Australian Government

Office of the Australian Information Commissioner

Australian Privacy Principles Guidelines

Privacy Act 1988

Combined October 2025

OAIC

The Office of the Australian Information Commissioner (OAIC) was established on 1 November 2010 by the Australian Information Commissioner Act 2010.

All OAIC publications can be made available in a range of accessible formats for people with disabilities. If you require assistance, please contact the OAIC.

Date of initial publication: February 2014.

Creative Commons

Office of the Australian Information Commissioner

GPO Box 5218 Sydney NSW 2001

Telephone: 1300 363 992

Email: enquiries@oaic.gov.au

Web: www.oaic.gov.au

Preface

The Privacy Act 1988 (Privacy Act) s 28(1)(a) provides that the Australian Information Commissioner may make guidelines for the 'avoidance of acts or practices that may or might be interferences with the privacy of individuals, or which may otherwise have any adverse effects on the privacy of individuals'. Additionally, s 28(1)(c)(i) provides that one of the functions of the Commissioner is to promote an understanding and acceptance of the Australian Privacy Principles (APPs) and the objects of those principles.

The Australian Privacy Principles guidelines (APP guidelines) outline:

- the mandatory requirements in the APPs, which are set out in Schedule 1 of the Privacy Act
- the Information Commissioner's interpretation of the APPs, including the matters that the Office of the Australian Information Commissioner may take into account when exercising functions and powers relating to the APPs
- examples that explain how the APPs may apply to particular circumstances
- good privacy practice to supplement minimum compliance with the mandatory requirements in the APPs.

The APP guidelines are not legally binding and do not constitute legal advice about how an entity should comply with the APPs in particular circumstances. An entity may wish to seek independent legal advice where appropriate.

The APP guidelines may be updated from time to time, including to take account of changes in the Privacy Act or other legislation, determinations made under s 52 of the Privacy Act and relevant tribunal and court decisions.

Prof. John McMillan

Australian Information Commissioner

Contents

A comprehensive contents page appears at the beginning of each Chapter of the APP guidelines.

General matters

Chapter A: Introductory matters

Chapter B: Key concepts

Chapter C: Permitted general situations

Chapter D: Permitted health situations

Part 1 — Consideration of personal information privacy

Chapter 1: APP 1 — Open and transparent management of personal information

Chapter 2: APP 2 — Anonymity and pseudonymity

Part 2 — Collection of personal information

Chapter 3: APP 3 — Collection of solicited personal information

Chapter 4: APP 4 — Dealing with unsolicited personal information

Chapter 5: APP 5 — Notification of the collection of personal information

Part 3 — Dealing with personal information

Chapter 6: APP 6 — Use or disclosure of personal information

Chapter 7: APP 7 — Direct marketing

Chapter 8: APP 8 — Cross-border disclosure of personal information

Chapter 9: APP 9 — Adoption, use or disclosure of government related identifiers

Part 4 — Integrity of personal information

Chapter 10: APP 10 — Quality of personal information

Chapter 11: APP 11 — Security of personal information

Part 5 — Access to, and correction of, personal information

Chapter 12: APP 12 — Access to personal information

Chapter 13: APP 13 — Correction of personal information

Chapter A:
Introductory matters

Version 1.2, July 2019

OAIC

Contents

Purpose 3
Australian Privacy Principles (APPs) 3
Who is covered by the APPs? 5
Do the APPs apply to a contracted service provider under a Commonwealth contract? 5
Do the APPs apply to a credit reporting participant? 5
Do the APPs apply to an APP entity bound by a registered APP Code? 6
Are APP entities responsible for acts and practices of, and disclosures to, staff? 6
What happens if an APP entity breaches an APP? 6
References in the APP guidelines 7
Where do I get more information? 7
APP guidelines and Australian Capital Territory public sector agencies 7

Purpose

A.1 The Australian Information Commissioner[1] issues these Australian Privacy Principles guidelines (APP guidelines) under s 28(1) of the Privacy Act 1988 (Privacy Act).[2] These guidelines are not a legislative instrument (s 28(4)).

