the risk of adversity increases
- the nature of the APP entity. Relevant considerations include an entity's size, resources and its business model. For example, the reasonable steps expected of an entity that operates through franchises or dealerships, or gives database and network access to contractors, may differ from the reasonable steps required of a centralised entity
- the practicability, including time and cost involved. A 'reasonable steps' test recognises that privacy protection must be viewed in the context of the practical options available to an APP entity. However, an entity is not excused from implementing particular practices, procedures or systems by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances.

1.7 The following are given as examples of practices, procedures and systems that an APP entity should consider implementing:

- procedures for identifying and managing privacy risks at each stage of the information lifecycle, including collection, use, disclosure, storage, destruction or de-identification
- security systems for protecting personal information from misuse, interference and loss and from unauthorised access, modification or disclosure (such as IT systems, internal access controls and audit trails) (see also Chapter 11 (APP 11))
- a commitment to conducting a Privacy Impact Assessment (PIA) for new projects in which personal information will be handled, or when a change is proposed to information handling practices. Whether a PIA is appropriate will depend on a

project's size, complexity and scope, and the extent to which personal information will be collected, used or disclosed[1]

- procedures for identifying and responding to privacy breaches, handling access and correction requests and receiving and responding to complaints and inquiries[2]
- procedures that give individuals the option of not identifying themselves, or using a pseudonym, when dealing with the entity in particular circumstances (see also Chapter 2 (APP 2))
- governance mechanisms to ensure compliance with the APPs (such as designated privacy officers and regular reporting to the entity's governance body)
- regular staff training and information bulletins on how the APPs apply to the entity, and its practices, procedures and systems developed under APP 1.2
- appropriate supervision of staff regularly handling personal information, and reinforcement of the entity's APP 1.2 practices, procedures and systems
- mechanisms to ensure that agents and contractors in the service of, or acting on behalf of, the entity comply with the APPs
- a program of proactive review and audit of the adequacy and currency of the entity's APP Privacy Policy and of the practices, procedures and systems implemented under APP 1.2.

Developing an APP Privacy Policy

1.8 APP 1.3 requires an APP entity to have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information. At a minimum, a clearly expressed policy should be easy to understand (avoiding jargon, legalistic and in-house terms), easy to navigate, and only include information that is relevant to the management of personal information by the entity. As the policy will usually be available on the entity's website (see paragraph 1.36), it should be written in a style and length that makes it suitable for web publication.[3]

1.9 An APP entity should regularly review and update its APP Privacy Policy to ensure that it reflects the entity's information handling practices. This review could, at a minimum, be undertaken as part of an entity's annual planning processes. An entity could also:

- include a notation on the policy indicating when it was last updated
- invite comment on the policy to evaluate its effectiveness, and explain how any comments will be dealt with.

[1] Further information about Privacy Impact Assessments is contained in OAIC, *Privacy Impact Assessment Guide*, OAIC website <www.oaic.gov.au>.

[2] For example, see OAIC, *Data Breach Notification – A Guide to Handling Personal Information Security Breaches* (2013), OAIC website <www.oaic.gov.au>.

[3] The OAIC has developed a guide to help mobile device application (app) developers embed better privacy practices in their products and services, see OAIC, *Mobile Privacy: A Better Practice Guide for Mobile APP Developers*, OAIC website <www.oaic.gov.au>.

1.10 An APP Privacy Policy should explain how the APP entity manages the personal information it collects, and the information flows associated with that personal information. This reflects the central object of APP 1, which is to ensure that entities manage personal information in an open and transparent manner. The policy is not expected to contain detail about all the practices, procedures and systems adopted to ensure APP compliance. The policy also differs from a collection notice provided to an individual under APP 5.1, which will provide specific information relevant to a particular collection of personal information (see Chapter 5 (APP 5)).

1.11 It is open to an APP entity to choose the style and format for its APP Privacy Policy, so long as the policy is clearly expressed, up-to-date and otherwise complies with the requirements of APP 1.

1.12 Where an APP Privacy Policy is made available online, using a layered approach to the provision of the information may assist an individual's understanding of the information in the policy. A layered approach means providing a condensed version of the full policy to outline key information, with direct links to the more detailed information in the full policy.[4]

1.13 An APP Privacy Policy should be tailored to the specific information handling practices of an entity. For example, for a large APP entity where distinct business units handle personal information differently, it may be appropriate for the entity to have a set of policies to cover the different types of personal information handled or different information handling practices.

