Chapter 4: Australian Privacy Principle 4 — Dealing with unsolicited personal information

Version 1.0, February 2014

Key points

- APP 4 outlines the steps an APP entity must take if it receives unsolicited personal information.
- Unsolicited personal information is personal information received by an APP entity where the entity has taken no active steps to collect the information.
- If an APP entity receives unsolicited personal information, it must decide whether it could have collected the information under APP 3 (collection of solicited personal information).
- If the entity determines it could not have collected the personal information under APP 3, different rules apply according to whether or not the information is contained in a 'Commonwealth record'.
- If the unsolicited personal information is contained in a Commonwealth record, APP 4 does not require it to be destroyed or de-identified.
- Other unsolicited personal information that could not have been collected under APP 3, must be destroyed or de-identified as soon as practicable if it is lawful and reasonable to do so.
- If an APP entity is not required to destroy or de-identify the unsolicited personal information under APP 4, the entity may retain the personal information but must deal with it in accordance with APPs 5–13.

What does APP 4 say?

4.1 APP 4 outlines the steps an APP entity must take if it receives unsolicited personal information. Unsolicited personal information is personal information received by an entity that has not been requested by that entity.

4.2 An APP entity that receives unsolicited personal information must decide whether or not it could have collected the information under APP 3, and:

- if the entity could not have collected the personal information and the information is not contained in a Commonwealth record — the entity must destroy or de-identify the information as soon as practicable, if it is lawful and reasonable to do so (APP 4.3), or
- if the entity could have collected the personal information under APP 3, or the information is contained in a Commonwealth record, or the entity is not required to destroy or de-identify the information under APP 4.3 because it would be unlawful or unreasonable to do so — the entity may keep the information but must deal with it in accordance with APPs 5–13. See Chapter B (Key concepts) for more information about Commonwealth records.

4.3 In effect, APP 4 requires an APP entity to consider the following issues:

- has the entity received unsolicited personal information?

- could the entity have collected that personal information under APP 3?
- if the entity is an agency or a 'contracted service provider', is the personal information contained in a Commonwealth record?
- should unsolicited personal information held by the entity be destroyed or de-identified, or should it be retained and dealt with in accordance with APP 5–13?

4.4 The objective of APP 4 is to ensure that personal information that is received by an APP entity is afforded appropriate privacy protection, even where the entity has not solicited the personal information.

'Unsolicited' personal information

4.5 All personal information received by an APP entity is either solicited or unsolicited personal information. Section 6(1) defines 'solicit' but does not define 'unsolicited'. Therefore, personal information received by an entity that does not fall within the definition of 'solicited' is unsolicited personal information.

4.6 The term 'solicit' is discussed in Chapter 3 (APP 3), including examples of solicited personal information collected by APP entities. An APP entity solicits personal information if it requests another agency, organisation, individual or small business operator to provide the personal information, or to provide a kind of information in which that personal information is included. A 'request' is an active step taken by an entity to collect information, and may not involve direct communication between the entity and an individual.

4.7 Applying that definition of 'solicit', unsolicited personal information is personal information that an APP entity receives but has taken no active steps to collect. Examples include:

- misdirected mail received by an entity
- correspondence to Ministers and Government departments from members of the community, or other unsolicited correspondence to an entity
- a petition sent to an entity that contains names and addresses
- an employment application sent to an entity on an individual's own initiative and not in response to an advertised vacancy
- a promotional flyer containing personal information, sent to an entity by an individual promoting the individual's business or services.

4.8 As a general rule, personal information provided to an APP entity that is additional to the information that has been requested by the entity should be treated as unsolicited personal information. For example, if an individual completes an application form provided by an entity but attaches financial records that have not been requested by the entity, these should be treated as unsolicited personal information. The entity must determine whether it could have collected the personal information under APP 3 (APP 4.1), and deal with the unsolicited personal information as required by either APP 4.3 or 4.4 (see below).

