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

Chapter 1

Draft version, August 2013

Australian Privacy Principle 1 – Open and transparent management of personal information

Key points

- APP 1 outlines the steps an APP entity must take 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 APP entities 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, where requested, 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. In effect, APP 1 reflects a principle of 'privacy by design'. 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 of the Privacy Act), 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 APP entities, in addition to being a general statement of their obligation to comply with other APPs. The purpose of APP 1.2 is to require entities 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. Entities are advised to keep a record of the steps taken to comply with APP 1.2 to ensure that personal information is managed in an open and transparent way.

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

- the nature of the entity holding the personal information. 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 nature of the personal information held. Generally, as the quantity, extent and sensitivity of personal information handled by an APP entity increases, further steps may be required to protect the privacy of that information
- the adverse consequences for an individual if their personal information is not handled as required by the APPs. Generally, more rigorous steps may be required as the risk of adversity increases
- the practicability of implementing particular practices, procedures and systems to ensure compliance with the APPs. A 'reasonable steps' test recognises that privacy protection must be viewed in the context of the practical options available to an APP entity. On the other hand, an entity is not automatically excused from adopting appropriate information management practices, procedures and systems by relying on the inconvenience or cost of doing so.

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

- procedures for identifying and managing privacy risks at each stage of the information lifecycle, including collection, use, disclosure, storage, destruction and de-identification

- security systems for protecting information from misuse, interference and loss and from unauthorised access, modification or disclosure (such as IT systems, internal access controls and audit trails)
- a commitment to conducting a Privacy Impact Assessment for any new project in which personal information will be handled, or when a change is proposed to information handling practices[1]
- procedures for identifying and reporting privacy breaches and for 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 APP entity in particular circumstances
- 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
- a program of periodic review 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. A Note to APP 1.5 advises that the policy will usually be available on the entity's website. Accordingly, the policy should be written in a style and length that makes it easy to understand and suitable for web publication.

1.9 An APP Privacy Policy should explain how the entity manages the personal information it collects, and the information flows associated with that information. The policy is not expected to contain the level of detail that may be recorded under APP 1.2 about the practices, procedures and systems adopted to ensure APP compliance. The policy is also not required to contain the same level of detail as a collection notice provided to an individual under APP 5.1, which will provide more specific information relevant to a particular collection of personal information from the individual.

1.10 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.[3]

1.11 Where a 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

[1] Further information about Privacy Impact Assessments is contained in OAIC, *Privacy Impact Assessment Guide* (2010), <www.oaic.gov.au>.

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

[3] For more information about layered privacy policies see the ….

the policy. A layered approach means providing a condensed version of the full policy outlining key information from the full policy with direct links to the more detailed information in the full policy.[4]

1.12 An APP Privacy Policy should be tailored to the specific information handling practices of an entity. For example, the policy may explain how different categories of personal information are handled within the entity or by separate business or service units in the entity, and the different stages of the information lifecycle in the entity.

1.13 The 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 entity. If personal information relevant to particular classes of people or segments of the community is handled differently within the entity, this should be explained. For example, different practices may be adopted in the entity for handling personal information relating to young people or people with a disability.

1.14 These differences should be clearly signposted by headings or a separate discussion of issues. An APP Privacy Policy should be easy to navigate, clearly expressed, readable by a diverse community, and avoid jargon, in-house terms and legalistic expressions. The policy should reflect the central object of APP 1, which is ensuring that entities manage personal information in an open and transparent manner.

Information that must be included in an APP Privacy Policy

1.15 APP 1.4 contains a non-exhaustive list of information that an 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))
- 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)).

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

Kinds of personal information collected and held (APP 1.4(a))

1.16 An APP Privacy Policy must describe in general terms the kinds of personal information an entity usually collects and holds. For example, the policy may list personal

[4] For an example of a layered approach, see the Office of the Australian Information Commissioner Condensed Privacy Policy, <www.oaic.gov.au>

information holdings as 'contact details', 'employment history', 'educational qualifications', 'complaint details'.

1.17 'Sensitive information' collected or held by the entity should be separately listed ('sensitive information' is defined in s 6(1) and explained in Chapter B (Key concepts)). For example, a policy may list sensitive information relating to 'mental health', 'disability', 'racial or ethnic origin', 'criminal convictions', 'religious affiliation', 'political affiliation', and 'tax file numbers'.

How personal information is collected and held (APP 1.4(b))

1.18 An APP Privacy Policy must explain an entity's usual approach to collecting personal information. 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.

1.19 The policy must describe an entity's usual approach to holding personal information, including storing and securing 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 (APP 1.4(c))

1.20 An APP Privacy Policy must describe the purposes for which personal information is usually collected, held, used and disclosed. This description will usually indicate the range of people or entities that may access that personal information. (Discussion of 'purpose' , 'collects', 'holds', 'uses' and 'discloses' is in Chapter B (Key concepts).)

