Chapter 5: Australian Privacy Principle 5 — Notification of the collection of personal information

Version 1.1, March 2018

Key points

- An APP entity that collects personal information about an individual must take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters.
- The matters include:
    - the APP entity's identity and contact details
    - the fact and circumstances of collection
    - whether the collection is required or authorised by law
    - the purposes of collection
    - the consequences if personal information is not collected
    - the entity's usual disclosures of personal information of the kind collected by the entity
    - information about the entity's APP Privacy Policy
    - whether the entity is likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located.
- An APP entity must take reasonable steps, before, or at the time it collects personal information. If this is not practicable, reasonable steps must be taken as soon as practicable after collection.

What does APP 5 say?

5.1 APP 5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters (generally referred to in this chapter as 'APP 5 matters'). The term 'collects' is discussed in Chapter B (Key concepts). Reasonable steps must be taken at or before the time of collection, or as soon as practicable afterwards.

5.2 The requirement to notify or ensure awareness of the APP 5 matters applies to all personal information 'collected' about an individual, either directly from the individual or from a third party. It applies to solicited personal information (APP 3) and also unsolicited personal information that is not destroyed or de-identified by the APP entity (APP 4) (see Chapter 3 (APP 3), Chapter 4 (APP 4) and Chapter B (Key concepts)).

Taking reasonable steps to notify or ensure awareness

5.3 An APP entity must take reasonable steps either to notify an individual of the APP 5 matters or to ensure the individual is aware of those matters (APP 5.1).

5.4 The reasonable steps for an APP entity will depend upon circumstances that include:

- the sensitivity of the personal information collected. More rigorous steps may be required when collecting 'sensitive information' (defined in s 6(1) and discussed in Chapter B (Key concepts)) or information of a sensitive nature
- the possible adverse consequences for an individual as a result of the collection. More rigorous steps may be required as the risk of adversity increases
- any special needs of the individual. More rigorous steps may be required if personal information is collected from an individual from a non-English speaking background who may not readily understand the APP 5 matters
- the practicability, including time and cost involved. However, an entity is not excused from taking particular steps 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 particular steps will depend on whether the burden is excessive in all the circumstances.

5.5 An individual may be notified or made aware of APP 5 matters through a variety of formats, provided the matters are expressed clearly. A notice may be prepared in advance (paper, online, telephone script) and staff should be trained to understand their obligation to take reasonable steps to notify or ensure awareness under APP 5. A notice may also be provided in layers, from a full explanation to a brief refresher as individuals become more familiar with how the APP entity operates and how personal information is handled. Brief privacy notices on forms or signs may be supplemented by longer notices made available online or in brochures.

5.6 Examples of reasonable steps that an APP entity could consider taking to notify or ensure awareness of the APP 5 matters include:

- if the entity collects personal information directly from an individual who completes a form or uses an online facility, clearly and prominently displaying the APP 5 matters in the form, or providing a readily accessible and prominent link to an APP 5 notice
- if personal information is collected by telephone, explaining the APP 5 matters to the individual at the commencement of the call (perhaps following a template script or using an automated message). Where this is not practicable, an entity should give the individual information about the APP 5 matters as soon as possible afterwards, such as in any subsequent electronic or paper-based communication, or directing the individual to the relevant notice on the entity's website
- if the entity collects personal information from another entity, ensuring that the other entity has notified or made the individual aware of the relevant APP 5 matters on its behalf (such as through an enforceable contractual arrangement)
- where it is not reasonable to notify or ensure awareness of the full range of APP 5 matters, an entity could alert the individual to specific sections of its APP Privacy Policy (see Chapter 1 (APP 1)), such as parts of the Policy about likely overseas disclosures (APP 5.2(i)), or other general documents containing relevant

information.[1] However, before doing so the entity should consider whether information in the APP Privacy Policy sufficiently covers the APP 5 matters as they relate to the particular collection, as the APP Privacy Policy may describe only the general information handling practices of the entity.

