Australian Privacy Principle 8 – cross-border disclosure of personal information

Chapter 8

Draft version, September 2013

Australian Privacy Principle 8 – cross-border disclosure of personal information

Key points

- Before an APP entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information (APP 8.1).
- An APP entity that discloses personal information to an overseas recipient is accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs (s 16C).
- There are exceptions to the requirement in APP 8.1 to take reasonable steps and to the accountability provision in s 16C.

What does APP 8 say?

8.1. APP 8 and s 16C create a framework for the cross-border disclosure of personal information. This framework generally requires an APP entity to ensure that an overseas recipient will handle the individual's personal information in accordance with the APPs, and makes the APP entity accountable if the overseas recipient mishandles the information.[1]

8.2. APP 8.1 provides that before an APP entity discloses personal information about an individual to an overseas recipient, the entity must take reasonable steps to ensure that the recipient does not breach the APPs in relation to that information. Where an APP entity discloses personal information to an overseas recipient, it is accountable for an act or practice of the overseas recipient that would breach the APPs (s 16C).

8.3. There are exceptions to the requirement in APP 8.1 and to the accountability provision in s 16C (see paragraphs 8.11 – 8.52).

8.4. When an APP entity discloses personal information to an overseas recipient it will also need to comply with APP 6 – that is, it must only disclose the information for the primary purpose for which it was collected unless an exception to that principle applies (see Chapter 6).

[1] An accountability approach was adopted in the Asia-Pacific Economic Cooperation (APEC) Privacy Framework in 2004, Information Privacy Principle IX (Accountability), see APEC website <www.publications.apec.org>. The accountability concept in the APEC Privacy Framework was in turn derived from the accountability principle from the Organisation for Economic Cooperation and Development (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 1980, see OECD website, <www.oaic.org.au>.

What is an overseas recipient?

8.5. Under APP 8.1, an 'overseas recipient' is a person who receives personal information from an APP entity and is:

- not in Australia or an external Territory
- not the APP entity disclosing the personal information, and
- not the individual to whom the personal information relates.

8.6. This means that where an APP entity in Australia sends information to an overseas office of the entity, APP 8 will not apply as the recipient is the same entity. [2] This is to be distinguished from the case where an APP entity in Australia sends personal information to a 'related body corporate' located outside of Australia. In that case, the related body corporate is a different entity to the APP entity in Australia. It will therefore be an 'overseas recipient' and APP 8 will apply.[3]

When does an APP entity 'disclose' personal information about an individual to an overseas recipient?

8.7. The term 'disclose' is not defined in the Privacy Act and bears its normal dictionary meaning.

8.8. An APP entity will generally disclose personal information when it permits that information to become known outside the entity and releases it from its effective control. The release of the information may be a proactive release or publication, a release in response to a specific request, or an accidental release. In the context of APP 8, an APP entity will disclose personal information to an overseas recipient where it:

- shares the personal information with an overseas recipient
- discusses the personal information at an international conference or meeting overseas
- sends a hard copy document or email containing an individual's personal information to on overseas client
- publishes the information on the internet, whether intentionally or not, and it is accessed by an overseas recipient.

8.8A 'Disclosure' is a separate concept from:

- 'unauthorised access' which is addressed in APP 11. An APP entity is not taken to have disclosed personal information where a third party intentionally exploits the entity's security measures and gains unauthorised access to the information.

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

[3] Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Act 2012* states 'APP 8 will apply where an organisation sends personal information to a 'related body corporate' located outside Australia' (p. 83). While section 13B(1) permits related bodies corporate to share personal information (unless an exception applies), it does not exempt an APP entity from complying with APP 8 before it discloses personal information to a related body corporate located overseas.

Examples include unauthorised access following a cyber-attack[4] or a theft, including where the third party then makes that information available to others outside the entity. However, where a third party gains unauthorised access, the APP entity may breach APP 11 if it did not take reasonable steps to protect the information from unauthorised access (see APP 11, Chapter 11)

- an individual's right to access their personal information, which is addressed in APP 12 (see Chapter 12)
- 'use'. An APP entity uses personal information where personal information is handled, or an activity is undertaken with the information, within the entity. An example of a 'use' of personal information is where an APP entity routes personal information through servers located outside Australia. In limited circumstances, the provision of personal information to a contractor may also be a 'use' of that information (see paras 8.10 to 8.13 below).

8.9. For further information about the concepts of 'use' and 'disclosure' of personal information, see Chapter B (Key concepts).