1.14 The APP Privacy Policy should be directed to the different audiences who may consult it. Primarily this will be individuals whose personal information is, or is likely to be, collected or held by the APP entity. If personal information relevant to particular classes of people or segments of the community is handled differently within the entity, this could be explained and signposted by headings. For example, different practices may be adopted in the entity for handling personal information relating to young people or people with a disability.

Information that must be included in an APP Privacy Policy

1.15 APP 1.4 contains a non-exhaustive list of information that an APP entity must include in its APP Privacy Policy:

- the kinds of personal information collected and held by the entity (APP 1.4(a))
- how personal information is collected and held (APP 1.4(b))
- the purposes for which personal information is collected, held, used and disclosed (APP 1.4(c))
- how an individual may access their personal information and seek its correction (APP 1.4(d))
- how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled (APP 1.4(e))

[4] For an example of a layered approach, see OAIC, *Summary of the OAIC's APP Privacy Policy*, OAIC website <www.oaic.gov.au>.

- whether the entity is likely to disclose personal information to overseas recipients (APP 1.4(f)), and if so, the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy (APP 1.4(g)).

1.16 Further guidance on each of these items is set out below.

Kinds of personal information collected and held

1.17 An APP Privacy Policy must describe in general terms the kinds of personal information an APP entity usually collects and holds (APP 1.4(a)). The terms 'collects' and 'holds' are discussed in Chapter B (Key concepts). For example, the policy may list personal information holdings as 'contact details', 'employment history', 'educational qualifications' and 'complaint details'.

1.18 'Sensitive information' collected or held by the entity could be separately listed ('sensitive information' is defined in s 6(1) and discussed in Chapter B (Key concepts)). For example, a policy may list sensitive information relating to 'health information about an individual', 'racial or ethnic origin', 'criminal records', 'religious affiliation' and 'political opinions.'

How personal information is collected and held

1.19 An APP Privacy Policy must explain an APP entity's usual approach to collecting personal information (APP 1.4(b)). For example, the policy may explain whether personal information is collected directly from individuals or from list purchases, competitions, or referrals from individuals or other entities.

1.20 The policy must describe an APP entity's usual approach to holding personal information. This should include how the entity stores and secures personal information. For example, the policy may explain that personal information is stored by a third party data storage provider, or is combined or linked to other information held about an individual. The description of security measures should not provide details that jeopardise the effectiveness of those measures.

Purposes for which the entity collects, holds, uses and discloses personal information

1.21 An APP Privacy Policy must describe the purposes for which personal information is usually collected, held, used and disclosed (APP 1.4(c)). An APP entity is not expected to publish details of purposes that form part of normal internal business practices, such as auditing, business planning, billing, and de-identifying personal information. The description of purposes could indicate the range of people or entities to which personal information is usually disclosed, and details about an entity's functions or activities that involve personal information that are contracted out. An organisation could also indicate if personal information is shared with a related body corporate.[5] Discussion of the terms 'purpose', 'collects', 'holds', 'uses' and 'discloses' is in Chapter B (Key concepts).

[5] Section 13B of the Privacy Act permits 'related bodies corporate' to share personal information in some circumstances. Related bodies corporate are discussed in Chapter B (Key concepts). The sharing of information between related bodies corporate is discussed in Chapter 3 (APP 3) and Chapter 6 (APP 6).

Accessing and seeking correction of personal information

1.22 An APP Privacy Policy must explain the procedure an individual can follow to gain access to or seek correction of personal information the APP entity holds (APP 1.4(d)). At a minimum, the policy should state:

- that individuals have a right to request access to their personal information and to request its correction (APPs 12 and 13), and
- the position title, telephone number, postal address and email address of a contact person for requests to access and correct personal information. An APP entity could establish a generic telephone number and email address that will not change with staff movements (for example privacy@agency.gov.au).[6]

1.23 If an APP entity wishes an individual to follow a particular procedure in requesting access to or correction of their personal information, the entity could publish that procedure and draw attention to it, for example, by providing a link in the entity's APP Privacy Policy. However, an APP entity cannot require the individual to follow a particular procedure to make the access or correction request (see Chapter 12 (APP 12) and Chapter 13 (APP 13)).

