Australian Privacy Principle 11 — security of personal information

Chapter 11

Draft version, September 2013

Australian Privacy Principle 11 — security of personal information

Key points

- An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.
- Where an APP entity no longer needs personal information for any purpose for which the information may be used or disclosed under the APPs, the entity must take reasonable steps to destroy the information or ensure that the information is de-identified. This requirement applies except where:
    - the information is part of a Commonwealth record, or
    - the APP entity is required by law or a court/tribunal order to retain the information.

What does APP 11 say?

11.1 APP 11 requires an entity to take active measures to ensure the security of personal information it holds,[1] and to actively consider whether it is able to retain personal information.[2]

11.2 An APP entity that holds personal information must take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure (APP 11.1).

11.3 An APP entity must destroy or de-identify the personal information it holds once the information is no longer needed for any purpose for which the information may be used or disclosed under the APPs. This requirement does not apply where the information is contained in a Commonwealth record or where the entity is required by law or a court/tribunal order to retain the information (APP 11.2).

[1] *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, Explanatory Memorandum, Schedule 1, Part 2, APP 11.
[2] *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, Explanatory Memorandum, Schedule 1, Part 2, APP 11.

When does an APP entity 'hold' personal information?

11.4 APP 11 only applies to personal information that an APP entity holds. An entity holds personal information 'if the entity has possession or control of a record that contains the personal information' (s 6(1)). The term 'holds' is discussed in more detail in Chapter B (Key concepts).

What are reasonable steps?

11.5 In the context of APP 11.1, 'reasonable steps' involve balancing security considerations (discussed in paragraphs 11.8 - 11.17) with other considerations, which could include:

- The nature of the APP entity. This includes the entity's business model or governance arrangements. For example, it may be reasonable for an APP entity:
    - with a large number of staff and resources to take additional steps compared to a smaller entity to ensure the security of the personal information the entity holds
    - that operates through franchises or dealerships, or that provides contractors with access to information it holds, to take different or further steps than a more centralised entity.
- The nature, quantity and extent of personal information held, and whether this requires the APP entity to take additional steps. For example, the more sensitive the information, the greater the risk of harm to the individual if the information is subject to misuse, interference or loss, or unauthorised access, modification or disclosure. It may therefore be reasonable for an APP entity to take additional steps to protect sensitive information it holds.
- The adverse consequences for an individual if their personal information is not secured. For example, an individual may suffer reputational harm if their personal information becomes public, or material harm if exposure of their information enables identity theft or fraud. Generally, more rigorous steps may be required as the risk of adverse consequences increases.
- The APP entity's data handling practices, such as how it collects, uses and stores personal information. This includes whether data handling practices are outsourced to third parties, and whether those third parties are subject to the Privacy Act.[3] If a third party is not subject to the Privacy Act, it may be reasonable for the entity to take steps to ensure the third party meets the entity's obligations under the Privacy Act, for example through specific privacy obligations in contracts and mechanisms to ensure these are being fulfilled.
- The practicability of implementing a particular measure. 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

[3] Agencies will also need to consider s 95B of the Privacy Act, which sets out requirements for Commonwealth contracts.

practices, procedures and systems by relying on the inconvenience or commercial cost of doing so.

- Whether a security measure is in itself privacy invasive. For example, while an APP entity should ensure that an individual is authorised to access information, it should not require an individual to supply more information than is necessary to identify themselves when dealing with the entity (see also Chapter 12).

11.6 Reasonable steps could including taking steps and implementing strategies to manage the following:

- governance
- ICT security
- data breaches
- physical security
- personnel security and training
- workplace policies
- the information life cycle
- standards
- regular monitoring and review.

11.7 For further discussion of the relevant considerations, and examples of steps that may be reasonable for an APP entity to take, see the Office of the Australian Information Commissioner's *Guide to information security: 'reasonable steps' to protect personal information* (OAIC Information Security Guide).[4]

What are the security considerations?

11.8 An APP entity should plan and implement reasonable steps, based on a clear understanding of the terms 'misuse', 'interference', 'loss', 'unauthorised access', 'modification' or 'disclosure'.