Provision of personal information to a contractor

8.10. Where an APP entity engages a contractor located overseas to perform services on its behalf, in most circumstances, the provision of personal information to that contractor is a disclosure. This means that the entity will need to comply with APP 8 before making that disclosure. Where a subcontractor may be engaged, the entity should also take reasonable steps to ensure that the subcontractor does not breach the APPs in relation to the information.

8.11. For example, the provision of personal information to a contractor is generally considered a 'disclosure' where:

- an Australian based retailer outsources the processing of online purchases through its website to an overseas contractor and, in order to facilitate this, provides the overseas contractor with personal information about its customers
- an Australian entity, as part of a recruitment drive, provides the personal information of job applicants to an overseas services provider to perform reference checks on behalf of the Australian entity
- an Australian organisation relies on its overseas parent company to provide technical and billing support, and as part of this, provides the overseas parent company with access to its Australian customer database (which includes personal information)

8.12. However, in limited circumstances, providing personal information to an overseas contractor to perform services on behalf of an APP entity may be a 'use'. In these circumstances, the entity would not need to comply with APP 8. For example, where an APP entity provides personal information to a cloud service provider located overseas for the limited purpose of storing and managing personal information, and:

[4] See OAIC, *Own Motion Investigation Report* – Sony Playstation Network/ Qriocity, September 2011, OAIC website, <www.oaic.gov.au>.

- the contract between the entity and the overseas cloud service provider binds the provider not to use or disclose the personal information except for the limited purpose of storing and managing the information
- the contract requires any sub-contractors to agree to the same obligations, and
- the contract between the entity and the cloud service provider gives the entity effective control of the information. Issues to consider include whether the entity retains the right or power to access, change or retrieve the information, who else will be able access the information and for what purposes, and what type of security measures will be used for the storage and management of the personal information.

8.13. Where the provision of personal information to an overseas recipient is a use, and the APP entity continues to hold that information, the APP entity still needs to comply with the APPs in relation to the information. An entity holds personal information if it 'has possession or control of a record that contains the personal information' (s 6(1)). 'Holds' is discussed in more detail in Chapter B (Key concepts).

When will an APP entity have taken reasonable steps?

8.14. The requirement in APP 8.1 to ensure that an overseas recipient does not breach the APPs is qualified by a 'reasonable steps' test. The appropriate steps for an entity will depend upon circumstances that include:

- the nature of the personal information. The more sensitive the information the greater the risk of harm to the individual should personal information be mishandled by an overseas recipient
- the entity's relationship with the overseas recipient. Additional steps may be required if an entity discloses information to an overseas recipient to which the entity has not previously disclosed personal information
- the risk of harm to an individual if the information is mishandled by the overseas recipient.
- existing technical and operational safeguards implemented by the overseas recipient which will protect the privacy of the personal information. For example, additional steps may be required where the recipient has limited safeguards in place
- the practicability of taking particular steps. 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 taking steps before an overseas disclosure by relying on the inconvenience or cost of doing so.

8.15. It is generally expected that an APP entity should enter into an enforceable contractual arrangement with the overseas recipient that requires the recipient to handle

the personal information in accordance with the APPs (other than APP 1).[5] Contractual arrangements may include:

- The types of personal information to be disclosed and the purpose of disclosure.
- A requirement that the overseas recipient complies with the APPs in relation to the collection, use, disclosure, storage and destruction or de-identification of personal information. This should also require the overseas recipient to enter a similar contractual arrangement with any third parties to whom it discloses the information (for example, a sub-contractor).
- The complaint handling process for privacy complaints.
- A requirement that the recipient implement a data breach response plan which includes a mechanism for notifying the entity where there are reasonable grounds to suspect a data breach and outlines appropriate remedial action (based on the type of personal information to be handled under the contract).[6]

8.16. Where an agency discloses personal information to a recipient that is engaged as a contracted service provider, the agency must also comply with s 95B of the Privacy Act. Section 95B(1) provides that an agency must take contractual measures to ensure that a contracted service provider does not do an act, or engage in a practice, that would breach an APP if done by that agency. The contract must contain provisions to ensure that such an act or practice is not authorised by a subcontract (s 95B(3)). Contractual measures taken under s 95B may help an agency to comply with the requirement in APP 8.1. However, additional steps may be required in some circumstances (see paragraph 8.14).