4.9 In some instances, an APP entity may have difficulty deciding whether personal information it receives falls within the terms of the entity's request and is therefore solicited personal information. In such circumstances, an entity should focus on the nature of the additional personal information and the connection it has with the entity's request. Where it is unclear whether the information is solicited or unsolicited personal information, the entity should err on the side of caution and treat the personal information as unsolicited personal information.

Determining whether unsolicited personal information could have been collected under APP 3

4.10 An APP entity that receives unsolicited personal information must, 'within a reasonable period after receiving the information', decide whether the personal information could have been collected by the entity under APP 3 (APP 4.1).

4.11 The tests for deciding whether personal information can be collected by an APP entity are set out in APP 3 (see Chapter 3):

- an agency may only collect personal information that is reasonably necessary for, or directly related to, one or more of its functions or activities (APP 3.1)
- an organisation may only collect personal information that is reasonably necessary for one or more of its functions or activities (APP 3.2)
- and, in addition to the above requirements, an APP entity may only collect sensitive information if the individual consents to the sensitive information being collected, unless an exception applies (APP 3.3).

4.12 What is a 'reasonable period' for deciding whether unsolicited personal information could have been collected under APP 3 will depend on the circumstances of the particular case. The APP entity may undertake internal processes before making this decision, but should do so promptly.

4.13 APP 4.2 permits an APP entity to use or disclose the unsolicited personal information (for example, in internal discussions) for the purpose of determining whether the personal information could have been collected under APP 3.

Dealing with unsolicited personal information that could not have been collected under APP 3

4.14 If an APP entity receives unsolicited personal information that it determines it could not have collected under APP 3, it has an obligation to destroy or de-identify the personal information as soon as practicable, unless it is contained in a 'Commonwealth record' or it is unlawful or unreasonable to do so (APP 4.3). In practice, this means that different rules apply to agencies and organisations when handling unsolicited personal information.

Unsolicited personal information received by an agency

4.15 The term 'Commonwealth record' in s 6(1) has the same meaning as in s 3 of the *Archives Act 1983* (the Archives Act) and is discussed in more detail in Chapter B (Key concepts).[1] The term is likely to include all or most personal information received by agencies. It may also include personal information received by contracted service providers.

4.16 If the unsolicited personal information is contained in a Commonwealth record, the agency is not required to destroy or de-identify the personal information under APP 4.3, even if it determines that it could not have collected the information under APP 3. The agency will instead be required to comply with the provisions of the Archives Act in relation to the Commonwealth record.

4.17 A Commonwealth record can, as a general rule, only be destroyed or altered in accordance with s 24 of the Archives Act. The grounds on which this may be done include with the permission of the National Archives of Australia (as set out in a records disposal authority) or in accordance with 'normal administrative practice'. See Chapter B (Key concepts) for more information about Commonwealth records.

4.18 Unsolicited personal information held by an agency in a Commonwealth record must be dealt with in accordance with APPs 5–13 (APP 4.4) (see paragraphs 4.28 to 4.30 below).

Unsolicited personal information received by an organisation

4.19 Unsolicited personal information received by an organisation, that could not have been collected under APP 3 must, as soon as practicable, be destroyed or de-identified if it is lawful and reasonable to do so (APP 4.3).

4.20 After an organisation has decided that the destruction or de-identification is lawful and reasonable, it should destroy or de-identify the personal information as promptly as practicable. In adopting a timetable that is 'practicable' an organisation can take technical and resource considerations into account. However, it is the responsibility of the organisation to be able to justify any delay in destroying or de-identifying the personal information.

[1] *Archives Act 1983*, s 3: *Commonwealth record means:*
(a) a record that is the property of the Commonwealth or of a Commonwealth institution; or
(b) a record that is to be deemed to be a Commonwealth record by virtue of a regulation under subsection (6) or by virtue of section 22;
but does not include a record that is exempt material or is a register or guide maintained in accordance with Part VIII.

Destruction or de-identification that is 'lawful'

4.21 The term 'lawful' is not defined in the Privacy Act. It is lawful for an organisation to destroy or de-identify unsolicited personal information if it is not unlawful to do so. That is, if the destruction or de-identification is not criminal, illegal or prohibited or proscribed by law. Unlawful activity does not include breach of a contract.