A.2 The APP guidelines outline:

- the mandatory requirements in the Australian Privacy Principles (APPs), which are set out in Schedule 1 of the Privacy Act — generally indicated by 'must' or 'is required to'
- the Information Commissioner's interpretation of the APPs, including the matters that the Office of the Australian Information Commissioner (OAIC) may take into account when exercising functions and powers relating to the APPs — generally indicated by 'should' or 'is expected to'
- examples that explain how the APPs may apply to particular circumstances — generally indicated by 'for example' or 'examples include'. Any examples given are not intended to be prescriptive or exhaustive of how an entity may comply with the mandatory requirements in the APPs; the particular circumstances of an entity will also be relevant
- good privacy practice to supplement minimum compliance with the mandatory requirements in the APPs — generally indicated by 'could'

A.3 The APP guidelines are not legally binding and do not constitute legal advice about how an entity should comply with the APPs in particular circumstances. An entity may wish to seek independent legal advice where appropriate.

A.4 The APP guidelines may also provide relevant guidance for Australian Capital Territory (ACT) public sector agencies covered by the Territory Privacy Principles in the ACT Information Privacy Act 2014 (see paragraphs A.29–A.32 below).

Australian Privacy Principles (APPs)

A.5 The APP guidelines should be read together with the full text of the APPs in the Privacy Act.[3]

A.6 The APPs are legally binding principles which are the cornerstone of the privacy protection framework in the Privacy Act.[4] The APPs set out standards, rights and obligations in relation to handling, holding, accessing and correcting personal information. They apply to most Australian Government (and Norfolk Island Government) agencies and some private sector organisations — collectively referred to as APP entities (see paragraphs A.12–A.14).[5]

---

[1] In the APP guidelines, where the Information Commissioner is referred to in a paragraph, all subsequent references to 'the Commissioner' within that paragraph also relate to the Information Commissioner.

[2] Section 28(1) of the Privacy Act sets out the guidance related functions of the Information Commissioner, including 'making guidelines for the avoidance of acts or practices that may or might be interferences with the privacy of individuals, or which may otherwise have any adverse effects on the privacy of individuals'.

[3] For the full text of the Australian Privacy Principles, see OAIC, Read the Australian Privacy Principles, OAIC website <https://www.oaic.gov.au/>, and Privacy Act 1988, Schedule 1, Federal Register of Legislation <https://www.legislation.gov.au/>.

[4] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 52.

[5] The APPs do not apply to Australian Capital Territory Government agencies. The Information Privacy Act 2014 (ACT) regulates how personal information is handled by ACT public sector agencies. This Act includes a set of Territory Privacy Principles, which cover the collection, use, storage and disclosure of personal information, and an individual's access to

A.7 The APPs are principles-based law. This provides APP entities with the flexibility to tailor their personal information handling practices to their diverse needs and business models, and to the diverse needs of individuals.[6] The APPs are also technology neutral, applying equally to paper-based and digital environments. This is intended to preserve their relevance and applicability, in a context of continually changing and emerging technologies.

A.8 The APPs are structured to reflect the personal information lifecycle. They are grouped into five parts:

- Part 1 — Consideration of personal information privacy (APPs 1 and 2)
- Part 2 — Collection of personal information (APPs 3, 4 and 5)
- Part 3 — Dealing with personal information (APPs 6, 7, 8 and 9)
- Part 4 — Integrity of personal information (APPs 10 and 11)
- Part 5 — Access to, and correction of, personal information (APPs 12 and 13)

A.9 The requirements in each of these principles interact with and complement each other. For example, when collecting personal information, an APP entity should consider the requirements in Part 2 as well as in Part 4 concerning the integrity of the information.

A.10 In developing the APP guidelines, the Information Commissioner has had regard to the objects of the Privacy Act, stated in s 2A:

- promoting the protection of the privacy of individuals
- recognising that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities
- providing the basis for nationally consistent regulation of privacy and the handling of personal information
- promoting responsible and transparent handling of personal information by entities
- facilitating an efficient credit reporting system while ensuring that the privacy of individuals is respected
- facilitating the free flow of information across national borders while ensuring that the privacy of individuals is respected
- providing a means for individuals to complain about an alleged interference with their privacy
- implementing Australia's international obligation in relation to privacy

A.11 The structure of the APP guidelines reflects the structure of the APPs: APPs 1 to 13 are each dealt with in separate chapters. The number of the chapter corresponds to the number of the APP. Chapters A to D contain guidance on general matters, including an explanation of key concepts that are used throughout the APPs and the APP guidelines (Chapter B), and guidance on permitted general situations (Chapter C) and permitted health situations (Chapter D), which are also relevant to a number of APPs.

---

and correction of that information. For more information about the TPPs, including how they differ from the APPs, see Privacy in the ACT, OAIC website <https://www.oaic.gov.au>.