11.9 The terms 'misuse', 'interference', 'loss', 'unauthorised access', 'modification' and 'disclosure' are not defined in the Privacy Act so it is appropriate to refer to the ordinary meaning of these words. An APP entity should also consider the meaning of these terms as clarified by courts from time to time, and in other consumer law contexts. Guidance on the meaning of these words is outlined below. These examples show some overlap between each term.

Misuse

11.10 'Misuse' means 'wrong or improper use' or 'misapplication'.[5] An example of a 'misuse' of personal information is where an APP entity uses information it holds for a

[4] See <www.oaic.gov.au>.
[5] Macquarie Dictionary, *Australian Online Dictionary*, <www.macquariedictionary.com.au>.

purpose other than a permitted purpose. APP 6 sets out when an APP entity is permitted to use personal information (see Chapter 6).

11.11 'Use' is discussed in more detail in Chapter B (Key concepts).

Interference

11.12 'Interference' of personal information occurs where there is an attack on personal information that an APP entity holds that interferes with the information but does not necessarily modify its content.[6] 'Interference' includes an attack on a computer system that, for example, leads to exposure of personal information.

Loss

11.13 'Loss' means 'the accidental or inadvertent losing of something dropped, misplaced, or of unknown whereabouts' or the 'failure to preserve or maintain'.[7] It covers an APP entity's 'loss' of personal information that it holds, other than by intentional destruction or de-identification. This includes when an APP entity:

- physically loses information, such as by leaving it in a public place, or
- electronically loses information, such as failing to keep adequate backups of personal information in the event of a systems failure.

11.14 Loss of personal information could also potentially occur following unauthorised access or modification of the information.

Unauthorised access

11.15 'Unauthorised access' of personal information occurs when personal information that an APP entity holds is accessed by someone that is not permitted to do so.

Unauthorised modification

11.16 'Unauthorised modification' of personal information occurs when personal information that an APP entity holds is altered by someone that is not permitted to do so.

Unauthorised disclosure

11.17 'Unauthorised disclosure' occurs when an APP entity releases personal information from its effective control in a way that is not permitted under the APPs. The term 'disclosure' is discussed in more detail in Chapter B (Key concepts).

Destroying or de-identifying personal information

11.18 An APP entity must take reasonable steps to destroy or de-identify personal information it holds if it no longer needs the information for any purpose for which it may be used or disclosed under the APPs (APP 11.2). The requirement to take reasonable steps to destroy or de-identify does not apply if personal information is contained in a

[6] *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, Explanatory Memorandum, Schedule 1, Part 2, APP 11, p 91.
[7] Macquarie Dictionary, *Australian Online Dictionary*, <www.macquariedictionary.com.au>.

Commonwealth record, or if an Australian law or a court/tribunal order requires it to be retained (APP 11.2). In practice, this means that different rules apply to agencies and organisations.

Personal information held by an agency

11.19 The term 'Commonwealth record' in s 6(1) of the Privacy Act has the same meaning as in s 3 of the *Archives Act 1983*. The core meaning is 'a record that is the property of the Commonwealth' or a Commonwealth agency.[8] This is likely to include, in almost all cases, all personal information held by agencies.

11.20 If the personal information is contained in a Commonwealth record, the agency is not required to destroy or de-identify the information under APP 11.2, even if it no longer needs the information for any purpose for which it may be used or disclosed under the APPs. However, an agency still needs to consider its obligations under the Archives Act.

11.21 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 'normal administrative practice' and destruction or alteration in accordance with an arrangement approved by the Archives (often titled a Records Disposal Authority). See Chapter B (Key concepts) for more information about Commonwealth records.

Personal information held by an organisation

11.22 An organisation should have practices, procedures and systems in place to identify personal information that needs to be destroyed or de-identified (see APP 1.2, discussed in Chapter 1).

11.23 Where an organisation 'holds' (see paragraph 11.4 and Chapter B (Key concepts) for a discussion of 'holds') personal information it no longer needs for a purpose that is permitted under the APPs, it must ensure that it takes reasonable steps to destroy or de-identify the personal information. This obligation applies even where the organisation does not physically possess the personal information, such as where it is held in electronic form on a third party's hardware.

11.24 Where an organisation holds personal information that needs to be destroyed or de-identified, it must take reasonable steps to destroy all copies it holds of that personal information, including copies that have been archived or are held as back-ups.