When not taking any steps might be reasonable

5.7 APP 5.1 acknowledges that it may be reasonable for an APP entity to not take any steps to provide a notice or ensure awareness of all or some of the APP 5 matters. It is the responsibility of the entity to be able to justify not taking any steps. The following are given as examples of when this may be reasonable:

- the individual is aware that personal information is being collected, the purpose of collection and other APP 5 matters relating to the collection, for example, a doctor has informed a patient that a specialist to whom the patient is referred for treatment will obtain the patient's health information from the doctor
- an entity collects personal information from an individual on a recurring basis in relation to the same matter. However, if a long period of time has elapsed since the notice was provided and the individual may no longer be aware of the APP 5 matters, the entity may need to take steps to notify or ensure awareness. Similarly, if a change in circumstances as to how personal information is collected affects any of the APP 5 matters, the entity should take reasonable steps to ensure an individual is aware of those matters.
- notification may pose a serious threat to the life, health or safety of an individual or pose a threat to public health or safety, for example, a law enforcement agency obtaining personal information from a confidential source for the purpose of an investigation
- notification may jeopardise the purpose of collection or the integrity of the personal information collected and there is a clear public interest in the purpose of collection, for example, a law enforcement agency undertaking lawful covert surveillance of an individual in connection with a criminal investigation
- notification would be inconsistent with another legal obligation, for example, by breaching a statutory secrecy provision, a client's legal professional privilege, or a legal obligation of confidence
- an entity collects personal information about a person who poses (or is alleged to pose) a risk of committing family violence and this collection is permitted by a legislated family violence information sharing scheme, such as that established by the *Family Violence Protection Act 2008* (Vic)

[1] *See Tenants' Union of Queensland Inc, Tenants' Union of NSW Co-op Ltd v TICA Default Tenancy Control Pty Ltd* [2004] PrivCmrACD 4 (16 April 2004) [80], [82], which states 'if an organisation provides the information required to meet its obligations on different forms or in different locations it would generally need to alert individuals to the fact the other information was available…it should [also] seek to ensure that there are appropriate references to that information in the primary form'.

- the impracticability of notification, including the time and cost, outweighs the privacy benefit of notification. For example:
    - where an entity collects personal information about the individual's next of kin for emergency contact purposes, it would generally be reasonable for the entity to take no steps to notify the next of kin of the collection of their personal information
    - where an individual provides unsolicited personal information to an entity about a third party for the purposes of a confidential alternative dispute resolution process, and the entity is not required to destroy or de-identify the information under APP 4 (see Chapter 4), it would generally be reasonable for the entity to take no steps to notify the third party. This is especially so where the entity will not rely on the personal information in investigating or resolving the matter, or does not have the contact details of the third party.

Matters about which an individual must be notified or made aware

5.8 APP 5.2 lists the matters (discussed separately below) that must be notified to an individual or of which they must be made aware. For each matter, an APP entity must consider whether notifying the individual is reasonable in the circumstances. This means that it may be reasonable for an entity to notify some but not all of the APP 5 matters. For example, it may be reasonable not to notify an individual of the collecting entity's identity where this is obvious from the circumstances.

The APP entity's identity and contact details

5.9 The matter set out in APP 5.2(a) is the identity and contact details of the APP entity. This could include the position title, telephone number and email address of a contact who handles enquiries and requests relating to the Privacy Act. Consideration could also be given to establishing a generic telephone number and email address (for example, privacy@agency.gov.au) that will not change with staff movements. This ensures awareness of a contact if an individual chooses to exercise any available rights such as to request access to, or correction of, personal information later (see Chapter 12 (APP 12) and Chapter 13 (APP 13)).

The facts and circumstances of collection

5.10 The matter set out in APP 5.2(b) is the fact and circumstances of collection. This may include how, when and from where the personal information was collected. This requirement applies where either the personal information has been collected from a third party or the individual may not be aware that the entity has collected their personal information.

5.11 The following examples illustrate matters that can be notified:

- where the individual's personal information was or will be collected from another entity, the individual should be made aware of the name of the entity. If this is not practicable because, for instance, the APP entity collects information from a wide variety of entities and it would not be practicable to give a separate notice in relation to each entity, the APP entity should instead indicate the kinds of entities from which it collects that information.
- where the individual's personal information was or will be collected from an individual, the name of that individual should be provided, unless doing so would be an interference with the privacy of that individual (for example, the use or disclosure breaches APP 6 because that individual would not reasonably expect their personal information to be disclosed in an APP 5 notice and no other exception in APP 6 applies) (see Chapter 6 (APP 6)).
- where the individual may not be aware of their personal information being collected, the individual should be made aware of the method of collection, for example, that personal information is collected through use of a hidden radio-frequency identification tag (RFID tags), software (such as cookies), or biometric technology (such as voice or facial recognition).