[6] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 52.

Who is covered by the APPs?

A.12 The APPs apply to APP entities (s 15). The term 'APP entity' means an agency or organisation (s 6(1)) and is discussed in more detail in Chapter B (Key concepts).

A.13 The APPs extend to an act or practice of an APP entity occurring outside Australia and the external Territories (s 5B). However, if the APP entity is an organisation, the organisation must also have an Australian link (s 5B(1A)). The term 'Australian link' is discussed in Chapter B (Key concepts).

A.14 In some circumstances, an act or practice of an APP entity is exempt from the Privacy Act, including the APPs. For example, an act done, or a practice engaged in by a Federal Court is exempt, except for acts or practices in respect of a matter of an administrative nature (s 7(1)(a)(ii) and (b)). The 'employee records' exemption (s 7B(3)) is an example of an exemption that applies to an act or practice of an organisation.

Do the APPs apply to a contracted service provider under a Commonwealth contract?

A.15 Special provisions apply to a contracted service provider (including a subcontractor) handling personal information under a Commonwealth contract. The term 'contracted service provider' is defined in s 6(1) and includes an organisation that is or was a party to a Commonwealth contract and that is or was responsible for providing services to an agency under that contract. The term also includes a sub-contractor for the contract. The term 'Commonwealth contract' is also defined in s 6(1) to mean a contract, to which the Commonwealth, Norfolk Island or an agency is or was a party, under which services are to be, or were to be, provided to an agency.

A.16 An agency entering into a Commonwealth contract must take contractual measures to ensure that the other party (the contracted service provider) does not do an act, or engage in a practice, that would breach an APP if done or engaged in by the agency (s 95B). In effect, s 95B ensures that the contracted service provider complies with the APPs as if it were an agency in respect of its activities under the contract. However, it is the contract that is the primary source of the contracted service provider's privacy obligations in relation to its activities under the contract.

A.17 If a provision of a Commonwealth contract authorises an organisation that is a contracted service provider to do an act or practice that would otherwise breach the APPs, an act done or practice engaged in for the purposes of meeting that obligation will not breach the APPs (s 6A(2)). A contract may include such a provision where, for example, the APPs contain different requirements for agencies and organisations. An act done or practice engaged in by the contracted service provider that is contrary to or inconsistent with such a contractual provision, is an 'interference with the privacy of an individual' (s 13(3)) (see paragraph 4 below).

Do the APPs apply to a credit reporting participant?

A.18 Part IIIA of the Privacy Act contains requirements for the handling of credit-related personal information by credit reporting participants, including credit reporting bodies, credit providers and some other third party recipients of that information. The provisions in Pt IIIA make clear whether the obligations in Pt IIIA replace relevant APPs or apply in addition to relevant APPs.

A.19 The APPs will apply to any credit reporting participant that is an APP entity in relation to the handling of personal information not regulated by Pt IIIA.

Do the APPs apply to an APP entity bound by a registered APP Code?

A.20 A 'registered APP code' is defined as an APP code that is included on the Codes Register and that is in force (s 26B(1)). A registered APP code does not replace the APPs for the entities which it binds, but operates in addition to the requirements of the APPs.[7] Therefore, an APP entity that is bound by an APP code must comply with both the APPs and the APP code.

A.21 Registered APP codes are discussed in more detail in Chapter B (Key concepts).

Are APP entities responsible for acts and practices of, and disclosures to, staff?

A.22 An act done or practice engaged in by a person in one of the following categories is taken to be an act done or practice engaged in by the APP entity:

- A person employed by, or in the service of an APP entity, in performing the duties of the person's employment.
- A person on behalf of an unincorporated body or other body that is established by or under a Commonwealth (or Norfolk Island) enactment, for the purpose of assisting or performing functions in connection with an APP entity.
- A member, staff member or special member of the Australian Federal Police in performing duties as such a member (s 8(1)).

A.23 Information disclosed to a person or member in one of the preceding categories is also taken to be information disclosed to the APP entity.

What happens if an APP entity breaches an APP?

A.24 An act or practice of an APP entity that occurs on or after 12 March 2014 and that breaches an APP in relation to personal information about an individual, is 'an interference with the privacy' of the individual (s 13(1)).

A.25 The Information Commissioner has powers to investigate possible interferences with privacy, either following a complaint by the individual concerned or on the Commissioner's own initiative (Part V of the Privacy Act). Where an individual makes a complaint, the Commissioner will generally attempt to conciliate the complaint (s 40A). The Commissioner also has a range of enforcement powers and other remedies available.

