Australian Government

Office of the Australian Information Commissioner

Australian Privacy Principles and National Privacy Principles – Comparison Guide

Summary and analysis of key differences for organisations

April 2013

Contents

Introduction to the Guide

The 13 Australian Privacy Principles (APPs) replace the National Privacy Principles (NPPs) for organisations from 12 March 2014. The APPs are found in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth).[1]

Part 1 of this Guide summarises the key differences between the two sets of principles, including the new obligations that apply to organisations. Part 2 of the Guide provides a comprehensive analysis of the differences between the APPs and the NPPs.

The APPs are a single set of principles that apply to both agencies and organisations, which are together defined as APP entities. While the APPs apply to all APP entities, in some cases, they impose specific obligations that apply only to organisations or only to agencies. As the purpose of this Guide is to highlight the differences between the NPPs and the APPs, and the new obligations that apply to organisations, it continues to use the term 'organisation' throughout.

This Guide is designed to be read with reference to the text of the NPPs and the APPs and does not purport to reproduce these principles in their entirety. Section references throughout the document are to the *Privacy Act 1988* (Cth).[2]

[1] See *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) <www.comlaw.gov.au/Details/C2012A00197>.

[2] See *Privacy Act 1988* (Cth) <www.comlaw.gov.au/Details/C2012C00903>.

Part 1 – Summary of changes

'Permitted general situations' and 'permitted health situations'

The amendments to the Privacy Act introduce the concept of a 'permitted general situation' and a 'permitted health situation'. The existence of a permitted general situation or permitted health situation is an exception to various obligations in the APPs.

A new s 16A outlines seven permitted general situations, where the collection, use or disclosure by an APP entity of personal information about an individual, or of a government related identifier, will not be a breach of certain APP obligations.

New s 16B outlines five permitted health situations, where the collection, use or disclosure of certain health information or genetic information, will not be a breach of certain APP obligations.

APP 1 – open and transparent management of personal information

APP 1 requires organisations to have ongoing practices and policies in place to ensure that they manage personal information in an open and transparent way.

APP 1 introduces more prescriptive requirements for privacy policies than the existing requirements in NPP 5.1. An organisation must have an APP privacy policy that contains specified information, including the kinds of personal information it collects, how an individual may complain about a breach of the APPs, and whether the organisation is likely to disclose information to overseas recipients. An organisation needs to take reasonable steps to make its APP privacy policy available free of charge and in an appropriate form.

APP 1 also introduces a positive obligation for organisations to implement practices, procedures and systems that will ensure compliance with the APPs and any registered APP codes.

For a more detailed comparison of APP 1 and NPP 5, see 'Openness' on page 16.

APP 2 – anonymity and pseudonymity

APP 2 sets out a new requirement that an organisation provide individuals with the option of dealing with it using a pseudonym. This obligation is in addition to the existing requirement that organisations provide individuals with the option of dealing with them anonymously.

Both requirements are subject to certain limited exceptions, including where it is impracticable for the organisation to deal with an individual who has not identified themselves, or where the law or a court/tribunal order requires or authorises the organisation to deal with individuals who have identified themselves.

For a more detailed comparison of APP 2 and NPP 8, see 'Anonymity' on page 21.

APP 3 – collection of solicited personal information

APP 3 outlines when and how an organisation may collect personal and sensitive information that it solicits from an individual or another entity.

An organisation must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the organisation's functions or activities.

APP 3 clarifies that, unless an exception applies, sensitive information must only be collected with an individual's consent if the collection is also reasonably necessary for one or more of the organisation's functions or activities.

An organisation must only collect personal information from the individual, unless it is unreasonable or impracticable to do so.

For a more detailed comparison of APP 3 and NPP 1, see 'Collection' on page 10, and between APP 3 and NPP 10, see 'Sensitive information' on page 24.

APP 4 – dealing with unsolicited personal information

APP 4 creates new obligations in relation to the receipt of personal information which is not solicited.

Where an organisation receives unsolicited personal information, it must determine whether it would have been permitted to collect the information under APP 3. If so, APPs 5 to 13 will apply to that information.

If the information could not have been collected under APP 3, and the information is not contained in a Commonwealth record, the organisation must destroy or de-identify that information as soon as practicable, but only if it is lawful and reasonable to do so.

For a more detailed comparison of APP 4 and NPP 1, see 'Collection' on page 10.

APP 5 – notification of the collection of personal information

APP 5 specifies certain matters about which an organisation must generally make an individual aware, at the time, or as soon as practicable after, the organisation collects their personal information.

In addition to the matters listed in NPP 1.3, APP 5 requires organisations to notify individuals about the access, correction and complaints processes in their APP privacy policies, and also the location of any likely overseas recipients of individuals' information.

