

Chapter 11:

Australian Privacy Principle 11 — Security of personal information

Version 1.2, July 2019

Contents

Key points	3
What does APP 11 say?	3
‘Holds’	3
Taking reasonable steps	4
What are the security considerations?	5
Misuse	5
Interference	5
Loss	5
Unauthorised access	6
Unauthorised modification	6
Unauthorised disclosure	6
Destroying or de-identifying personal information	6
Personal information held by an agency	7
Personal information held by an organisation	7
Required by or under an Australian law or a court/tribunal order	7
Taking reasonable steps to destroy or de-identify personal information	8
Destroying personal information — irretrievable destruction	8
Destroying personal information held in electronic format — putting beyond use	9
De-identifying personal information	10

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 it is de-identified. This requirement applies except where:
 - the personal information is part of a Commonwealth record, or
 - the APP entity is required by law or a court/tribunal order to retain the personal information
- Many of the issues discussed in this Chapter are discussed in more detail in the Office of the Australian Information Commissioner's (OAIC) Guide to Securing Personal Information.¹

What does APP 11 say?

- 11.1 APP 11 requires an APP entity to take active measures to ensure the security of personal information it holds, and to actively consider whether it is permitted 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 take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for any purpose for which the personal information may be used or disclosed under the APPs. This requirement does not apply where the personal information is contained in a Commonwealth record or where the entity is required by law or a court/tribunal order to retain the personal information (APP 11.2).

‘Holds’

- 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)).
- 11.5 The term ‘holds’ extends beyond physical possession of a record to include a record that an APP entity has the right or power to deal with. For example, an entity that outsources the storage of personal information to a third party, but retains the right to deal with that information, including to access and amend it, holds that personal information.
- 11.6 The term ‘holds’ is discussed in more detail in Chapter B (Key concepts).

¹ See OAIC website <<https://www.oaic.gov.au>>.

² Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 86.

Taking reasonable steps

11.7 The ‘reasonable steps’ that an APP entity should take to ensure the security of personal information will depend upon circumstances that include:

- the nature of the APP entity. Relevant considerations include an APP entity’s size, resources, the complexity of its operations and its business model. For example, the reasonable steps expected of an entity that operates through franchises or dealerships, or that outsources its personal information handling to a third party may be different to those it would take if it did not operate in this manner.
- the amount and sensitivity of the personal information held. Generally, as the amount and/or sensitivity of personal information that is held increases, so too will the steps that it is reasonable to take to protect it. ‘Sensitive information’ (defined in s 6(1)) is discussed in more detail in Chapter B (Key concepts)
- the possible adverse consequences for an individual in the case of a breach. More rigorous steps may be required as the risk of adversity increases
- the practical implications of implementing the security measure, including time and cost involved. However an entity is not excused from taking particular steps to protect 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 take particular steps will depend on whether the burden is excessive in all the circumstances
- 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 (APP 12)).

11.8 Reasonable steps should include, where relevant, taking steps and implementing strategies in relation to the following:

- governance, culture and training
- internal practices, procedures and systems
- ICT security
- access security
- third party providers (including cloud computing)
- data breaches
- physical security
- destruction and de-identification
- standards

11.9 As part of taking reasonable steps to protect personal information (also known as ‘personal information security’) an APP entity should consider how it will protect personal information at all stages of the information lifecycle. This should be considered before an entity collects personal information (including whether it should collect the information at all), as well as when the information is collected and held, and when it is destroyed or de-identified when no longer needed.

- 11.10 For further discussion of personal information security and the information lifecycle and examples of steps that may be reasonable for an APP entity to take under APP 11.1, see the OAIC's Guide to Securing Personal Information.³

What are the security considerations?

- 11.11 The six terms listed in APP 11, 'misuse', 'interference', 'loss', 'unauthorised access', 'unauthorised modification' and 'unauthorised disclosure', are not defined in the Privacy Act. The following analysis and examples of each term draws on the ordinary meaning of the terms. As the analysis indicates, there is overlap in the meaning of the terms.

Misuse

- 11.12 Personal information is misused if it is used by an APP entity for a purpose that is not permitted by the Privacy Act. APP 6 sets out when an entity is permitted to use personal information (see Chapter 6). APPs 7 and 9 also contain requirements relating to an organisation's use of personal information for the purpose of direct marketing, and use of government related identifiers, respectively (see Chapters 7 and 9).
- 11.13 'Use' is discussed in more detail in Chapter B (Key concepts).

