Australian Government

Office of the Australian Information Commissioner

Guide to developing an APP privacy policy

May 2014

Contents

Background

Australian Privacy Principle 1

Australian Privacy Principle (APP) 1.3 requires an APP entity[1] to have a clearly expressed and up-to-date APP privacy policy describing how it manages personal information.[2]

An APP privacy policy is a key tool for meeting APP 1's objective of ensuring that APP entities manage personal information in an open and transparent way (see APP 1.1).

The building blocks for developing an APP privacy policy are the 'practices, procedures and systems' that an APP entity must implement to ensure it complies with the APPs (see APP 1.2).

The specific requirements for an APP privacy policy are in:

- APP 1.4, which sets out the topics an APP privacy policy must cover
- APP 1.5, which requires an APP entity to take reasonable steps to make the privacy policy available free of charge and in an appropriate format
- APP 1.6, which requires an APP entity to take reasonable steps to give its privacy policy to an individual in the form the individual asks for.

The purpose of this Guide to developing an APP privacy policy

This Guide to developing an APP privacy policy (privacy policy guide) is designed to help APP entities prepare and maintain an APP privacy policy. It provides some tips and a process for developing a privacy policy.

We have also included a checklist to help you work out whether you have considered all the relevant aspects of developing an APP privacy policy and for your regular checks to make sure your policy remains up-to-date. [3]

This privacy policy guide is based on the APPs in the *Privacy Act 1988* (Privacy Act)[4] and the Office of the Australian Information Commissioner's (OAIC) *APP guidelines*.[5] You should read this privacy policy guide together with the full text of the APPs and the APP guidelines.[6]

Entities participating in the credit reporting system must have a privacy policy about their management of credit-related personal information. This privacy policy guide does not

[1] 'APP entity' is defined in s 6(1) of the *Privacy Act 1988* as 'an agency or organisation'. 'Organisation' is defined in s 6C of the Privacy Act.

[2] Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable.

[3] In this privacy policy guide where we say 'you' or 'your' we mean the organisation or agency which the privacy policy is being developed for.

[4] For the full text of the Australian Privacy Principles, see OAIC, *Privacy Fact Sheet 17: Australian Privacy Principles*, OAIC website <www.oaic.gov.au>, and *Privacy Act 1988*, Schedule 1, ComLaw website <www.comlaw.gov.au>.

[5] See OAIC, *Australian Privacy Principle guidelines*, OAIC website <www.oaic.gov.au>.

[6] See in particular, *Australian Privacy Principle guidelines*, Chapter 1: APP 1 — Open and transparent management of personal information, OAIC website <www.oaic.gov.au>.

specifically address credit reporting privacy policies. However, it will be a useful resource for organisations developing and maintaining such a privacy policy.

Tips

Although your APP privacy policy must cover all the topics mentioned in APP 1.4 (outlined in the checklist below), here are some tips to make it genuinely informative and manageable.

- **Think about your audience.** Don't treat the privacy policy as a legal document to manage legal risk. It should be a document that creates trust in your entity and speaks to your customers or clients
- **Don't just repeat the words in the APPs.** Make the privacy policy specific to your business or operation
- **Consult.** Seek input from all areas of your entity including your public relations department, which may have ideas about innovative formats for better communicating the policy, for example, through video or other mechanisms relevant to the communication channel (paper, telephone, email, online) that you are using
- **Focus on what is important to the reader.** Do not try to cover everything in minute detail
- **Keep it simple.** Use simple language and test readability in content and format against external standards such as the Flesch-Kincaid grade level[7]
- **Consider having more than one policy.** For large or complex entities, consider whether you need to have more than one policy (for different parts of your operation or business, or different functions or activities)
- **Take a layered approach.** For example, for online publication provide a condensed (summary version) of key matters in the privacy policy, with a link to the full policy
- **It is not an APP 5 notice.** The APP privacy policy is not meant to be a substitute for the notice requirements under APP 5. However, it may be used to help meet requirements in some circumstances. See APP Guidelines, Chapter 5: APP 5 — Notification of the collection of personal information, for further information on the interaction between an APP privacy policy and APP 5 notice.[8]

Steps in developing an APP privacy policy

Information gathering

The key to developing a privacy policy is to have an overview of the personal information held by your entity, as well as your personal information handling practices, procedures and systems. This will enable you to accurately describe (and summarise) how your entity currently handles personal information.