If the collection is required or authorised by law

5.12 The matter set out in APP 5.2(c) is the fact (if applicable) that a collection is required or authorised by or under an Australian law or a court/tribunal order. The phrase 'required or authorised by or under an Australian law or court/tribunal order' is discussed in Chapter B (Key concepts).

5.13 The name of the Australian law (or, if applicable, the regulation or other instrument), or details of the particular court or tribunal order, that requires or authorises the collection, must also be included. If practicable, the notice could include the provision of the law, regulation or other instrument relied upon for collection.

5.14 If it is not reasonable to name the particular law relied upon (for example, multiple Australian laws authorise or require the collection) the more practical option may be to include a generic description of the laws under which personal information is collected (for example, 'taxation laws').

The purposes of collection

5.15 The matter set out in APP 5.2(d) is the purposes for which the APP entity collects the personal information. This includes the primary purpose of collection, that is, the specific function or activity for which particular personal information is collected.

5.16 If the APP entity may use or disclose personal information for purposes other than the primary purpose (known as a 'secondary purpose'), these could also be included. This may create a reasonable expectation that the personal information will be used or disclosed for a secondary purpose, of relevance to the exception in APP 6.2(a) (this exception is discussed in Chapter 6 (APP 6)). The entity does not need to include in its description internal purposes that form part of normal business practices, such as auditing, business planning, billing or de-identifying personal information.

5.17 The term 'purpose', including 'primary purpose', 'secondary purpose' and how a purpose should be described, are discussed in Chapter B (Key concepts) and Chapter 6 (APP 6)).

The consequences for the individual if personal information is not collected

5.18 The matter set out in APP 5.2(e) is the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity.

5.19 An APP entity is not required to list all possible or remote consequences or those that would be obvious to a reasonable person. Instead, it should describe significant consequences that could be expected to result. If the individual can avoid or lessen those consequences by providing some but not other personal information, this should be explained.

5.20 The following are given as examples of consequences that may result if personal information is not collected:

- an application for a licence, benefit, allowance or concession cannot be processed
- an APP entity cannot properly investigate or resolve an individual's complaint
- a different level of service will be provided to the individual. For example, the individual may not be eligible to purchase a discounted flight without providing personal information about a medical emergency in the individual's family.

Other APP entities, bodies or persons to which the personal information is usually disclosed

5.21 The matter set out in APP 5.2(f) is any other APP entity, body or person, or the types of other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity.

5.22 An APP entity is not required to include that a particular disclosure has occurred or will occur. Rather, APP 5.2(f) requires an entity to notify or ensure awareness of the 'usual' practices of the entity in disclosing personal information of that 'kind' to other APP entities, bodies or persons or 'types' of APP entities, bodies or persons.

5.23 A 'usual' disclosure is one that occurs regularly, under an agreed arrangement, or that can reasonably be predicted or anticipated. It does not include a disclosure that may occur in exceptional or special circumstances (such as a disclosure under a lawful warrant to a law enforcement agency).

5.24 The 'kind' of personal information that is usually disclosed may be described, for example, as 'contact details', 'employment history', 'educational qualifications' or 'complaint details'.

5.25 If the personal information is usually disclosed to a particular APP entity (including a related body corporate), body or person, it should be named, unless it would be impracticable to include a long list of APP entities, bodies or persons. In that case, the 'type' of APP entity, body or person should be described, for example, as 'health insurers' or 'State Government motor vehicle licensing authorities' or 'related bodies corporate.' An APP entity is not required to describe the disclosure practices of the APP entity, body

or person to which the information is disclosed. However, if it is known that that APP entity, body or person usually discloses the personal information to other entities, this could be noted.

Information about access and correction in the APP entity's APP Privacy Policy

5.26 The matters set out in APP 5.2(g) and (h) are that the APP entity's APP Privacy Policy contains information about how the individual may:

- access and seek correction of their personal information held by the entity (APP 5.2(g))
- complain to the entity about a breach of the APPs, or any registered APP code that binds the entity, and how the entity will deal with such a complaint (APP 5.2(h)).