[7] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 199.

References in the APP guidelines

A.26 The APP guidelines distinguish between mandatory requirements under the APPs, the Information Commissioner's interpretation of the APPs and good practice privacy guidance as discussed in paragraph A.2 above.

A.27 In the APP guidelines:

- a reference to a paragraph is to a paragraph of text in the same chapter of these guidelines
- a reference to a section of an Act is to a section of the Privacy Act or other Act as specified

Where do I get more information?

A.28 The Office of the Australian Information Commissioner (OAIC) has developed a range of materials to assist APP entities to comply with the Privacy Act, and to provide information to individuals. These are available on the OAIC website, see <https://www.oaic.gov.au>.

APP guidelines and Australian Capital Territory public sector agencies

A.29 The ACT Information Privacy Act 2014 regulates how personal information is handled by ACT public sector agencies. The Information Privacy Act includes a set of Territory Privacy Principles (TPPs), which cover the collection, use, storage and disclosure of personal information, and an individual's access to and correction of that information.

A.30 Under an arrangement between the ACT Government and the Australian Government, the Information Commissioner is exercising some of the functions of the ACT Information Privacy Commissioner. These responsibilities include handling privacy complaints against, and receiving data breach notifications from, ACT public sector agencies, and conducting assessments of ACT public sector agencies' compliance with the Information Privacy Act.

A.31 The TPPs are substantially similar to the APPs. The main differences are:

- there is no TPP equivalent to APP 7 (direct marketing) or APP 9 (adoption, use or disclosure of government related identifiers)
- the TPPs and the Information Privacy Act do not cover personal health information or health records[8]

A.32 Given these similarities, the information, examples and good privacy practices outlined in the APP guidelines may assist the general public and ACT public sector agencies to interpret and apply the TPPs. The guidelines should be read with reference to the full text of the TPPs and the Information Privacy Act.[9]

[8] For more information about the TPPs, see Privacy in the ACT, OAIC website <https://www.oaic.gov.au>

[9] See Territory Privacy Principles, OAIC website <https://www.oaic.gov.au>

Chapter B:
Key concepts

Version 1.4, December 2022

OAIC

Contents

APP entity 4
Australian Link 6
Carries on business in Australia 6
Carry on business 6
In Australia 7
'Australian link' prior to 13 December 2022 8
Collects 8
Commonwealth record 9
Consent 10
Express or implied consent 10
Voluntary 11
Informed 11
Current and specific 12
Capacity 12
De-identification 13
Disclosure 14
Enforcement body 15
Enforcement related activities 16
Health information 17
Health Service 19
Holds 19
Immigration Department 20
Personal information 20
Meaning of 'reasonably identifiable' 21
Deceased persons 22
Purpose 22
Primary purpose and secondary purpose 22
Reasonable, Reasonably 23
Reasonable steps 24
Reasonably believes 24
Reasonably necessary and necessary 25
Recognised external dispute resolution scheme 25
Registered APP code 26
Related body corporate 26

Required or authorised by or under an Australian law or a court/tribunal order **27**
Meaning of 'required' 27
Meaning of 'authorised' 27
Meaning of 'Australian law' 27
Meaning of 'court/tribunal order' 28
Sensitive information **28**
Use **29**

B.1 This Chapter outlines some key words and phrases that are used in the Privacy Act and the Australian Privacy Principles (APPs).

APP entity

B.2 An 'APP entity' is defined to be an agency or organisation (s 6(1)).

B.3 An 'organisation' is defined to be:

- an individual (including a sole trader)
- a body corporate
- a partnership
- any other unincorporated association, or
- a trust

unless it is a small business operator, registered political party, State or Territory authority or a prescribed instrumentality of a State (s 6C).

B.4 The following terms are also defined in the Privacy Act: 'small business operator' (s 6D), 'registered political party' (s 6(1)) and 'State or Territory authority' (s 6C).