4.22 Examples of where destruction may not be lawful include:

- a legislative provision in an Act or subordinate instrument requires an organisation to retain the personal information for a specified purpose — for example, for auditing, inspection or reporting purposes
- a court, tribunal or body with legal power to issue binding orders, has made an order requiring the personal information to be retained for a specified purpose or period.

4.23 As those examples illustrate, it is important that each organisation is aware of the legal rules or orders that may prevent it from destroying or de-identifying unsolicited personal information.

Destruction or de-identification that is 'reasonable'

4.24 Whether destruction or de-identification is reasonable is a question of fact in each individual case. It is an objective standard that has regard to how a reasonable person, who is properly informed, would be expected to act in the circumstances. It is the responsibility of the organisation to be able to justify that its conduct was reasonable.

4.25 Relevant considerations may include:

- the amount and sensitivity of the personal information
- whether the personal information is commingled with solicited personal information, and it would be impractical for the organisation to separate the personal information (see paragraph 4.26 below for an example of where it may be practicable to separate solicited and unsolicited personal information)
- whether a law enforcement authority has requested that the personal information be retained pending the completion of an investigation
- whether the organisation has considered a range of options for destroying or de-identifying the personal information
- whether the individual that the personal information is about has expressly requested the organisation to return the information to the individual, rather than destroying or de-identifying the information, and the organisation does not retain another copy of the personal information
- where destruction or de-identification is unreasonable within a short timeframe, whether the destruction or de-identification task could be undertaken using a staged approach
- the practicability, including time and cost involved. However, an organisation is not excused from destroying or de-identifying the personal information by reason only

that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to destroy or de-identify the personal information will depend on whether the burden is excessive in all the circumstances.

4.26 Those and other relevant considerations should be applied cautiously. Before deciding that it is reasonable to retain unsolicited personal information, an organisation should examine viable options for destroying or de-identifying it. For example, it may be practicable to transcribe or convert, and produce a new record of, solicited personal information that is commingled with unsolicited personal information. The original record containing the unsolicited personal information could then be destroyed or de-identified.

4.27 For further discussion of destroying and de-identifying personal information, see Chapter B (Key concepts) and Chapter 11 (APP 11).

Dealing with unsolicited personal information that could have been collected under APP 3, or is not destroyed or de-identified

4.28 An APP entity may retain unsolicited personal information if the entity has determined that it could have collected the personal information under APP 3, or the personal information is contained in a Commonwealth record, or the entity is not required to destroy or de-identify the personal information under APP 4.3 because it would be unlawful or unreasonable to do so. The personal information must then be dealt with in accordance with APPs 5–13 (APP 4.4). This means, for example, that a notice of collection may be required (see Chapter 5 (APP 5)), the personal information may only be used or disclosed for the primary purpose for which it was collected unless an exception applies (see paragraph 4.29 below and Chapter 6 (APP 6)), the security of the personal information must be protected (see Chapter 11 (APP 11)), an individual can request access to the personal information (see Chapter 12 (APP 12)) and an individual can request the entity to correct the personal information (see Chapter 13 (APP 13)).

4.29 Two other matters should be borne in mind by an APP entity that retains personal information for one of the reasons listed in paragraph 4.28. The first is that the personal information, though retained by the APP entity, may not be information that could have been collected for a particular purpose under APP 3.1 (for example, where the personal information is retained because it is contained in a Commonwealth record, or because it is not lawful or reasonable for the entity to destroy or de-identify it). Consequently, if the entity has not collected the personal information for a particular primary purpose, the entity may only use or disclose it if an exception in APP 6 applies (see Chapter 6).

4.30 Secondly, APP 11.2 requires an APP entity to destroy or de-identify personal information it holds but which it no longer needs for any purpose permitted by the APPs, unless the personal information is contained in a Commonwealth record or the entity is required by or under an Australian law, or a court/tribunal order, to retain the information. Consequently, personal information that is retained under APP 4.4 may

nevertheless need to be destroyed or de-identified in accordance with APP 11.2 (see Chapter 11 (APP 11)).