For a more detailed comparison of APP 5 and NPP 1, see 'Collection' on page 10.

APP 6 – use and disclosure of personal information

APP 6 outlines the circumstances in which an organisation may use or disclose the personal information that it holds about an individual.

APP 6 generally reflects the NPP 2 use and disclosure obligations. In addition, APP 6 introduces a limited number of new exceptions to the general requirement that an organisation only uses or discloses personal information for the purpose for which the information was collected. These exceptions include where the use or disclosure is reasonably necessary:

- to assist in locating a missing person
- to establish, exercise or defend a legal or equitable claim, or
- for the purposes of a confidential alternative dispute resolution.

For a more detailed comparison of APP 6 and NPP 2, see 'Use and disclosure' on page 12.

APP 7 – direct marketing

The use and disclosure of personal information for direct marketing is now addressed in a discrete privacy principle (rather than as an exception in NPP 2).

Generally, organisations may only use or disclose personal information for direct marketing purposes where the individual has either consented to their personal information being used for direct marketing, or has a reasonable expectation that their personal information will be used for this purpose, and conditions relating to opt-out mechanisms are met.

APP 7.5 permits contracted service providers for Commonwealth contracts to use or disclose personal information for the purpose of direct marketing if certain conditions are met.

For a more detailed comparison of APP 7 and NPP 2, see 'Use and disclosure' on page 12.

APP 8 – cross-border disclosures

APP 8 and a new s 16C introduce an accountability approach to organisations' cross-border disclosures of personal information.

Before an organisation discloses personal information to an overseas recipient, the organisation must take reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to that information. In some circumstances an act done, or a practice engaged in, by the overseas recipient that would breach the APPs, is taken to be a breach of the APPs by the organisation. There are a number of exceptions to these requirements.

For a more detailed comparison of APP 8 and NPP 9, see 'Transborder data flows' on page 22.

APP 9 – adoption, use or disclosure of government related identifiers

APP 9 prohibits an organisation from adopting, using or disclosing a government related identifier unless an exception applies. APP 9 generally retains the same exceptions as NPP 7, with some additions and amendments.

The terms 'identifier' and 'government related identifier' are now defined in s 6.[3]

For a more detailed comparison of APP 9 and NPP 7, see 'Identifiers' on page 20.

APP 10 – quality of personal information

Under APP 10, an organisation must take reasonable steps to ensure the personal information it collects is accurate, up-to-date and complete (as required by NPP 3).

In relation to use and disclosure, the quality requirements differ from NPP 3. For uses and disclosures, the personal information must be relevant, as well as, accurate, up-to-date and complete, having regard to the purpose of the use or disclosure.

For a more detailed comparison of APP 10 and NPP 3, see 'Data quality' on page 15.

APP 11 – security of personal information

APP 11 requires an organisation to take reasonable steps to protect the personal information it holds from interference, in addition to misuse and loss, and unauthorised access, modification and disclosure (as required by NPP 4.1).

Like NPP 4.2, APP 11 requires an organisation to take reasonable steps to destroy or de-identify personal information if the organisation no longer needs it for any authorised purpose. Under APP 11 there are two exceptions to this requirement:

- the personal information is contained in a Commonwealth record, or
- the organisation is required by or under an Australian law or a court/tribunal order to retain the information.

For a more detailed comparison of APP 11 and NPP 4, see 'Data security' on page 15.

APP 12 – access to personal information

The APPs separate the access and correction requirements into two separate principles.

Like NPP 6, APP 12 requires an organisation to give an individual access to the personal information that it holds about that individual, unless an exception applies. The exceptions are substantially similar to the exceptions in NPP 6.

There is a new requirement for organisations to respond to requests for access within a reasonable period. In addition, organisations must give access in the manner requested by the individual if it is reasonable to do so. If an organisation decides not to give an individual access, it must generally provide written reasons for the refusal and the mechanisms available to complain about the refusal.

If an organisation charges an individual for giving access to the individual's personal information, the charge must not be excessive, and must not apply to the making of the request.

[3] See Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) <http://www.comlaw.gov.au/Details/C2012A00197>.

For a more detailed comparison of APP 12 and NPP 6, see 'Access and correction' on page 17.

APP 13 – correction of personal information

APP 13 introduces some new obligations in relation to for correcting personal information, which differ from those in NPP 6. The APPs remove the NPP 6 requirement for an individual to establish that their personal information is inaccurate, incomplete or is not up-to-date and should be corrected.

APP 13 now requires an organisation to take reasonable steps to correct personal information to ensure that, having regard to a purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading, if either:

- the organisation is satisfied that it needs to be corrected, or
- an individual requests that their personal information be corrected.