B.5 In general, a small business operator is an individual (including a sole trader), body corporate, partnership, unincorporated association or trust that has an annual turnover of $3,000,000 or less for a financial year, unless an exception applies (s 6D). If an exception applies this kind of business may be an organisation. The exceptions include businesses that:

- provide a health service and hold health information other than in an employee record
- disclose personal information about another individual for a benefit, service or advantage, or provide a benefit, service or advantage to collect personal information about another individual from anyone else, unless they do so with the consent of the individual or are required or authorised by or under legislation to do so
- are contracted service providers for a Commonwealth contract (s 6D(4))

B.6 Following are two examples of how the second exception may apply:

- An example of an entity that discloses personal information for a benefit, service or advantage is an entity that sells a list of personal information to another entity so that the other entity can use that information for the purpose of direct marketing.
- An example of an entity that provides a benefit, service or advantage to collect personal information is a lobby group that pays another entity to collect information about the political preferences of an individual.

B.7 A non-APP entity may be treated as an organisation (and therefore as an APP entity) in certain circumstances, for example, a small business operator that is related to an organisation covered by the Privacy Act (s 6D(9)), an entity that chooses to be treated as an organisation (s 6EA) or a small business operator that is accredited under the Consumer Data Right System under Part IVD of the *Competition and Consumer Act 2010* (s 6E(1D)). Also, some small business operators are treated as organisations (and therefore an APP entity) in relation to the following activities they carry out:

- activities of reporting entities or authorised agents relating to the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and its Regulations and Rules (s 6E(1A))
- certain acts and practices in connection with the operation of a residential tenancy database (s 6E(2)) and regulation 7 of Privacy Regulation 2013
- activities related to the conduct of a protection action ballot (s 6E(1)(B))[1]

B.8 'Agency' refers to Australian Government (and Norfolk Island Government) agencies,[2] but does not include State and Territory agencies. An 'agency' is defined to be:

- a Minister
- a Department
- a body (whether incorporated or not), or a tribunal, established or appointed for a public purpose by or under a Commonwealth enactment, not being:
  - an incorporated company, society or association; or
  - an organisation that is registered under the Fair Work (Registered Organisations) Act 2009 or a branch of such an organisation
- a body established or appointed by the Governor-General, or by a Minister, other than by or under a Commonwealth enactment
- a person holding or performing the duties of an office established by or under, or an appointment made under, a Commonwealth enactment, other than a person who, by virtue of holding that office, is the Secretary of a Department
- a person holding or performing the duties of an appointment, being an appointment made by the Governor-General, or by a Minister, other than under a Commonwealth enactment
- a federal court
- the Australian Federal Police
- a Norfolk Island agency
- the nominated AGHS company[3]
- an eligible hearing service provider, or
- the service operator under the Healthcare Identifiers Act 2010 (s 6(1))

B.9 Section 6(5) clarifies that a person shall not be taken to be an agency merely because the person is the holder of, or performs the duties of, certain offices, such as a judicial office or of an office of magistrate.

---

[1] See also, s 6F which describes when a state instrumentality will be treated as an organisation.

[2] The APPs do not apply to Australian Capital Territory Government agencies. The Information Privacy Act 2014 (ACT) regulates how personal information is handled by ACT public sector agencies. This Act includes a set of Territory Privacy Principles, which cover the collection, use, storage and disclosure of personal information, and an individual's access to and correction of that information. For more information about the TPPs, including how they differ from the APPs, see Privacy in the ACT, OAIC website https://www.oaic.gov.au.

[3] Nominated AGHS company means 'a company that (a) is the nominated company (within the meaning of Part 2 of the Hearing Services and AGHS Reform Act 1997); and (b) is either (i) Commonwealth owned (within the meaning of that Part); or (ii) a corporation' (s 6(1)).

Australian Link

B.10 The APPs extend to an act done, or practice engaged in, outside Australia and the external Territories by an organisation, or small business operator, that has an Australian link (s 5B(1A)).

B.11 An organisation or small business operator has an Australian link where it is:

- an Australian citizen or a person whose continued presence in Australia is not subject to a legal time limitation
- a partnership formed, or a trust created, in Australia or an external Territory
- a body corporate incorporated in Australia or an external Territory, or
- an unincorporated association that has its central management and control in Australia or an external Territory (s 5B(2))

B.12 An organisation that does not fall within one of those categories will also have an Australian link where it carries on business in Australia or an external Territory (s 5B(3)(b)).

Carries on business in Australia

B.13 The phrase 'carries on business in Australia' in s 5B(3)(b) is not defined in the Privacy Act. However, it arises in other areas of law, including corporations and consumer law. Guidance may be drawn from judicial consideration of the phrase in those contexts.