Interference

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

Loss

- 11.15 'Loss' of personal information covers the accidental or inadvertent loss of personal information held by an APP entity. This includes when an APP entity:
- physically loses personal information, (including hard copy documents, computer equipment or portable storage devices containing personal information), for example, by leaving it in a public place, or
 - electronically loses personal information, such as failing to keep adequate backups of personal information in the event of a systems failure
- 11.16 Loss may also occur as a result of theft following unauthorised access or modification of personal information or as a result of natural disasters such as floods, fires or power outages.
- 11.17 However, it does not apply to intentional destruction or de-identification of that personal information that is done in accordance with the APPs.

³ See OAIC website <<https://www.oaic.gov.au>>. Agencies should also see the Attorney-General's Department's Protective Security Policy Framework and the Australian Signals Directorate's Australian Government Information Security Manual, which set out the Australian Government's requirements for protective security and standardise information security practices across government.

Unauthorised access

11.18 ‘Unauthorised access’ of personal information occurs when personal information that an APP entity holds is accessed by someone who is not permitted to do so. This includes unauthorised access by an employee of the entity⁴ or independent contractor, as well as unauthorised access by an external third party (such as by hacking).

Unauthorised modification

11.19 ‘Unauthorised modification’ of personal information occurs when personal information that an APP entity holds is altered by someone who is not permitted to do so, or is altered in a way that is not permitted under the Privacy Act. For example, unauthorised modification may occur as a result of unauthorised alteration by an employee, or following unauthorised access to databases by an external third party.

Unauthorised disclosure

11.20 ‘Unauthorised disclosure’ occurs when an APP entity:

- makes personal information accessible or visible to others outside the entity, and
- releases that information from its effective control in a way that is not permitted by the Privacy Act⁵

11.21 This includes an unauthorised disclosure by an employee of the APP entity.⁶ The term ‘disclosure’ is discussed in more detail in Chapter B (Key concepts).

Destroying or de-identifying personal information

11.22 An APP entity must take reasonable steps to destroy personal information or ensure it is de-identified if it no longer needs the information for any purpose for which it may be used or disclosed under the APPs (APP 11.2).

11.23 This means that an APP entity will not need to destroy or de-identify personal information it holds if the information is still necessary for the primary purpose of collection or for a secondary purpose for which it may be used or disclosed under APP 6 (see Chapter 6). Where the entity is an organisation and the personal information is needed for the purpose of direct marketing, or is a government related identifier, whether it may be used or disclosed under APPs 7 and 9 may also be relevant (see Chapters 7 and 9 respectively). ‘Purpose’ is discussed in more detail in Chapter B (Key concepts).

11.24 The requirement to take reasonable steps to destroy or de-identify does not apply if personal information is contained in a Commonwealth record, or if an Australian law or a

⁴ Under s 8(1) of the Privacy Act, an APP entity needs to take reasonable steps to ensure that an employee does not gain unauthorised access to personal information ‘in the performance of the duties of the person’s employment’.

⁵ See Chapter 6 (APP 6) for more information about disclosures that are permitted by the Privacy Act.

⁶ An APP entity needs to take reasonable steps to ensure that an employee does not carry out an unauthorised disclosure of personal information ‘in the performance of the duties of the person’s employment’ (s 8(1)).

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

- 11.25 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).⁷ The definition is likely to include all or most personal information held by agencies. It may also include personal information held by contracted service providers.
- 11.26 If the personal information is contained in a Commonwealth record, the agency is not required to destroy or de-identify the personal information under APP 11.2, even if it no longer needs the personal information for any purpose for which it may be used or disclosed under the APPs. The agency will instead be required to comply with the provisions of the Archives Act in relation to those Commonwealth records.
- 11.27 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 a ‘normal administrative practice’. See Chapter B (Key concepts) for more information about Commonwealth records.

Personal information held by an organisation

- 11.28 Where an organisation ‘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, but has the right or power to deal with it. ‘Holds’ is discussed in more detail in paragraphs 11.4–11.6 above and Chapter B (Key concepts).
- 11.29 Where an organisation holds personal information that needs to be destroyed or de-identified, it must take reasonable steps to destroy or de-identify all copies it holds of that personal information, including copies that have been archived or are held as back-ups.
- 11.30 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, Chapter 1).