Organisations generally need to notify other APP entities that have been provided with the personal information of any correction, if that notification is requested by the individual.

APP 13 contains similar provisions to NPP 6 in relation to associating a statement with the personal information if the organisation refuses to correct the information and the individual requests a statement to be associated.

An organisation must also respond to a correction request or a request to associate a statement by the individual within a reasonable period after the request is made, and must not charge the individual for making the request, for correcting the personal information, or for associating the statement with the personal information.

When refusing an individual's correction request, an organisation must generally provide the individual with written reasons for the refusal and notify them of available complaint mechanisms.

For a more detailed comparison of APP 13 and NPP 6, see 'Access and correction' on page 17.

Part 2 – Analysis of differences between NPPs and APPs

Collection

Summary of NPP 1

NPP 1 states that an organisation must:

- not collect personal information unless it is necessary for one or more of its functions or activities
- only collect personal information by lawful and fair means, and not in an unreasonably intrusive way
- where reasonable and practicable, only collect personal information from the individual concerned.

NPP 1 also outlines the information that organisations must take reasonable steps to ensure individuals are aware of at or before the time of collecting personal information, including:

- the purposes for which the information is collected, and
- the organisations to which information of that kind is usually disclosed.

Relevant APPs

APP 2 – anonymity and pseudonymity

APP 3—collection of solicited personal information

APP 4—dealing with unsolicited personal information

APP 5 – notification of the collection of personal information

Key differences

APP 2 – anonymity and pseudonymity

APP 2 requires an organisation to provide an individual with the option of not identifying themselves, or of using a pseudonym, when dealing with the organisation in relation to a particular matter. Exceptions apply to this requirement. APP 2 is discussed in more detail under ‘Anonymity’ on p 21 of this Guide.

APP 3—collection of solicited personal information

APP 3 deals with the collection of personal information that is solicited by an organisation. There are no material changes to when and how an organisation can collect personal information (other than sensitive information), noting that:

- APP 3.2 states that an organisation must not collect personal information (other than sensitive information) unless it is ‘reasonably necessary’ for one of its functions or activities (whereas NPP 1.1 used the term ‘necessary’). However, this does not

reflect a change in when personal information can be collected, as 'necessary' in NPP 1.1 is generally considered to imply an objective test.

- APP 3.5 states that personal information must be collected 'only by lawful and fair means'. While the NPP 1 words 'not in an unreasonably intrusive way' are not expressly mentioned, the concept of 'fair' extends to the obligation not to use 'unreasonably intrusive' means.

See 'Sensitive information' on p 24 for a discussion of the elements of APP 3 that are relevant to the handling of sensitive information, including exceptions relating to 'permitted general situations' and 'permitted health situations' contained in ss 16A and 16B respectively.

APP 4 —dealing with unsolicited personal information

APP 4 is a new principle applying to the receipt of personal information which is not solicited. Unsolicited personal information must be afforded the same privacy protection as solicited personal information.

Where unsolicited personal information is received:

- an organisation must determine whether it could have collected the information under APP 3 (APP 4.1)
- if the information could have been collected, then APPs 5 to 13 apply to the information (APP 4.4)
- if the organisation could not have collected the information, it must destroy or de-identify the information as soon as practicable, but only if lawful and reasonable to do so, and only if the information is not contained in a Commonwealth record (APP 4.3).

APP 5 – notification of the collection of personal information

APP 5 maintains all of the NPP 1 notification requirements, but also requires an organisation to take reasonable steps to notify an individual, or otherwise ensure that the individual is aware:

- that its APP privacy policy contains information about how to access and seek correction of personal information, and information about the organisation's complaints process (APP 5.2(g)-(h))
- of whether it is likely to disclose an individual's personal information to overseas recipients and, if it is practicable to specify, the countries in which those recipients are likely to be located (APP 5.2(i)-(j)). If it is not practicable to specify the countries in the notification, the organisation may make the individual aware of them in another way.

If the organisation collects the personal information from someone other than the individual, or the individual may not be aware that the organisation has collected the personal information, it must also take reasonable steps to notify an individual, or otherwise ensure that the individual is aware:

- that the organisation collects or has collected the information, and
- of the circumstances of that collection (APP 5.2(b)).

Use and disclosure

Summary of NPP 2

An organisation must not use or disclose personal information for a purpose (the secondary purpose) other than the primary purpose of collection, unless an exception applies (NPP 2.1).

Exceptions include where:

- the secondary purpose is related to the primary purpose, and the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose (NPP 2.1(a))
- the individual has consented to the use or disclosure (NPP 2.1(b))
- the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety; or a serious threat to public health or safety (NPP 2.1(e))
- the organisation uses or discloses the personal information in investigating a suspicion of unlawful activity or in reporting its concerns to relevant persons or authorities (NPP 2.1(f))
- the use or disclosure is required or authorised by or under law (NPP 2.1(g)).