B.14 The two elements — 'carries on business' and 'in Australia' — are connected but can be considered separately. Australian courts have held that both are questions of fact.[4] An assessment should be made having regard to all relevant circumstances, particularly the nature of the enterprise conducted by an entity, and the particular Act being applied.[5] In this instance, it is the Privacy Act being applied.

Carry on business

B.15 The general law concept of 'carrying on business' has been said to 'generally involve conducting some form of commercial enterprise, systematically and regularly with a view to profit'[6]; or to embrace 'activities undertaken as a commercial enterprise in the nature of a going concern, that is, activities engaged in for the purpose of profit on a continuous and repetitive basis'.[7]

B.16 The focus of those definitions upon conducting or establishing a commercial enterprise for the purpose of profit is important. Nevertheless, a necessary modification of the concept in the context of the Privacy Act is that the Act can apply to a non-profit entity that is an 'organisation' as defined in s 6C(1). As to those entities, the more important element may be the repetition of commercial acts on a systematic or continuing basis as part of the activities of the entity.

---

[4] See Luckins v Highway Motel (Carnavon) Pty Ltd (1975) 133 CLR 164, per Stephen J, at [186]; Bray v F Hoffman-La Roche Ltd (2002) 118 FCR 1; ASIC v Active Super (No 1) [2012] FCA 1519 at [47]

[5] See ASIC v Edwards [2004] QSC 344 at [62]; Eltran Pty Ltd v Starport Futures Trading Corporation [2009] QSC 94 at [8]

[6] Gebo Investments (Labuan) Ltd v Signatory Investments Pty Ltd [2005] NSWSC 544, at [38]

[7] Hope v Council of the City of Bathurst (1980) 144 CLR 1 at [8]. For a discussion of the indicia of a 'business', see On Call Interpreters and Translators Agency Pty Ltd v Commissioner of Taxation (No 3) [2011] FCA 366 at [217] – [281]

In Australia

B.17 Whether a business is carried on 'in Australia' focusses upon whether activity is undertaken in Australia as part of the entity's business. There is 'a need for some physical activity in Australia through human instrumentalities, being activity that itself forms part of the course of conducting business'.[8] However, as noted in another decision, 'provided that there are acts within Australia which are part of the company's business, the company will be doing business in Australia although the bulk of its business is conducted elsewhere and it maintains no office in Australia'.[9]

B.18 An important consideration in applying this territorial requirement in the context of the Privacy Act is that the Act, though technologically-neutral, operates in an environment where personal information is regularly collected, held, used and disclosed online by organisations that may simultaneously carry on business through the web in many countries. In addition, an object of the Privacy Act is to 'promote the protection of the privacy of individuals' (s 2A(a)), which requires that regard be had to contemporary and practical circumstances.

B.19 In this context, factors that may be considered in assessing if an entity carries on business in Australia include whether:

- the entity has a place of business in Australia
- people who undertake business acts for the entity are located in Australia – for example, an entity may carry on business in Australia where an agent acting on its behalf carries on its business from some fixed place in Australia[10]
- the entity has a website that offers goods or services to countries including Australia
- Australia is one of the countries on the drop-down menu appearing on the entity's website
- web content that forms part of carrying on the business, was uploaded by or on behalf of the entity, in Australia
- business or purchase orders are assessed or acted upon in Australia
- the entity is the registered proprietor of trademarks in Australia[11]

B.20 The presence or absence of one of these factors may not be determinative in assessing whether an entity carries on business in Australia. For example, where an entity does not have a place of business in Australia, this does not necessarily mean that it does not carry on business in Australia.

B.21 An entity will not generally be regarded as carrying on business in Australia solely on the basis that a purchase order can be placed in Australia or that it has a website that can be accessed from Australia.[12]

[8] Gebo Investments (Labuan) Ltd v Signatory Investments Pty Ltd [2005] NSWSC 544 at [33]

[9] Australian Securities and Investments Commission v ActiveSuper Pty Ltd (No 1) [2012] FCA 1519 at [47]

[10] Bray v F Hoffman-La Roche Ltd (2002) 118 FCR 1 at [62]

[11] Australian Wool Innovation Ltd v Newkirk (no 3) [2005] FCA 1308 at [34]

[12] Gebo Investments (Labuan) Ltd v Signatory Investments Pty Ltd [2005] NSWSC 544

'Australian link' prior to 13 December 2022

B.22 The *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* came into force on 13 December 2022 and repealed s 5B(3)(c) of the Privacy Act. This means that the previous test under s 5B(3) will apply to acts and practices outside Australia and the external Territories that occurred before 13 December 2022.