[7] For example, a quick online test is available at <readability-score.com>.
[8] OAIC website <www.oaic.gov.au>.

You may have some of this information already, or you may need to investigate. For example, you might need to do an audit and make a list of the personal information held by your entity, or develop policies and procedures if they are missing.

To be able to write a privacy policy you should be able to describe your entity's functions and activities and understand your entity's personal information handling procedures. More information on this below.

Describe your entity's functions and activities

You should be able to describe your entity's main functions and activities and identify those that involve personal information handling. For example:

- providing [specified] services
- conducting publicity campaigns
- handling complaints
- managing employee records
- running a website
- sending out a newsletter.

For each activity you should be able to describe:

- the personal information you collect and hold, and how you collect and hold it
- the reasons, or purposes for which you collect, hold, use and disclose that personal information, and
- whether you disclose personal information to overseas entities.

Understand your entity's personal information handling procedures

You should understand your entity's personal information handling practices, procedures and systems (written or otherwise), for the entity as a whole or for each of its key functions and activities including:

- specific approaches, principles or commitments your entity has decided to adopt for handling particular personal information. For example:
    - in relation to X process or collection, the entity will link personal information across business processes in all cases, or never do so, or only do so if the individual would expect it, or only with the individual's consent, or only if not sensitive information, or only for X purpose
    - the entity will never sell information about individuals to anyone else, or will only do so in particular circumstances
    - the entity will only disclose information overseas in X circumstances, or will never disclose information overseas
- processes for identifying, assessing and managing privacy and security risk, as well as developing and monitoring controls for those risks

- security protections (for example, encryption, audit and monitoring) you have in place (see APP 11.1), taking into account the guidance in the OAIC's Guide to Information Security[9]
- approaches to identifying and handling personal information your entity no longer needs:
    - in the case of an agency holding Commonwealth records, your practices under the *Archives Act 1983*
    - in the case of an organisation, your approach to destruction or de-identification of personal information (ideally identifying from these the specific periods that have been set for archiving, destruction or de-identification of personal information relating to the key functions and activities that individuals will be concerned about) (see APPs 4.3 and 11.2)
- processes for providing access to and correction of personal information (see APPs 12 and 13)
- complaints handling processes (see APP 1.4(d))
- policies relevant to your entity's personal information handling. For example, your approach to:
    - maintaining the quality of personal information that is used and disclosed (see APP 10)
    - anonymity or pseudonymity (see APP 2)
- policies for managing contractors when personal information may be disclosed.

You are not expected to include all this information in your entity's privacy policy, but it will enable you to identify what is going to be most important to your readers, and to work on what you should focus on in detail, and what you can accurately summarise.

Work out content and structure

Although the APP privacy policy must cover all the topics in APP 1.4 (outlined in the checklist below), the information does not have to be presented in that order — the goal is to make it as easy as possible for individuals to find the information that is most important to them.

Arrange information in a way that makes sense

You should arrange the information in a way that makes sense for your entity's functions, activities and audience. For example, you could separate out personal information flows for particular groups for whom your entity has different information handling practices (for example, staff, consumers/clients/members, service users, business relationships).

Where distinct sections or business units handle information in different ways you could consider having more than one privacy policy. If you do so, make the scope of each policy clear and, if practical, explain how each policy links to the others.

[9] See OAIC website <www.oaic.gov.au>.

Focus on what is likely to be most important to readers

Focus with more specific detail on the areas of personal information handling that individuals are:

- most concerned about, or may find objectionable (Why do you collect date of birth or age or health information? How are you going to protect it? Do you give or sell information about me to someone else without my knowledge or consent?)
- unaware of, won't reasonably expect, or may not understand easily (Do you collect information about me from public sources, or from third party list brokers? Do you track me when I use your website? If so, what do you use the information for? Can I interact with you anonymously or pseudonymously?).