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

- 11.31 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)).

⁷ 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.

11.32 ‘Australian law’ and ‘court/tribunal order’ are defined in s 6(1). The term ‘required by or under an Australian law or court/tribunal order’ is discussed in Chapter B (Key concepts).

Taking reasonable steps to destroy or de-identify personal information

11.33 The ‘reasonable steps’ that an organisation should take to destroy or de-identify personal information will depend upon circumstances that include:

- the amount and sensitivity of the personal information — more rigorous steps may be required as the quantity of personal information increases, or if the information is ‘sensitive information’ (defined in s 6(1) and discussed in Chapter B (Key concepts)) or other personal information of a sensitive nature
- the nature of the organisation. Relevant considerations include an organisation’s size, resources and its business model. For example, the reasonable steps expected of an organisation that operates through franchises or dealerships, or gives database and network access to contractors, may differ from the reasonable steps required of a centralised organisation
- the possible adverse consequences for an individual if their personal information is not destroyed or de-identified — more rigorous steps may be required as the risk of adversity increases
- the organisation’s information handling practices, such as how it collects, uses and stores personal information, including whether personal information handling practices are outsourced to third parties
- the practicability, including time and cost involved — however an organisation is not excused from destroying or de-identifying 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 take a particular step will depend on whether the burden is excessive in all the circumstances

11.34 For further discussion of the relevant considerations, and examples of steps that may be reasonable for an APP entity to take under APP 11.2, see the OAIC’s Guide to Securing Personal Information.⁸

11.35 While APP 11.2 requires an organisation to take reasonable steps to either destroy or de-identify personal information, in some circumstances one or the other may be more appropriate (see paragraphs 11.38 and 11.44 below).

Destroying personal information — irretrievable destruction

11.36 Personal information is destroyed when 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.

11.37 For example, for personal information held:

⁸ See OAIC website <<https://www.oaic.gov.au>>.

- in hard copy, disposal through garbage or recycling collection would not ordinarily constitute taking reasonable steps to destroy the personal information, unless the personal information had already been destroyed through a process such as pulping, burning, pulverising, disintegrating or shredding
- in electronic form, reasonable steps will vary depending on the kind of hardware used to store the personal information. In some cases, it may be possible to ‘sanitise’ the hardware to completely remove stored personal information.⁹ 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 could instead comply with APP 11.2 by taking reasonable steps to de-identify the personal information (see paragraphs 11.41–11.45 below), or should put the information beyond use (see paragraphs 11.38–11.40 below)
- on a third party’s hardware, such as cloud storage, where the organisation has instructed the third party to irretrievably destroy the personal information, reasonable steps would include taking steps to verify that this has occurred

Destroying personal information held in electronic format — putting beyond use

11.38 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 personal information ‘beyond use’. However, an organisation could instead consider whether de-identifying the data would be appropriate (see paragraphs 11.41–11.45 below) and if so, take reasonable steps to de-identify the personal information.

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

11.40 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, where technical reasons may make it impossible to irretrievably destroy the personal information without also irretrievably destroying other information held with that personal information, which the entity is required to retain.

⁹ See the ‘Media sanitisation’ section of the Australian Government Information Security Manual (ISM) on the Australian Signals Directorate website <<https://www.asd.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.

De-identifying personal information

- 11.41 Personal information is de-identified ‘if 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).
- 11.42 An organisation that intends to comply with APP 11.2 by taking reasonable steps to ensure that personal information is de-identified should consider whether de-identification is appropriate in the circumstances. For more information on when and how to de-identify information, and how to manage and mitigate the risk of re-identification, see De-identification and the Privacy Act.¹⁰
- 11.43 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 organisation shares de-identified information with researchers, or
 - an organisation uses de-identified information to develop new products
- 11.44 Regardless of the de-identification technique chosen, the risk of re-identification must be actively assessed and managed to mitigate this risk. Where it is not possible for the risk of re-identification to be appropriately minimised, the organisation could instead consider taking reasonable steps to destroy the personal information (see paragraphs 11.36–11.42 above).
- 11.45 Where the personal information is held on a third party’s hardware, such as cloud storage, and the organisation has instructed the third party to de-identify the personal information, reasonable steps to de-identify the personal information would include taking steps to verify that this has occurred.

¹⁰ See OAIC, De-identification and the Privacy Act, OAIC website <<https://www.oaic.gov.au>>.