B.23 Prior to 13 December 2022, s 5B(3) provided that an organisation will have an Australian link where:

- it carries on business in Australia or an external Territory (s 5B(3)(b)), and
- it collected or held personal information in Australia or an external Territory, either before or at the time of an act or practice (s 5B(3)(c)).

B.24 The phrase 'carries on business' is discussed above at B.13 – B.21.

B.25 Personal information is collected 'in Australia', if it is collected from an individual who is physically present in Australia or an external Territory, regardless of where the collecting entity is located or incorporated. An example is the collection of personal information from an individual who is physically located in Australia or an external Territory, via a website that is hosted outside Australia. This applies even if the website is owned by a company that is located outside of Australia or that is not incorporated in Australia.[13]

Collects

B.26 An APP entity collects personal information 'only if the entity collects the personal information for inclusion in a record or generally available publication' (s 6(1)).

B.27 The term 'record' is defined in s 6(1) and includes a document or an electronic or other device. Some items are excluded from the definition, such as anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition, and Commonwealth records in the open access period.

B.28 The term 'generally available publication' is defined in s 6(1) to mean a 'magazine, book, article, newspaper or other publication that is, or will be, generally available to members of the public', regardless of the form in which it is published and whether it is available on payment of a fee.

B.29 An APP entity does not collect personal information where that information is acquired but not included in a record or generally available publication. For example, a newspaper article containing personal information will not be 'collected' by the entity unless, for example, a clipping of the article is kept and stored with other documents held by the entity or the article is scanned and saved into the entity's electronic database.

B.30 The concept of 'collection' applies broadly, and includes gathering, acquiring or obtaining personal information from any source and by any means, including from:

- individuals
- other entities
- generally available publications

[13] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 218.

- surveillance cameras, where an individual is identifiable or reasonably identifiable
- information associated with web browsing, such as personal information collected by cookies[14]
- biometric technology, such as voice or facial recognition

B.31 Collection may also take place when an APP entity generates personal information from other data it holds, such as the generation of an audit log.

Commonwealth record

B.32 A 'Commonwealth record' has the same meaning as in the Archives Act 1983 (Archives Act) (s 6(1)).

B.33 The Archives Act states that a 'Commonwealth record' means:

- a record[15] that is the property of the Commonwealth or a Commonwealth institution, or
- a record that is deemed to be a Commonwealth record either by a regulation made under the Archives Act or under s 22 of the Archives Act (which applies to records kept by a Royal Commission or Commission of inquiry) (s 3(1))

B.34 Some categories of records are excluded from that definition:

- 'exempt material', which includes, for example, material included in the memorial collection of the Australian War Memorial, and material included in the collections maintained by the National Library of Australia, the National Gallery of Australia, the National Portrait Gallery of Australia, and the National Museum of Australia
- a register or guide maintained by the Archives, namely, the Australian National Register of Records, Australian National Guide to Archival Material or Australian National Register of Research Involving Archives (see Part VIII, Archives Act)

B.35 It is likely that all or most personal information collected or received by an agency will be included in a 'Commonwealth record'. Where an organisation is a contracted service provider under a Commonwealth contract, the records collected, received or held by that organisation under the contract may also be Commonwealth records.

B.36 APPs 4.3 and 11.2 require the destruction or de-identification of personal information in certain circumstances (see Chapters 4 and 11). These requirements do not apply to information contained in a Commonwealth record. Retention, destruction and alteration of Commonwealth records is governed by the Archives Act. A Commonwealth record can, as a general rule, only be destroyed or altered in accordance with s 24 of the Archives Act. The grounds on which this may be done include with the permission of the National Archives of Australia (as set out in a records disposal authority) or in accordance with 'normal

[14] Analytical information collected from cookies (e.g., the number of times a page was visited) will not be personal information under the Privacy Act unless an individual is reasonably identifiable (see paragraphs B.85–B.96 below).

[15] 'Record' is defined in s 3(1) of the Archives Act as 'a document, or an object, in any form (including any electronic form) that is, or has been, kept by reason of: (a) any information or matter that it contains or that can be obtained from it; or (b) its connection with any event, person, circumstance or thing'.

administrative practice'. Further information about Archives Act requirements is available from the National Archives of Australia at <www.naa.gov.au>.