Be as specific as possible

Be as specific as possible about how your entity handles personal information, as this will provide clarity and trust. Creating clarity will be most important in areas of common concern such as contact details, health information, financial information or other information of a sensitive nature. Unqualified use of vague words such as 'may' could lead to concern about uses and disclosures that are not intended.

Summarise where possible

Accurately summarise as much as possible in areas that:

- individuals know about already (for example, where they have provided personal information directly by filling out a form)
- individuals would expect as common business or administrative practice (for example, using an address for billing purposes or to enable a contractor to perform these services on behalf of the entity)
- are common across the entity for all personal information handling.

Provide information in layers

Take a layered approach to providing information about how your entity will handle personal information by providing a summary version that focuses on what the reader would like to know, with a link to the full APP privacy policy. [10] This will be particularly effective in the online environment.

Headings in the summary policy may vary according to the particular functions and activities of your entity, but often include:

- **Scope** — describes what the policy applies to

[10] For more information about taking a layered approach, see the Centre for Information Policy Leadership, *Ten steps to develop a multilayered privacy notice*, Centre for Information Policy Leadership website <www.informationpolicycentre.com>. For an example of a layered approach, see OAIC, *Privacy policy summary*, OAIC website <www.oaic.gov.au>.

- **Collection of personal information** — provides the key information about what personal information is collected and why. Focus on areas that are most sensitive or that the reader would least expect
- **Disclosure (sharing)** — describes the key disclosures and the conditions around those disclosures. This is a good place to mention overseas disclosures. Disclosures of personal information are usually the most important to individuals, but unexpected uses could be mentioned too
- **Rights and choices** — describes any key choices that individuals can make, including the right to request access and correction of personal information held about them
- **How to make a complaint** — briefly describes how to make a complaint about privacy and what to do if they are not satisfied with the outcome
- **Contact details** — including (at least) a generic telephone and email address that won't change with personnel.

Draft your privacy policy

Once you have a list of the personal information that your entity holds, as well as the other necessary information identified above, and have worked out the content and structure of your privacy policy, you can begin drafting.

Your privacy policy must be clearly expressed. To ensure the policy is accessible, easy to navigate and easy to read:

- use the active tense (you, we, I) and simple language — avoid legal jargon, acronyms, and in-house terms
- use short sentences and break up text into paragraphs
- use headings to help people find information easily, including information that may particularly apply to their situation or relationship with the entity
- keep in mind how you are going to publish it — if it is going on your entity's website, make sure it is in a form suited to online publication. For agencies, there are mandatory web accessibility standards[11]
- take into account your main audience in the design and format of the policy — for example, if your audience is likely to view the policy via a mobile app, or, conversely, to request a hard copy (see APP 1.6) you should create a policy that works effectively in that format
- avoid unnecessary length by giving careful consideration to what information is and is not needed in your policy
- only include information that is relevant to the way your entity handles personal information — don't include non-privacy related terms and conditions

[11] <https://www.dta.gov.au/standard/9-make-it-accessible/>

- ensure the policy is readable. You can test this by using external standards such as the Flesch-Kincaid grade level test.[12] You should try to keep the summary to no more than 500 words.

Test your privacy policy

Test out your privacy policy on the target audience or audiences, including likely readers. Where your resources are limited and systematic testing is not possible, having a family member or friend read it could give you some idea of how easy it is to read. Regardless of the target audience, it should be able to be easily read and understood by a 14 year old.

To ensure that your APP privacy policy covers all relevant topics and accurately reflects your entity's information handling practices, you could also test the summary and full policies with internal staff with personal information handling responsibilities.

Make your privacy policy easily available

APP 1.5 requires an entity to make its privacy policy available free of charge and in an appropriate form. If your entity has a website, you should publish it on your website.

APP 1.6 requires you to take reasonable steps to make your privacy policy available in the particular form a person asks for.

If you make your privacy policy available using a layered approach online, the first link to it should be to the summary. The summary should then have a prominent link to the full privacy policy. The privacy policy should be easy to download and accessible, including to people with a disability.

Regularly review and update your privacy policy

You should regularly review and update your privacy policy to ensure that it reflects your current personal information handling practices.

Does my entity's privacy policy comply with APP 1?