NPP 2.1(c) allows organisations to use non-sensitive personal information for the secondary purpose of direct marketing where, among other things:

- it is impracticable to seek the individual's consent before using their information and
- the individual is told that they may express a wish not to receive any further direct marketing communications, and has not made such a request.

Relevant APPs

APP 6 – use or disclosure of personal information

APP 7 – direct marketing

Key differences

APP 6 – use or disclosure of personal information

Under APP 6, if an organisation collects personal information about an individual for a particular purpose (the primary purpose), it must not use or disclose the information for another purpose (the secondary purpose) unless the individual consents to the use or disclosure, or another exception applies.

APP 6 retains all of the NPP 2.1 exceptions, with some amendments, and introduces a limited number of new exceptions, which permit the use or disclosure of personal information for secondary purposes.

The exceptions in APP 6 that broadly reflect the NPP 2.1 exceptions are where the use or disclosure for a secondary purpose is:

- required or authorised by or under an Australian law or a court/tribunal order (APP 6.2(b)).

  Definitions of the terms 'Australian law' and 'court/tribunal order' have been inserted into s 6 in order to clarify the scope of this exception.[4]

- necessary to lessen or prevent a serious threat to any individual's life, health or safety, or to public health or safety, and it is unreasonable or impracticable to obtain the consent of the individual whose personal information is to be used or disclosed (APP 6.2(c), permitted general situation 1 (s 16A(1), item 1)).

  The requirement for the threat to be imminent has been removed. The removal of the imminence requirement is balanced by the introduction of the requirement to assess whether it is unreasonable or impracticable to seek consent.

- necessary in order for an organisation to take appropriate action in relation to a reasonable suspicion of unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities (APP 6.2(c), permitted general situation 2 (s 16A(1), item 2)).

  The requirement that the unlawful activity or serious misconduct must relate to the entity's functions or activities is new. It is intended to clarify that this exception applies to an entity's internal investigations.

APP 6.2(e) permits the use or disclosure of personal information for a secondary purpose to an enforcement body for one or more enforcement related activities. The term 'enforcement related activities' is now defined in s 6, and generally replicates the activities of enforcement bodies that are listed in NPP 2.1(h).[5] Two new activities have been included:

- the conduct of surveillance activities, intelligence gathering activities or monitoring activities
- the conduct of protective or custodial activities.

APP 6 adds new exceptions for organisations, where the use or disclosure of personal information for a secondary purpose is reasonably necessary:

- to assist any APP entity, body or person to locate a person who has been reported as missing (where the entity reasonably believes that this use or disclosure is reasonably necessary, and where that use or disclosure complies with rules made by the Commissioner under s 16A(2)) (APP 6.2(c), permitted general situation 3 (s 16 A (1), item 3))
- for the establishment, exercise or defence of a legal or equitable claim (APP 6.2(c), permitted general situation 4 (s 16A(1), item 4))

[4] See Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) <http://www.comlaw.gov.au/Details/C2012A00197>.

[5] See Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) <http://www.comlaw.gov.au/Details/C2012A00197>.

- for the purposes of a confidential alternative dispute resolution process (APP 6.2(c), permitted general situation 5 (s 16A(1), item 5)).

APP 7 – direct marketing

APP 7 takes a different approach to the direct marketing provisions in NPP 2.1(c). APP 7 addresses direct marketing as a discrete subject, rather than as a type of secondary purpose of collection, as in NPP 2.

Generally, organisations may only use or disclose personal information for direct marketing purposes if an exception, listed in APPs 7.2 to 7.5, applies.

The exception in APP 7.2 is similar to the current exception for use and disclosure of personal information in NPP 2.1(a)(ii), that 'the individual would reasonably expect the organisation to use or disclose the information for a secondary purpose'. APP 7.2 applies this requirement specifically to direct marketing.

Under APP 7.2, an organisation may use or disclose personal information (other than sensitive information) about an individual if:

- it collected the information from the individual
- the individual would reasonably expect that their personal information would be used or disclosed for direct marketing
- the organisation has provided a simple means by which the individual can request not to receive direct marketing, and
- the individual has not made such a request.

Under APP 7.3, where an individual would not reasonably expect his or her personal information to be used for direct marketing, or the information has been collected from a third party, an organisation may only use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

- the individual has consented to the use or disclosure for this purpose, or it is impracticable to seek this consent
- the organisation has provided a simple means by which the individual can opt out of direct marketing and the individual has not opted out, and
- in each direct marketing communication the organisation must include a prominent statement telling the individual that he or she may request to no longer receive direct marketing, and no request is made.