5.27 Where practicable, an APP 5 notice could include a prominent and accessible link to the APP Privacy Policy on the entity's website or explain how it may be accessed. The APP Privacy Policy requirements are discussed in Chapter 1 (APP 1).

Likely cross-border disclosures of the personal information

5.28 The matters set out in APP 5.2(i) and (j) are:

- whether the APP entity is likely to disclose the personal information to overseas recipients (APP 5.2(i)), and
- if so, the countries in which such recipients are likely to be located if it is practicable to specify those counties in the notice or to otherwise make the individual aware of them (APP 5.2(j)).

5.29 This requirement only applies to a likely disclosure of personal information to an overseas recipient. It does not apply to a use of personal information by an APP entity that does not constitute a disclosure. For example, routing personal information, in transit, through servers located outside Australia would usually be considered a 'use' and not a 'disclosure'.[2] Similarly, if an entity makes personal information accessible to an overseas office of the entity (for example, a consular office), this is a use and not a disclosure.[3] 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).

5.30 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 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. Whether these factors make it impracticable to specify the countries will depend on whether the burden is excessive in all the circumstances. In this,

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

as in other examples, it is the responsibility of the entity to be able to justify that this is impracticable.

5.31 The requirement to notify an individual or ensure awareness if information being collected is likely to be disclosed to overseas recipients, and the location of those recipients, complements the obligation on APP entities under APP 1.4(f) and (g) to describe overseas disclosure practices in an APP Privacy Policy (see Chapter 1 (APP 1)).

5.32 If the personal information is disclosed to numerous overseas locations, one practical option may be to list those countries in an appendix to the notice rather than in the body of the notice. Where it is not practicable to specify the countries, the entity could instead identify general regions (such as European Union countries).

5.33 An APP entity that regularly discloses personal information overseas could consider including additional information in an APP 5 notice about these disclosures, to ensure transparent handling of personal information. For example, the APP 5 notice could explain:

- how the overseas recipient might use, disclose and protect the personal information, including whether the overseas recipient may be required to disclose the personal information under a foreign law (see discussion of s 6A(4) in Chapter 8 (APP 8))
- how the individual can request further information about laws or binding schemes that protect privacy in the country of receipt (this information may be particularly relevant if an entity intends to rely on the exception in APP 8.2(a) (see Chapter 8 (APP 8))
- how the individual can access personal information held by the overseas recipient.

When notification is to occur

5.34 An APP entity must take any reasonable steps to comply with APP 5:

- at or before the time an APP entity collects an individual's personal information, or
- if that is not practicable, as soon as practicable after the collection occurs.

5.35 This requirement recognises that it is preferable that an individual can make an informed choice about whether to provide personal information to an APP entity.

5.36 Examples of when it may not be practicable to take reasonable steps at or before the time of collection include where:

- urgent collection of the personal information is required and giving a notice or ensuring awareness would unreasonably delay the collection, for example, where there is a serious threat to an individual's life or health or to public safety
- the medium through which personal information is collected makes it impracticable to provide a detailed APP 5 notice or ensure awareness at or before the time of collection. For example, where personal information is collected by telephone, it

may be impracticable to notify or ensure the individual is aware of all of the APP 5 matters at the time of collection (see paragraph 5.5).[4]

5.37 The test of practicability is an objective test. It is the responsibility of the APP entity to be able to justify that it is not practicable to give notification or ensure awareness before or at the time of collection. Options for providing early notification or ensuring awareness should, so far as practicable, be built into information collection processes and systems – for example, by including relevant information in standard forms and online collection mechanisms (see APP 1.2, Chapter 1).

5.38 If notification does not occur before or at the time of collection, the APP entity must take reasonable steps to provide notification, or ensure the individual is aware, as soon as practicable after the collection. In adopting a timetable that is 'practicable', an entity can take technical and resource considerations into account. However, it is the responsibility of the entity to be able to justify any delay in notification.

[4] See also OAIC, *Mobile Privacy: A Better Practice Guide for Mobile App Developers,* "Section 4: Timing of User Notice and Consent is Critical", OAIC website <www.oaic.gov.au>.