Below is a detailed checklist to help you work out whether you have considered everything while developing your privacy policy, as described above. It will also assist when you are undertaking your regular maintenance checks to make sure your privacy policy is up-to-date.

The issues and examples given describe some of the relevant issues in deciding whether your privacy policy meets the requirements of APP 1. However, they are not intended to be prescriptive or exhaustive — the particular circumstances of your entity will also be relevant.

For a more detailed discussion of the requirements of APP 1, as well as information about the OAIC's interpretation of the APPs and suggestions for good privacy practice, see Chapter 1 (APP 1) of the OAIC's APP guidelines.

[12] A quick online test is available at <readability-score.com>.

APP privacy policy checklist

APP 1.3—You must have a clearly expressed and up-to-date APP privacy policy about how you manage personal information

Issue	Yes/No	Comments
Management of personal information Does the policy explain how you manage personal information? For example, the policy: • covers the required topics under APP 1.4 • covers any other matters necessary in order to adequately describe how you manage personal information (some additional matters are described in the section on Other Matters below).		
Relevant Does the policy only include information that is relevant to how you manage personal information? For example, make sure the only terms and conditions that are included relate to privacy.		

Easy to understand
 	
Is the policy clearly expressed and understandable?
 	
For example:
 	
• a 14 year old would understand it
• it does not use
  o legalistic terminology
  o jargon
  o acronyms
  o in-house terms
• it uses short sentences and text broken up into paragraphs
• it meets external readability standards.		

Easy to find Is the policy easy to navigate so that people can find information that is relevant to them?		

Issue	Yes/No	Comments
For example, it: • has a summary notice that outlines the key points people will want to know about, with links to the full privacy policy (if online) • uses headings to make information easier to find.		
Specific Is the policy tailored to reflect your specific functions, activities and personal information handling practices? For example: • it is as specific as possible and does not use words such as 'may' • it is not simply based on a generalised template used by a different entity • it does not just repeat language in the APPs without providing further details. If you have distinct organisational areas that handle personal information differently, do you have a set of policies to cover the different personal information handled or the different practices?		
Tailored Is the policy directed to the specific audiences who may be reading it? For example, if you handle personal information differently for particular classes of people or segments of the community, such as young people, people with a disability, staff or applicants for employment, the policy: • uses headings to separate out information relevant to those particular audiences • uses language appropriate to the target audience • explains the different information handling practices relevant to the particular group.		
Review Has the policy been reviewed recently, to ensure that it reflects your current information handling practices? The policy could include a version number and date.		

APP 1.4—What information your APP privacy policy must cover

Issue	Yes/No	Comments
The kinds of personal information that you collect and hold. For example, the policy: • gives enough detail about the personal information that is collected and held • lists sensitive information separately, and gives more detail about the circumstances in which it is collected and held.		
How you collect personal information. For example, the policy describes: • the personal information that it usually collected directly and by what means (this can be in general terms) • the information collected indirectly and by what means (this could be in more detail, as people may not be aware of this collection and holding, for example collection by purchase from list brokers, competitions or referrals).		
How you hold personal information. For example, in relation to storage, the policy explains, if applicable: • if you store personal information with a third party storage provider • if you do or do not combine or link other personal information held about an individual. For example, in relation to security, the policy explains: • your approach to security and risk management • in broad terms, the measures you have in place to manage those risks, such as audit and monitoring of internal staff access to personal information.		
The purposes for which you collect, hold, use and disclose personal information. For example, the policy: • covers each of these topics for each of your key functions and activities involving personal information • focuses in most detail on the particular uses or disclosures that individuals are most likely to be concerned about or interested in,		

Issue	Yes/No	Comments
such as key disclosures to related companies • indicates the functions or activities for which you use contractors. The policy is not expected to describe normal internal operational or business practices such as billing, financial auditing or planning.		
How an individual may access their personal information and seek correction of it. For example, the policy: • states that individuals have a right to request access to personal information you hold about them • states that individuals have a right to request personal information to be corrected • gives contact details for individuals to make such requests which include: o position title of the contact person o a generic telephone number o postal address o a generic email address • includes information about any procedure that you wish an individual to follow in requesting access or correction (although you can't require the individual to follow that procedure). The policy of an agency could refer to processes for access and correction under the *Freedom of Information Act 1982*.		