APP 7.4 requires an organisation to obtain the consent of the individual before using or disclosing sensitive information for the purpose of direct marketing.

If the organisation is a contracted service provider for a Commonwealth contract, it may use or disclose personal information for the purpose of direct marketing if doing so meets an obligation under the contract (APP 7.5).

APP 7 also gives an individual the right to contact an organisation to:

- request not to receive direct marketing communications from that organisation (APP 7.6(c))
- request the organisation not to disclose their personal information to other organisations for the purposes of direct marketing (APP 7.6(d)), or
- request the organisation to provide its source of the individual's personal information (APP 7.6(e)).

The organisation must comply with these requests within a reasonable period and free of charge. They do not need to comply with requests to disclose the source of information if it is impracticable or unreasonable to do so (APP 7.7).

APP 7 is subject to the operation of other direct marketing legislation, including the *Do Not Call Register Act 2006* and the *Spam Act 2003* (APP 7.8).

Data quality

Summary of NPP 3

An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

Relevant APPs

APP 10 – quality of personal information

Key differences

APP 10 contains the same obligations as NPP 3, requiring an organisation to take reasonable steps to ensure that the personal information that it collects is accurate, up-to-date and complete.

In relation to use and disclosure, the APP 10 requirements differ from NPP 3. For uses and disclosures, an organisation will need to take reasonable steps to ensure that the personal information is accurate, up-to-date, and complete as well as relevant, having regard to the purpose of that use or disclosure.

Data security

Summary of NPP 4

An organisation must take reasonable steps to ensure that the personal information it holds is:

- protected from misuse and loss, and from unauthorised access, modification, or disclosure and
- destroyed or permanently de-identified if it is no longer required for any purpose for which it may be used or disclosed under NPP 2.

Relevant APPs

APP 11 – security of personal information

Key differences

APP 11.1 imposes the same obligation as NPP 4 in relation to the protection of the personal information that an organisation holds. However, APP 11.1 now also requires organisations to protect personal information from interference.

APP 11.2 introduces new exceptions to the requirement that an organisation take reasonable steps to destroy or de-identify personal information, once it is no longer needed for any purpose for which it may be used or disclosed in accordance with the APPs:

- if it is not contained in a Commonwealth record (APP 11.2(c))[6], and
- if the organisation is not required by or under an Australian law, or a court/tribunal order, to retain the information (APP 11.2(d)).[7]

Openness

Summary of NPP 5

An organisation must have a document that sets out clearly expressed policies about how it manages personal information, and make it available to anyone who asks for it. If requested by an individual, an organisation must let that individual know, generally, what sort of personal information it holds, for what purposes, and how it handles that information.

Relevant APPs

APP 1 – open and transparent management of personal information

Key differences

APP 1.2 introduces the requirement for an organisation to take reasonable steps to implement practices, procedures and systems relating to the organisation's functions or activities that:

- will ensure that the organisation complies with the APPs and any registered APP code that binds the organisation, and

[6] A definition of 'Commonwealth record' has been inserted into s 6. The term has the same meaning as in the *Archives Act 1983*, which is: '(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.' See Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) <http://www.comlaw.gov.au/Details/C2012A00197>.

[7] Definitions of the terms 'Australian law' and 'court/tribunal order' have been inserted into s 6 of the Act in order to clarify the scope of this exception. See Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) <http://www.comlaw.gov.au/Details/C2012A00197>.

- will enable the organisation to deal with inquiries or complaints from individuals.

APP 1.3 specifies that, not only must an organisation's APP privacy policy be clearly expressed, it must also be up-to-date.

APP 1 expands on the requirements in NPP 5 by identifying the minimum information that must be contained in an organisation's APP privacy policy (APP 1.4). This includes:

- how an individual can access and seek correction of their personal information
- how to complain about a breach of the APPs, and how the organisation will deal with such a complaint, and
- whether the organisation is likely to disclose personal information to overseas recipients, and if practicable, in which countries these recipients are likely to be located.

APP 1 also introduces a new obligation on organisations to take reasonable steps to make their privacy policies available:

- free of charge (APP 1.5(a))
- in an appropriate form (APP 1.5(b)), and
- in the form that an individual or body requests (APP 1.6).

Access and correction

Summary of NPP 6

An organisation must provide an individual with access to the personal information it holds about them, unless an exception applies. Exceptions include:

- access to personal information other than health information, where giving access would pose a serious and imminent threat to the life or health of any individual (NPP 6.1(a))
- access to health information, where providing access would pose a serious threat to the life or health of any individual (NPP 6.1(b))
- where denying access is required or authorised by or under law (NPP 6.1(h))
- where providing access would be likely to prejudice an investigation of possible unlawful activity (NPP 6.1(i))
- where providing access would be likely to prejudice actions by or on behalf of an enforcement body in relation to unlawful activity or seriously improper conduct (NPP 6.1(k)).