Accessing and seeking correction of personal information (APP 1.4(d))

1.21 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. At a minimum, the policy should state:

- that individuals have a right to request access to their personal information and to request its correction, under APPs 12 and 13 (see Chapters 12 (APP 12) and 13 (APP 13)), and
- the position title, telephone number and email address of a contact person for requests to access and correct personal information. Consideration should be given to establishing a generic telephone number and email address that will not change with staff movements (for example privacy@agency.gov.au).[5]

[5] 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>.

1.22 An agency's APP Privacy Policy could also explain whether requests for access to or correction of personal information should be made under the Privacy Act, the FOI Act or an administrative access arrangement the entity has established. (These alternative avenues for access and correction are discussed in Chapters 12 (APP 12) and 13 (APP 13).)

Complaints about a breach of the APPs or a binding registered APP code (APP 1.4(e))

1.23 An APP Privacy Policy must explain how an individual can complain about an entity's breach of the APPs or a binding registered APP code. Details that should be included are the procedure and contact details for complaining directly to the entity (see for example, the generic contact details in paragraph 1.20); and 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 or the OAIC).[6] The policy can inform people of the different stages in complaint handling: that a complaint should first be made in writing to the APP entity, as required by the Privacy Act 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.

1.24 The policy may 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 may note the different procedures for privacy and non-privacy complaints (or link to other explanatory material the entity has published).

Likely overseas disclosures (APP 1.4(f) and 1.4(g))

1.25 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.' This includes a likely disclosure to a related body corporate located overseas, and the country in which that body is located. The policy should note the kinds of personal information that are likely to be sent to particular countries.

1.26 The Privacy Act does not provide guidance on when it may be impracticable to specify the countries in which overseas recipients of personal information are likely to be located. A possible example is where personal information is likely to be disclosed to numerous overseas recipients and determining where those recipients are likely to be located is unduly costly. However, in that as in other examples, the onus will rest on the entity to explain why it is impracticable to list the countries.

1.27 If personal information is disclosed to numerous overseas locations, the more practical option may be to list those countries in an appendix to the APP Privacy Policy rather than in the body of the policy.

[6] Further information about external dispute resolution schemes recognised by the Commissioner is available in OAIC*, Guidelines for recognising External Dispute Resolution Schemes* (Note: these guidelines will be finalised prior to March 2014).

1.28 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 information is likely to be disclosed to overseas recipients and the location of those recipients. (Notification requirements are discussed in Chapter 5 (APP 5).)

Other matters for inclusion in an APP Privacy Policy

1.29 The list of matters that must be included in an APP Privacy Policy, as discussed above, is not exhaustive. Consideration should be given to including other details that more fully describe how an APP entity manages personal information.

1.30 Following are examples of other information that could be included:

- 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 period for which personal information records are kept – and, for agencies, the arrangements for transferring personal information records to the National Archives of Australia under a Records Disposal Authority
- the entity's process or schedule for updating its APP Privacy Policy, and how changes will be publicised
- if the APP 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 information
- the situations in which a person can deal with the APP entity by not identifying themselves or using a pseudonym (see Chapter 2 (APP 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 in an appropriate form

1.31 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.

1.32 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 1.11). The policy should be prominently displayed and be easy to access and download. 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.[7]

1.33 Different publication options may need to be considered where the APP entity does not have an online presence or, where individuals who regularly interact with the entity may not have internet access. Options may 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.

1.34 The expectation is that an entity's APP Privacy Policy should be available free of charge, in whatever form it is made available. However, in special circumstances a charge can be imposed consistently with the requirement of APP 1.5 that 'reasonable steps' be taken to make the policy freely accessible. If a charge is imposed, the reason for the charge and the basis of calculation should be clearly explained, and the charge should be calculated at the lowest reasonable cost. Making an APP Privacy Policy publicly available in an appropriate form should be treated as part of an APP entity's normal operating costs.

Making an APP Privacy Policy available in a requested form

1.35 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.

1.36 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.

1.37 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. For example, doing so may be unduly costly or unnecessary in light of other steps taken by the entity to make its policy publicly available and accessible. Before refusing a particular request, an entity should consider any reasons given by the body or person for requesting the policy in a particular form, any special need the requester may have to be given access in a particular form, whether the entity has unique or unusual information handling practices, and whether the nature, volume or sensitivity of the personal information held by the entity makes it appropriate that its policy is made available in additional forms.

1.38 Inherent in the obligation to take 'reasonable steps' is an expectation that a 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.

[7] See, for example, <http://webguide.gov.au/accessibility-usability/accessibility>.

1.39 If a request for access in a particular form is declined, or an access charge is imposed, 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. Any charge should be clearly communicated and explained before the policy is made available.