1.24 An agency's APP Privacy Policy could also refer to the *Freedom of Information Act 1982* (FOI Act) and explain that the access and correction requirements in the Privacy Act operate alongside and do not replace other informal or legal procedures by which an individual can be provided with access to, or correction of, their personal information, including the FOI Act (this is discussed in more detail in Chapter 12 (APP 12) and Chapter 13 (APP 13)).

Complaints about a breach of the APPs or a binding registered APP code

1.25 An APP Privacy Policy must explain how an individual can complain about an APP entity's breach of the APPs or a binding registered APP code (APP 1.4(e)). It is implicit in this requirement that an entity which is bound by a binding, registered APP code should clearly state that fact and name the code.

1.26 Details that should also be included in the APP Privacy Policy are the procedure and contact details for complaining directly to the APP entity (see for example, the generic contact details in paragraph 1.22) and, where applicable, the procedure for complaining to an external complaint body (such as an external dispute resolution scheme of which the entity is a member and that is recognised by the Information Commissioner).[7] The policy could inform individuals of the different stages in complaint handling: that a complaint should first be made in writing to the entity, as required by s 40(1A), and that the entity should be given a reasonable time (usually 30 days) to respond; the complaint may then be taken to a recognised external dispute resolution scheme of which the entity is a member; and lastly that the complaint may be taken to the OAIC.

[6] The OAIC has published guidance for agencies about developing their access to information webpages. This includes recommendations about adopting a new 'Access to information' icon. This guidance may assist agencies in developing online access and correction processes, which could then be explained in the APP Privacy Policy under APP 1.4(d). See OAIC, *Guidance for agency websites: 'Access to information' web page*, OAIC website <www.oaic.gov.au>.

[7] Further information about external dispute resolution schemes recognised by the Information Commissioner is available in OAIC*, Guidelines for recognising External Dispute Resolution Schemes*, OAIC website <www.oaic.gov.au>.

1.27 The policy could refer to other complaint avenues that operate alongside the Privacy Act. For example, banks are required to provide information to customers about complaint handling and dispute resolution in relation to the bank's obligations under the *Corporations Act 2001*, the Code of Banking Practice, and the Electronic Funds Transfer Code of Conduct. In these circumstances, the APP Privacy Policy could note the different procedures for privacy and non-privacy complaints (or link to other explanatory material the APP entity has published).

Likely overseas disclosures

1.28 An APP Privacy Policy must set out whether personal information is likely to be disclosed to overseas recipients and the countries in which such recipients are likely to be located 'if it is practicable to specify those countries in the policy' (APP 1.4(f) and 1.4(g)). This includes a likely disclosure to a related body corporate located overseas, and the country in which that body is located. An APP entity can be regarded as likely to disclose personal information to an overseas recipient if it is the entity's current practice or it has established plans to do so.

1.29 An APP entity is required to set out in the policy only likely disclosures of personal information to overseas recipients, and not likely uses of personal information by the entity. For example, routing personal information, in transit, through a server located outside Australia would usually be considered a 'use'.[8] Similarly, it would also be a use and not a disclosure for an entity to make personal information accessible to an overseas office of the entity, such as a consular office.[9] For further discussion of the requirements applying to a cross-border disclosure of personal information, and what is considered a disclosure, see Chapter 8 (APP 8).

1.30 An example of when it may be impracticable to specify the countries in which overseas recipients of personal information are likely to be located is where personal information is likely to be disclosed to numerous overseas recipients and the burden of determining where those recipients are likely to be located is excessively time-consuming, costly or inconvenient in all the circumstances. However, an APP entity is not excused from specifying the countries by reason only that it would be inconvenient, time-consuming or impose some cost to do so. As in other examples, it is the responsibility of the entity to be able to justify that this is impracticable.

1.31 If personal information is disclosed to numerous overseas locations, one practical option may be to list those countries in an appendix to the APP Privacy Policy rather than in the body of the policy. Another option in these circumstances may be to include a link in the APP Privacy Policy to a regularly updated list of those countries, accessible from the APP entity's website. Where it is not practicable to specify the countries, the entity could instead identify general regions (such as European Union countries).

1.32 This requirement to describe overseas disclosure practices in an APP Privacy Policy complements the obligation on an APP entity under APP 5.2(j) and (i) to notify an individual when personal information is being collected if the personal information is likely to be disclosed to overseas recipients and the location of those recipients (see Chapter 5 (APP 5)).