Issue	Yes/No	Comments
How an individual may complain if you or a contractor breaches the APPs or a binding registered APP code. For example, the policy: • describes the process you use to handle complaints • describes the contact details for making a complaint • indicates that you are bound by a registered APP code, if applicable • outlines the process for complaining to an external complaint body, such as a recognised external dispute resolution scheme, if applicable • describes the different stages in the complaint-handling process: that the complaint must be made directly to you first, that the complaint may then be taken to a recognised external dispute resolution scheme (if applicable), and lastly, that the complaint may be taken to the OAIC.		

Whether you are likely to disclose personal information to overseas recipients (including a related body corporate), and the likely countries that information may be sent.
 	
For example, the policy:
 	
• lists the specific countries you are, or are likely to disclose personal information to (unless it is impractical to specify those countries in the policy)
• where impractical to list countries in the policy:
  o lists countries in an appendix or in another document to which the policy has a link, or
  o lists general regions, for example, the European Union.		

Other matters under APP 1.3

The list of matters that must be included in an APP privacy policy, as discussed above, is not exhaustive. In order to comply with APP 1.3, your policy should include enough information to describe how you manage personal information. This may mean that your privacy policy should cover additional topics.

Issue	Yes/No	Comments
If your functions or activities could have a major impact on an individual's privacy, but are exempt from some or all of the Privacy Act, the policy could outline: • the particular functions or activities that are exempt • the protections you have in place to protect the privacy of personal information, as related to those functions or activities.		
Whether you retain a record of personal information about all individuals (or categories of persons) with whom you deal. For example, if you do not collect any personal information from some of the individuals you deal with, or only anonymous information, the policy could outline these circumstances.		
If you hold information about individuals that is often accessed by people other than the individual themselves, for example, carers, or parents, or a law enforcement agency, the policy could outline: • the basis on which you will allow such access • the process to be followed for such access.		
If your information handling practices change frequently in ways that will importantly affect individuals, the policy could: • describe your process or schedule for updating your privacy policy • describe how the changes will be publicised.		
If you interact with and collect personal information about a vulnerable segment of the community (such as children), the policy could highlight: • the purpose of such collection • the specific circumstances in which you will collect, use and disclose such information • the procedures you follow in collecting, holding, using and disclosing the information.		
Particularly where it is possible for individuals to interact with you anonymously or pseudonymously, or where individuals may often ask not		

Issue	Yes/No	Comments
to be identified, the policy could describe: • the situations in which it is possible to be anonymous or pseudonymous • the situations in which it is not possible to be anonymous or pseudonymous and why.		
Particularly where you hold personal information of a sensitive nature or personal information that is likely to quickly go out of date, the policy could describe: • the specific practices you adopt to ensure the quality of the personal information • the destruction or de-identification period or approach to archiving of that personal information.		

APP 1.5—You must take reasonable steps to make the APP privacy policy available free of charge and in an appropriate form

Issue	Yes/No	Comments
Is the privacy policy available for free?		
Is the privacy policy available in an appropriate form? For example: • is it available on your website? • if you don't have a website, or have a significant group of customers who do not have access to the internet, do you: o display your policy at the entrance to your premises o include details about how to get a copy of the policy on your correspondence o provide a print out of the full policy on request o tell individuals via telephone message how they can access the policy when they call?		
If the privacy policy is published on your website, it is in a form appropriate for website publication? For example, it is: • easy to download • accessible, including to people with a disability: for agencies, in compliance with the Government website accessibility requirements at <www.webguide.gov.au/accessibility-usability/accessibility>.		

APP 1.6—You must take reasonable steps to provide the APP privacy policy in the form requested

Issue	Yes/No	Comments
Do you have steps in place to respond in a timely manner to requests for your privacy policy to be provided in a different format?		

For further information

telephone: 1300 363 992
email: enquiries@oaic.gov.au
write: GPO Box 5218, Sydney NSW 2001
Or visit our website at **www.oaic.gov.au**