If an organisation is not required to provide the individual with access to the information, the organisation must consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties (NPP 6.3).

If an individual is able to establish that their personal information is not accurate, complete and up-to-date, an organisation must take reasonable steps to correct the information (NPP

6.5). If the organisation and the individual disagree about the accuracy, completeness and currency of the information, the organisation must attach a statement to the information noting this, if the individual requests it to do so (NPP 6.6).

An organisation must give reasons for denial of access or a refusal to correct personal information (NPP 6.7).

Relevant APPs

APP 12 – access to personal information

APP 13 – correction of personal information

Key differences

The APPs divide access and correction across two separate principles: APP 12 and APP 13.

APP 12 - access to personal information

Consistent with the access principle in NPP 6.1, APP 12 requires organisations to give an individual access to their personal information, at the request of that individual. APP 12 retains the NPP 6 exceptions to this principle, with some amendments.

APP 12.3(a) combines the two exceptions relating to a 'serious threat', and:

- removes the distinction between health information and information other than health information
- removes the requirement that the threat must be imminent
- introduces a ground for the organisation to refuse access based on a serious threat to public health or safety.

Access may now be denied if required or authorised by or under an Australian law or a court/tribunal order (APP 12.3(g)).[8]

APP 12.3(h) expands on the NPP 6.1(i) exception relating to unlawful activity. Under the APPs, an entity is not required to give an individual access to their personal information if:

- 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
- giving access would be likely to prejudice the taking of appropriate action in relation to the matter.

Under APP 12.3(i), an organisation is not required to give an individual access to their personal information if giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body. The term

[8] Definitions of the terms 'Australian law' and 'court/tribunal order' have been inserted into s 6 of the Act in order to clarify the scope of this exception. See Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)* <http://www.comlaw.gov.au/Details/C2012A00197>.

'enforcement related activities' is now defined in s 6, and generally replicates the activities of enforcement bodies that are listed in NPP 6.1(j).[9]

Where an organisation refuses access on one of the specified grounds of refusal, APP 12.5 requires the organisation to take reasonable steps to give access in a way that meets the needs of the entity and the individual. This could include giving access through the use of a mutually agreed intermediary (APP 12(6)). This strengthens the obligation under NPP 6.3 to 'consider' the use of a mutually agreed intermediary.

APP 12.8 retains the same obligations as NPP 6.4 in relation to access charges. If an organisation charges an individual for giving access to the individual's personal information, the charge must not be excessive, and must not apply to the making of the request.

APP 12 is more specific about the information that an organisation must give to an individual if it refuses to give access, or refuses to give access in the manner requested by the individual. An organisation must provide a written notice that outlines:

- the reasons for the refusal, unless, having regards to the grounds for the refusal, it would be unreasonable to do so
- the complaint mechanisms available to the individual, and
- any other matters prescribed by the regulations (APP 12.9).

APP 12.4 introduces a new requirement for organisations to respond to a request for access within a reasonable period, and in the manner requested by the individual, if it is reasonable and practicable to do so.

APP 13 – correction of personal information

APP 13 expands on the correction principle in the NPPs. It amends the requirement in NPP 6.5 for an individual to establish that their personal information is not accurate, complete and up-to-date.

Instead, if:

- an organisation is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out-of-date, incomplete or irrelevant or misleading, or
- the individual to whom the personal information relates requests the organisation to correct the information

the organisation must take reasonable steps to correct the personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading.

If an organisation corrects personal information about an individual that it has previously disclosed to another APP entity, the organisation must take reasonable steps to notify the

[9] See discussion of the new definition of 'enforcement related activities' under 'Use and disclosure' on page 12. See Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) <http://www.comlaw.gov.au/Details/C2012A00197>.

other APP entity of the correction, where that notification is requested by the individual (APP 13.2).

APP 13.3 requires an organisation to provide an individual with written notice if it refuses to correct the personal information as requested by the individual. The written notice must set out:

- the reason for refusal (unless this would be unreasonable)
- the mechanisms available to complain about the refusal, and
- any other matter prescribed by regulation.

If an organisation refuses to make a correction, and an individual requests that a statement be attached to the record stating that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, the organisation generally needs to attach this statement in a way that will make the statement apparent to users of the information (APP 13.4).

APP 13.5 introduces a new requirement for an organisation to respond to a correction request within a reasonable period. The organisation must not charge the individual for making the request, for correcting the information or for associating the statement with the personal information (APP 13.5).