Required by or under an Australian law or a court/tribunal order

11.25 If an organisation is required by or under an Australian law or a court/tribunal order to retain personal information, it is not required to take reasonable steps to destroy or de-identify it (APP 11.2(d)).

---

[8] *Archives Act 1983* section 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.

11.26 'Australian law' is defined in s 6(1). The term 'required by or under an Australian law' is discussed in Chapter B (Key Concepts).

Reasonable steps to destroy personal information – irretrievable destruction

11.27 Personal information is destroyed where it can no longer be retrieved. The steps that are reasonable for an organisation to take to destroy personal information will depend on whether the personal information is held in hard copy or electronic form.

11.28 For example, for information held:

- in hard copy, disposal through garbage or recycling collection would not ordinarily constitute taking reasonable steps to destroy the information, unless the information had already been destroyed through a process such as pulping, burning, pulverising, disintegrating or shredding[9]
- in electronic form, reasonable steps will vary depending on the kind of hardware used to store the information. In some cases it may be possible to 'sanitise' the hardware to completely remove stored information.[10] For hardware that cannot be sanitised, reasonable steps must be taken to destroy the personal information in another way, such as by irretrievably destroying it. Where it is not possible to irretrievably destroy personal information held in electronic format, an organisation should instead comply with APP 11.2 by taking reasonable steps to de-identify the personal information (see para 11.31 below), or by putting it beyond use (see para 11.29 below).
- on a third party's hardware, such as cloud storage, where the organisation has instructed the third party to delete the personal information, reasonable steps would include taking steps to verify that deletion has occurred (by either destruction or de-identification, as appropriate).

Reasonable steps to destroy personal information held in electronic format –putting beyond use

11.29 Where it is not possible for an organisation to irretrievably destroy personal information held in electronic format, reasonable steps to destroy it would include putting the information 'beyond use'. Information is 'beyond use' if the organisation:

- is not able, and will not attempt, to use or disclose the personal information
- cannot give any other entity access to the personal data

[9] See the *Information security management guidelines* of the Australian Government *Protective Security Policy Framework* (PSPF), Attorney-General's Department Protective Security website, <www.protectivesecurity.gov.au>. Although the PSPF only applies to Australian Government agencies, the examples may also be relevant to organisations in complying with APP 11.2.

[10] See the 'Controls' section of the Defence Security Directorate's *Information Security Manual* (ISM), Defence Signals Directorate website, <www.dsd.gov.au>. The ISM also discusses how various forms of hardware should be sanitised or destroyed. Although the ISM only applies to Australian Government agencies, it may be of interest to organisations in complying with APP 11.2.

- surrounds the personal information with appropriate technical and organisational security. This should include, at a minimum, access controls together with log and audit trails, and
- commits to take reasonable steps to irretrievably destroy the information if, or when, this becomes possible.

11.30 It is expected that only in very limited circumstances would it not be possible for an organisation to destroy personal information held in electronic format. For example, only where technical reasons may make it impossible to delete the personal information without also deleting other information held with that information, which the entity is required to retain.

De-identifying personal information

11.31 Personal information is de-identified once the information is no longer about an identifiable individual or an individual who is reasonably identifiable (s 6(1)). De-identification is discussed in more detail in Chapter B (Key concepts).[11]

11.32 An organisation that intends to comply with APP 11.2 by taking reasonable steps to de-identify personal information should consider whether de-identification is appropriate in the circumstances. For guidance on de-identifying personal information see the OAIC's De-identification Fact Sheet.[12] Regardless of the de-identification technique chosen, an organisation undertaking de-identification must take reasonable steps to minimise the likelihood that the information could be re-identified.

11.33 De-identification of personal information may be more appropriate than destruction where the de-identified information could provide further value or utility to the organisation or a third party. For example, where:

- an agency makes de-identified information available for public access and reuse, or
- an organisation shares de-identified information with researchers.

11.34 On the other hand, where it is unclear whether the risk of re-identification can be appropriately minimised, the organisation should instead consider the reasonable steps available to destroy the information.

[11] De-identification, including examples of de-identification techniques are discussed in the OAIC *Information Security Guide*, see <www.oaic.gov.au>.
[12] To be published on the OAIC's website, <www.oaic.gov.au>, before 12 March 2014.