Disclosure of personal information to an overseas recipient that is subject to a similar law or binding scheme

8.17. An APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where the APP entity reasonably believes that:

- the overseas recipient is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way the APPs protect the information, and
- mechanisms can be accessed by the individual to enforce that protection of the law or binding scheme (APP 8.2(a)).

[5] Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, p. 83

[6] See OAIC, *Data breach notification: a guide to handling personal information security breaches,* OAIC website, <www.oaic.gov.au>.

'Reasonable belief'

8.18. The 'reasonable belief' test enables an APP entity to assess the applicability of this exception on a case-by-case basis, by considering the information available to it at the time of the disclosure and the context of the particular disclosure.[7]

8.19. The APP entity must have sound evidence to support this belief. For example this might be based on independent legal advice.

'Law or binding scheme'

8.20. An overseas recipient may be subject to a law or binding scheme, where, for example, it is:

- bound by a privacy or data protection law that applies in the jurisdiction of the recipient
- required to comply with another law that imposes obligations in relation to the handling of personal information – for example some taxation law includes provisions that expressly authorise and prohibit specified uses and disclosures, permit the retention of some data, require destruction after a certain period of time and under particular circumstances, and include a right of access to an individual's personal information
- subject to an industry scheme or privacy code that is enforceable once entered into, irrespective of whether the recipient was obliged or volunteered to participate or subscribe to the scheme or code.

8.21. However, an overseas recipient may not be subject to a law or binding scheme where, for example:

- the overseas recipient is exempt from complying, or is authorised not to comply, with part, or all of the privacy or data protection law in the jurisdiction
- the recipient can opt out of the binding scheme without notice and without returning or destroying the personal information.

'Substantially similar to'

8.22. A substantially similar law or binding scheme would provide a comparable, or a higher level of privacy protection to that provided by the APPs. Each provision of the law or scheme is not required to correspond directly to an equivalent APP. Rather, the overall effect of the law or scheme is of central importance.

8.23. Whether there is substantial similarity is a question of fact. Factors that may indicate that the overall effect is substantially similar, include:

- the law or scheme includes a comparable definition of personal information that would apply to the information disclosed to the recipient

[7] Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, p. 83.

- the law or scheme regulates the collection of personal information in a comparable way
- the law or scheme requires the recipient to notify individuals about the collection of their personal information
- the law or scheme requires the recipient to only use or disclose the personal information for authorised purposes
- the law or scheme includes comparable data quality and data security standards
- the law or scheme includes a right to access and seek correction of personal information.

Mechanisms to enforce privacy protections

8.24. A range of dispute resolution or complaint handling models may satisfy the requirement for an accessible enforcement mechanism. It is not essential that the mechanism provide recourse to a regulatory body, similar to the Office of the Australian Information Commissioner (OAIC). Instead, these mechanisms may be expressly included in a law or scheme or may take effect through the operation of cross-border enforcement arrangements between the OAIC and an appropriate regulatory authority in the foreign jurisdiction.[8]

8.25. Any enforcement mechanisms must be easily accessible to the individual, for example, via the internet.

Disclosure of personal information to an overseas recipient with the individual's consent after being expressly informed

8.26. An APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where:

- the APP entity expressly informs the individual that if they consent to the disclosure, this principle will not apply, and
- the individual then consents to the disclosure (APP 8.2(b)).

'Expressly inform'

8.27. An APP entity should provide the individual with a clear written or oral statement explaining the potential consequences of providing consent. At a minimum, this statement should explain that if the individual consents to the disclosure and the overseas recipient handles the information in breach of the APPs:

- the entity will not be accountable under the Privacy Act
- the individual will not be able to seek redress under the Privacy Act.

8.28. The statement should also:

[8] Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, p. 83.

- if applicable, explain that the individual may not be able to seek redress in the overseas jurisdiction
- be made at the time consent is sought
- not rely on assumed prior knowledge of the individual
- explain any other practical effects or risks associated with the disclosure that it is aware of, or would be reasonably expected to be aware of. These may include that:
    - the recipient may not be subject to any privacy obligations or to any principles similar to the APPs
    - the recipient is subject to a foreign law that could compel the disclosure of personal information to a third party, such as an overseas authority.

Consent

8.29. Consent is defined in s 6(1) as 'express consent or implied consent', and is discussed in more detail in Chapter B (Key concepts). The four key elements of consent are:

- the consent must be voluntary
- the individual must be adequately informed before giving consent (in this case 'expressly informed')
- the consent must be current and specific, and
- the individual must have the capacity to understand and communicate their consent.