Identifiers

Summary of NPP 7

An organisation must not adopt as its own identifier, an identifier assigned by an agency, an agent of an agency acting in this capacity, or a contracted service provider for a Commonwealth contract acting in this capacity (NPP 7.1). An organisation that has been prescribed by regulations may adopt a prescribed identifier in prescribed circumstances (NPP 7.1A).

An organisation must not use or disclose an identifier unless a listed exception applies (NPP 7.2). The exceptions include where:

- the use or disclosure is necessary for the organisation to fulfil its obligations to the agency or
- the organisation has been prescribed by regulations to use or disclose a prescribed identifier in prescribed circumstances.

NPP 7.2 also refers to exceptions 2.1(e) to 2.1(h) in NPP 2, and permits organisations to use or disclose an identifier if one or more of these exceptions apply. See the summary of NPP 2 on page 12 for an outline of these exceptions.

An identifier ‘includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation’s operations’.

Relevant APPs

APP 9 – adoption, use or disclosure of government related identifiers

Key differences

APP 9 states that an organisation must not adopt, use or disclose a government related identifier of an individual as its own identifier of the individual unless an exception applies.

The new term 'government related identifier' is defined in s 6 and adds State and Territory authorities to the list of entities that can assign identifiers.[10]

The definition of 'identifier' is now also included in s 6 and has been expanded to specify that an identifier can be a number, letter or symbol, or a combination of any or all of these, and can be used to identify the individual or to verify the identity of the individual.[11]

APP 9.1 prohibits an organisation from adopting a government related identifier of an individual as its own identifier unless an exception applies. APP 9.1 adds a new exception to the existing NPP 7 exceptions, which will permit the adoption of a government related identifier if required or authorised by or under an Australian law or a court/tribunal order.[12]

APP 9.2 prohibits the use and disclosure of government related identifiers by organisations, unless an exception applies. APP 9.2 retains the NPP 7.2 exceptions with some amendments and some additions. Some of the main amendments and additions are:

- where the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions (APP 9.2(a))
- where the use or disclosure is required or authorised by a court/tribunal order(APP 9.2(c)), or
- where the use or disclosure is reasonably necessary for an enforcement related activity being conducted by, or on behalf of, an enforcement body (APP 9.2(e)) (see discussion of the new definition of 'enforcement related activities' under 'Use and disclosure' on page 12).

Anonymity

Summary of NPP 8

Where lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

[10] See Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) <http://www.comlaw.gov.au/Details/C2012A00197>.

[11] See Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) <http://www.comlaw.gov.au/Details/C2012A00197>.

[12] Definitions of the terms 'Australian law' and 'court/tribunal order' have been inserted into s 6 of the Act in order to clarify the scope of this exception. See Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) <http://www.comlaw.gov.au/Details/C2012A00197>.

Relevant APPs

APP 2 – anonymity and pseudonymity

Key differences

APP 2 introduces the concept of pseudonymity, in addition to anonymity. Under APP 2, individuals must have the option of not identifying themselves or of using a pseudonym when dealing with an organisation.

APP 2 introduces exceptions to this requirement:

- where the organisation is required or authorised by or under an Australian law, or a court/tribunal order,[13] to deal with individuals who have identified themselves (APP 2.2(a)) or
- where it is impracticable to deal with individuals who have not identified themselves (APP 2.2(b)).

Transborder data flows

Summary of NPP 9

An organisation in Australia or an external Territory may only transfer personal information to someone in a foreign country if:

- the organisation reasonably believes that the recipient is subject to a law, binding scheme or contract which effectively upholds the principles for the fair handling of the information that are substantially similar to the NPPs (NPP 9(a)) or
- the individual consents to the transfer (NPP 9(b)) or
- the transfer is necessary for the performance of a contract between the individual and the organisation (or related pre-contractual measures) (NPP 9(c)) or
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party (NPP 9(d)) or
- the transfer is for the benefit of the individual, and it is impracticable to obtain the consent of the individual, and if it were practicable to obtain consent, the individual would be likely to give it (NPP 9(e)) or
- the organisation has taken reasonable steps to ensure that the information will not be handled by the recipient inconsistently with the NPPs (NPP 9(f)).

[13] Definitions of the terms 'Australian law' and 'court/tribunal order' have been inserted into s 6 of the Act in order to clarify the scope of this exception. See Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) <http://www.comlaw.gov.au/Details/C2012A00197>.

Relevant APPs

APP 8 – cross border disclosure of personal information

Key differences

APP 8.1 introduces a new accountability approach to cross-border disclosure of personal information. Before an organisation discloses personal information to an overseas recipient, the organisation must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information (APP 8.1).