[8] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.
[9] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.

Other matters for inclusion in an APP Privacy Policy

1.33 The list of matters that must be included in an APP Privacy Policy, as discussed above, is not exhaustive. The policy should contain sufficient information to describe how the APP entity manages personal information.

1.34 The following are examples of other information that could be included:

- any exemptions under the Privacy Act that apply to personal information held by the entity or to any of its acts or practices
- whether the APP entity retains a record of personal information about all individuals (or categories of persons) with whom it deals
- who, other than the individual, can access personal information, and the conditions for access
- the entity's process or schedule for updating its APP Privacy Policy, and how changes will be publicised
- if the entity interacts with and collects personal information about a vulnerable segment of the community (such as children), the criteria that will be applied and the procedure that will be followed in collecting and holding that personal information
- the situations in which a person can deal with the entity by not identifying themselves or by using a pseudonym (see APP 2, Chapter 2)
- information retention or destruction practices or obligations that are specific to the entity.

Making an APP Privacy Policy publicly available

Making an APP Privacy Policy available free of charge and in an appropriate form

1.35 APP 1.5 requires an APP entity to take reasonable steps to make its APP Privacy Policy available free of charge, and in an appropriate form. This furthers the objective of APP 1 of ensuring that personal information is managed in an open and transparent way.

1.36 An APP entity is generally expected to make its policy available by publishing it on its website (see Note to APP 1.5). The information in the policy may be provided using a layered approach (see paragraph 1.12 above). The policy should be prominently displayed, accessible and easy to download. For example, a prominent link or privacy icon, displayed on each page of the entity's website, could provide a direct link to the APP Privacy Policy. If it is foreseeable that the policy may be accessed by individuals with special needs (such as individuals with a vision impairment, or individuals from a non-English speaking background), appropriate accessibility measures should be put in place. Agencies are also required to comply with any applicable government accessibility requirements.[10]

[10] See, for example, Australian Government, *Web Guide*, <webguide.gov.au/accessibility-usability/accessibility>.

1.37 Online publication may not be appropriate in some circumstances, for example, where the APP entity does not have an online presence or, where individuals who regularly interact with the entity may not have internet access. In these circumstances, options that an entity should consider include:

- displaying the policy on a stand at the entity's premises, so that it can be seen by members of the public
- distributing a printout of the policy on request
- including details about how to access the policy at the bottom of all correspondence to individuals
- where the entity interacts with individuals by telephone, informing them during the telephone call of how the policy may be accessed in a particular form.

Making an APP Privacy Policy available in a requested form

1.38 APP 1.6 requires an APP entity, upon request, to take reasonable steps to provide a person or body with a copy of its APP Privacy Policy in the form requested. This should be done as soon as reasonably practicable after the request is received.

1.39 The reference to a 'body' requesting a copy of a policy makes it clear that a request may be made other than by an individual or entity that is subject to the Privacy Act.

1.40 An APP entity can decline to provide a copy of its APP Privacy Policy in a particular form if it would not be reasonable in the circumstances to meet the request. The steps that are reasonable will depend upon:

- other steps taken by the entity to make its policy publicly available and accessible
- the practicability, including time and cost involved. However, an entity is not excused from providing a copy in a particular form by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances
- the sensitivity of the personal information held. More rigorous steps may be required where the entity holds 'sensitive information' (defined in s 6(1) and discussed in Chapter B (Key concepts)) or information of a sensitive nature
- whether the entity has unique or unusual information handling practices
- any reasons given by the body or person for requesting the policy in a particular form
- any special needs of the body or person requesting the policy. For example, it may be reasonable to provide the policy in a form that can be accessed via assistive technology where this meets the requester's special needs.

1.41 Inherent in the obligation to take 'reasonable steps' is an expectation that an APP Privacy Policy will usually be made available free of charge. The cost of doing so should be treated as part of an APP entity's normal operating costs. If a charge is imposed in special circumstances, the reason for the charge and the basis of calculation should be clearly communicated and explained before the policy is made available in the requested form, and the charge should be calculated at the lowest reasonable cost.

1.42 If a request for access in a particular form is declined, the APP entity should explain this decision to the person or body making the request. The entity should be prepared to undertake reasonable consultation with the requester about the request.