8.30. An APP entity does not need to obtain consent before every proposed cross-border disclosure.[9] It may obtain an individual's consent to disclose a particular kind of personal information to the same overseas recipient for the same purpose on multiple occasions, providing it has expressly informed the individual of the potential consequences of providing that consent. In doing this the entity should not seek a broader consent than is necessary for its purposes, for example, consent for undefined future uses, or consent to all legitimate uses or disclosures.

8.31. If an individual withdraws their consent, the entity must no longer rely on the original consent when dealing with the individual's personal information.

Disclosure of personal information to an overseas recipient as required or authorised by law

8.32. An APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where the disclosure is 'required or authorised by or under an Australian law or a court/tribunal order' (APP 8.2(c)). An APP entity cannot rely on a requirement or authorisation in an overseas jurisdiction (see paragraph 8.60). The

[9] Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, p. 84.

meaning of 'required or authorised by or under an Australian law or a court/tribunal order' is discussed in Chapter B (Key concepts).

8.33. The following are examples of where a law or order may require or authorise disclosure of personal information to an overseas recipient:

- An APP entity disclosing personal information to the government of a foreign country under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth).*

- An agency disclosing personal information to an overseas recipient under the *Australian Federal Police Act 1979* or the *Mutual Assistance in Criminal Matters Act 1987 (Cth)*.

8.34. An agency that intends to rely on this exception should consider establishing administrative arrangements, memorandums of understanding or protocols with the overseas recipient that set out mutually agreed standards for the handling of personal information. These should provide privacy protections comparable to the APPs (see discussion of contractual measures in paragraph 8.15).

Disclosure of personal information to an overseas recipient where a permitted general situation exists

8.35. The cross-border principle will not apply if a permitted general situation exists for that disclosure (APP 8.2(d)). Section 16A lists five permitted general situations that may exist for a cross border disclosures. These situations are set out below, and are discussed in more detail in Chapter C (Permitted general situations) (including the meaning of relevant terms).

Lessening or preventing a serious threat to life, health or safety

8.36. An APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where:

- the entity reasonably believes the disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety, and

- it is unreasonable or impracticable to obtain consent (s 16A(1), Item 1).

8.37. For example, this exception might apply where an APP entity discloses the personal information of an individual to a foreign authority, based on a reasonable belief that this disclosure will lessen a serious threat to the health or safety of that individual's children, but seeking the individual's consent may increase the threat.

Taking appropriate action in relation to suspected unlawful activity or serious misconduct

8.38. An APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where the entity:

- has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in, and

- reasonably believes that the cross-border disclosure is necessary for the entity to take appropriate action in relation to the matter (s 16A(1), Item 2).

8.39. For example, this exception may apply where an APP entity that is a global organisation has reason to suspect that an individual is engaging in transnational fraud affecting the entity's activities, and the entity reasonably believes that disclosing personal information to an overseas authority is necessary to take appropriate action.

Locating a missing person

8.40. An APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where:

- the entity reasonably believes that the disclosure is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing, and

- the disclosure complies with rules made by the Information Commissioner under s 16A(2) of the Privacy Act (s 16A(1), Item 3).

Necessary for a diplomatic or consular function or activity

8.41. An agency may disclose personal information to an overseas recipient without complying with APP 8.1 where the agency reasonably believes that the disclosure is necessary for the agency's diplomatic or consular functions or activities (s 16A(1), Item 6).

8.42. For example, this exception may apply where an agency discloses personal information to an overseas recipient to assist an Australian citizen who is in distress overseas, such as where an Australian individual is detained or is the victim of crime, or where assistance is required with repatriation in the case of death or serious illness.

Necessary for certain Defence force activities outside Australia

8.43. The Defence Force (as defined in s 6(1)) may disclose personal information to an overseas recipient without complying with APP 8.1 where it reasonably believes that the disclosure is necessary for a warlike operation, peacekeeping, civil aid, humanitarian assistance, a medical emergency, a civil emergency or disaster relief occurring outside Australia and the external Territories (s 16A(1, Item 7).

8.44. For example, this exception might apply where, in the immediate aftermath of a natural or man-made disaster outside Australia, the Defence Force discloses an

individual's personal information to an overseas recipient in order to assist in the provision of proper medical care to that individual.

Disclosure of personal information to an overseas recipient as required or authorised under an international agreement relating to information sharing

8.45. An agency may disclose personal information to an overseas recipient without complying with APP 8.1 where the disclosure is 'required or authorised by or under an international agreement relating to information sharing to which Australia is a party' (APP 8.2(e)).