In certain circumstances an act done, or a practice engaged in, by the overseas recipient is taken to have been done, or engaged in, by the organisation and to be a breach of the APPs by that organisation (s 16C, see Note to APP 8.1). Generally, this will apply where:

- APP 8.1 applies to the disclosure (APP 8.1 applies to all cross-border disclosures of personal information, unless an exception in APP 8.2 applies), and
- the overseas recipient is not subject to the APPs, but the act or practice would be a breach of the APPs if they were.

APP 8.2 lists a number of exceptions to APP 8.1. For example, APP 8.1 will not apply where:

- the organisation reasonably believes that the recipient is subject to a law or binding scheme that has the effect of protecting the information in a way that is, overall, substantially similar to the APPs; and there are mechanisms available to the individual to enforce that protection or scheme (APP 8.2(a)). The requirement for an overseas jurisdiction to have accessible enforcement mechanisms introduces a higher threshold than the equivalent NPP 9 exception.
- an individual consents to the cross-border disclosure, after the organisation informs them that APP 8.1 will no longer apply if they give their consent (APP 8.2(b)).

APP 8.2 also introduces a number of new circumstances in which APP 8.1 will not apply:

- where the cross border disclosure is required or authorised by or under an Australian law, or a court/tribunal order (APP 8.2(c))
- where an organisation reasonably believes that 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 (APP 8.2(d), s16A item 1)
- where an organisation reasonably believes that the disclosure is necessary to take action in relation to the suspicion of unlawful activity or misconduct of a serious nature that relates to the organisation's functions or activities (APP 8.2(d), s 16A item 2)
- where an organisation reasonably believes that the disclosure is necessary to assist any APP entity, body or person to locate a person who has been reported as missing (APP 8.2(d), s 16A item 3).

APP 8 does not replicate the NPP 9 exceptions relating to the performance and conclusion of contracts (NPP 9(c) and (d)). NPP 9(e) has also been removed. This relates to transfers of

information that will benefit the individual and where the individual is likely to consent to the transfer, but where it is impracticable to seek consent.

Sensitive information

Summary of NPP 10

An organisation must not collect an individual's sensitive information unless a listed exception applies (NPP 10.1). Sensitive information is defined in s 6.

NPP 10.2 and 10.3 set out specific exceptions regarding the collection of health information.

Relevant APPs

APP 3 – collection of solicited personal information

Key differences

APP 3 clarifies that an organisation must only collect sensitive information about an individual if the individual consents to the collection and the information is reasonably necessary for the organisation's functions or activities, or an exception applies (APP 3.3).

The definition of sensitive information in s 6 has been extended to include:

- biometric information that is to be used for the purpose of automated biometric verification or biometric identification or
- biometric templates.[14]

Sensitive information may also be collected about an individual:

- if required or authorised by or under an Australian law or a court/tribunal order (APP 3.4(a))[15]
- when a permitted general situation or permitted health situation applies (APP 3.4(b)-(c), s 16A).

Permitted general situations include the collection of sensitive information where:

- the entity reasonably believes that the collection 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 the individual's consent to the collection (APP 3.4(b), permitted general situation 1 (s 16A item 1)).

  This exception reflects the wording of NPP 10.1(c), but removes the requirement that the threat must be imminent. This exception also replaces the specific

[14] See Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) <http://www.comlaw.gov.au/Details/C2012A00197>.

[15] Definitions of the terms 'Australian law' and 'court/tribunal order' have been inserted into s 6 of the Act in order to clarify the scope of this exception. See Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) <http://www.comlaw.gov.au/Details/C2012A00197>.

circumstances set out in NPP 10.1(c) in which an individual may be unable to consent, with the more general 'unreasonable or impracticable'.

- 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 the entity reasonably believes that the collection is necessary for the entity to take appropriate action in relation to the matter (APP 3.4(b), permitted general situation 2 (s 16A item 2)).

  This is a new exception in relation to the collection of sensitive information.

- the entity reasonably believes that the collection is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing (APP 3.4(b), permitted general situation 3 (s 16A item 3)).

  This is a new provision in relation to the collection of sensitive information.

The permitted health situations replicate the wording of NPP 10.2 and NPP 10.3, in relation to the collection of health information for the provision of a health service and for research.

APP 3.4(e) relates to non-profit organisations and replaces NPP 10.1(d). APP 3.4(e) permits the collection of an individual's sensitive information by non-profit organisations where the information:

- relates to the activities of the organisation, and
- relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

The definition of 'non-profit organisation' is now included in s 6.[16] It states that a 'non-profit organisation' means an organisation that is a non-profit organisation, and engages in activities for cultural, recreational, political, religious, philosophical, professional, trade or trade union purposes. This definition replaces the terms 'racial' and 'ethnic' in the NPP 10.5 definition with the term 'cultural'. In addition, it also includes in the definition organisations with a 'recreational' purpose.

[16] See Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) <http://www.comlaw.gov.au/Details/C2012A00197>.