8.46. Information sharing need not be the primary subject matter of the agreement, so long as the agreement makes provision for information sharing.

8.47. An agency must be able to identify a specific provision in the agreement that requires, or grants a discretion to, the agency to disclose the type of information. The meaning of 'required' and 'authorised' is discussed in more detail in Chapter B (Key concepts).

8.48. The exception is intended to include all forms of agreements relating to information sharing (for example, treaties and exchanges of letters)[10] to which Australia is a party.

Disclosure of personal information to an overseas recipient for an enforcement related activity

8.49. An agency may disclose personal information to an overseas recipient without complying with APP 8.1 where both of the following apply:

- the agency reasonably believes that the disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body, and
- the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body (APP 8.2(f)).

8.50. This exception is intended to enable an agency that is an enforcement body to cooperate with international counterparts for enforcement related activities.

8.51. 'Enforcement body' is defined in s 6(1) as a list of specific bodies. The list includes Commonwealth, State and Territory bodies that are responsible for policing, criminal investigations, and administering laws to protect the public revenue or to impose penalties or sanctions. Examples of Commonwealth enforcement bodies are the Australian Federal Police, Australian Crime Commission, Customs, the Integrity

[10] Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, p. 84.

Commissioner,[11] Australian Prudential Regulation Authority and Australian Securities and Investments Commission.

8.52. 'Enforcement related activities' is defined in s 6(1) and discussed in Chapter B (Key concepts). For further discussion of a similar exception in APP 6.2(e), see Chapter 6.

When is an APP entity accountable for personal information that it discloses to an overseas recipient?

8.53. An APP entity that discloses personal information to an overseas recipient is accountable, in certain circumstances, for an act or practice of the overseas recipient in relation to the information that would breach the APPs (s 16C(1)). Accountable means that the act or practice is taken to have been done by the APP entity and to be a breach of the APPs by that entity (s 16C(2)).

8.54. This accountability provision only applies where:

- APP 8.1 applies to the disclosure – that is, none of the exceptions in APP 8.2 apply to the disclosure
- the APPs do not apply to an act or practice of the overseas recipient in relation to the information - for example, where an exemption to the Privacy Act applies to the recipient (Part II) or where the recipient is not an agency and does not have an Australian link (the term Australia link is discussed in more detail in Chapter B (Key Concepts)),[12] and
- the overseas recipient's act or practice would breach the APPs (other than APP 1) if it had applied to the conduct (s 16C(1)).

8.55. Under the accountability provision, an APP entity may be liable for the acts or practices of the overseas recipient (and the individual will have a means of redress) even where:

- the entity has taken reasonable steps to ensure the overseas recipient complies with the APPs (see APP 8.1) and the overseas recipient subsequently does an act or practice that would breach the APPs
- the overseas recipient discloses the individual's personal information to a subcontractor and the subcontractor breaches the APPs[13]
- the overseas recipient inadvertently breaches the APPs in relation to the information.

Overseas acts or practices required by a foreign law

8.56. Section 6A(4) provides that an act or practice required by an applicable law of a foreign country will not breach the APPs if it is done, or engaged in, outside Australia and

[11] 'Integrity Commissioner' is defined in s 6(1) as having the same meaning as in the *Law Enforcement Integrity Commissioner Act 2006*.
[12] See section 5B of the Privacy Act about the extra-territorial operation of the Privacy Act.
[13] Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, p. 84

the external Territories. The meaning of 'required' by a law is discussed in Chapter B (Key concepts).

8.57. The effect of this provision is that where an overseas recipient of personal information does an act or practice that is required by an applicable foreign law, this will not breach the APPs. The APP entity will also not be responsible for the act or practice under the accountability provision.

8.58. For example, the Patriot Act (USA) may require the overseas recipient to disclose personal information to the Government of the United States of America.[14] In these circumstances, the APP entity would not be responsible under the accountability provision for the disclosure required by that Act.

8.59. An APP entity should consider notifying an individual, if applicable, that the overseas recipient may be required to disclose their personal information under a foreign law. The entity could also explain that the disclosure will not breach the APPs. This information could be included in the APP entity's APP 5 notice (for a more detailed discussion of the requirements for notice at the time of collection, see Chapter 5).

8.60. This provision does not apply to acts or practices that are done or engaged in, within Australia. Where a foreign law requires an APP entity in Australia to disclose personal information to an overseas recipient the entity must comply with APPs 6 and 8.

[14] See *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act 2001*