Consent

B.37 Consent is relevant to the operation of a number of APPs. In some, consent is an exception to a general prohibition against personal information being handled in a particular way (for example, APPs 3.3(a) and 6.1(a)). In others, consent provides authority to handle personal information in a particular way (for example, APPs 7.3, 7.4 and 8.2(b)).

B.38 Consent means 'express consent or implied consent' (s 6(1)). The four key elements of consent are:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent

Express or implied consent

B.39 Express consent is given explicitly, either orally or in writing. This could include a handwritten signature, an oral statement, or use of an electronic medium or voice signature to signify agreement.

B.40 Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the APP entity.

B.41 An APP entity should not assume that an individual has consented to a collection, use or disclosure that appears to be advantageous to that person. Nor can an entity establish implied consent by asserting that if the individual knew about the benefits of the collection, use or disclosure, they would probably consent to it.

B.42 Generally, it should not be assumed that an individual has given consent on the basis alone that they did not object to a proposal to handle personal information in a particular way. An APP entity cannot infer consent simply because it provided an individual with notice of a proposed collection, use or disclosure of personal information. It will be difficult for an entity to establish that an individual's silence can be taken as consent. Consent may not be implied if an individual's intent is ambiguous or there is reasonable doubt about the individual's intention.

B.43 Use of an opt-out mechanism to infer an individual's consent will only be appropriate in limited circumstances, as the individual's intention in failing to opt-out may be ambiguous. An APP entity will be in a better position to establish the individual's implied consent the more that the following factors, where relevant, are met:

- the opt out option was clearly and prominently presented
- it is likely that the individual received and read the information about the proposed collection, use or disclosure, and the option to opt out
- the individual was given information on the implications of not opting out
- the opt out option was freely available and not bundled with other purposes

- it was easy for the individual to exercise the option to opt out, for example, there was little or no financial cost or effort required by the individual
- the consequences of failing to opt out are not serious
- an individual who opts out at a later time will, as far as practicable, be placed in the position as if they had opted out earlier

B.44 An APP entity should generally seek express consent from an individual before handling the individual's sensitive information, given the greater privacy impact this could have.

B.45 An APP entity should as far as practicable implement procedures and systems to obtain and record consent. This may resolve any doubt about whether consent was given (either on the basis of express or implied consent).

Voluntary

B.46 Consent is voluntary if an individual has a genuine opportunity to provide or withhold consent. Consent is not voluntary where there is duress, coercion or pressure that could overpower the person's will.

B.47 Factors relevant to deciding whether consent is voluntary include:

- the alternatives open to the individual, if they choose not to consent
- the seriousness of any consequences if an individual refuses to consent
- any adverse consequences for family members or associates of the individual if the individual refuses to consent

Bundled consent

B.48 Bundled consent refers to the practice of an APP entity 'bundling' together multiple requests for an individual's consent to a wide range of collections, uses and disclosures of personal information, without giving the individual the opportunity to choose which collections, uses and disclosures they agree to and which they do not.

B.49 This practice has the potential to undermine the voluntary nature of the consent. If a bundled consent is contemplated, an APP entity could consider whether:

- it is practicable and reasonable to give the individual the opportunity to refuse consent to one or more proposed collections, uses and/or disclosures
- the individual will be sufficiently informed about each of the proposed collections, uses and/or disclosures
- the individual will be advised of the consequences (if any) of failing to consent to one or more of the proposed collections, uses and/or disclosures (see also, discussion of 'informed' below)

Informed

B.50 An individual must be aware of the implications of providing or withholding consent, for example, whether access to a service will be denied if consent is not given to collection of a specific item of personal information. An APP entity should ensure that an individual is properly and clearly informed about how their personal information will be handled, so they

can decide whether to give consent (see also, discussion of 'capacity' below). The information should be written in plain English, without legal or industry jargon.

Current and specific

B.51 An APP entity should generally seek consent from an individual for collection and proposed uses and disclosures of personal information at the time the information is collected. Alternatively, if consent was not sought at the time of collection, or that consent did not cover a proposed use or disclosure, an entity should seek the individual's consent at the time of the use or disclosure.

B.52 Consent given at a particular time in particular circumstances cannot be assumed to endure indefinitely. It is good practice to inform the individual of the period for which the consent will be relied on in the absence of a material change of circumstances.

B.53 An APP 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' (see also, discussion of 'bundled consent' above). When seeking consent, an entity should describe the purpose to which it relates. The level of specificity required will depend on the circumstances, including the sensitivity of the personal information.

B.54 An individual may withdraw their consent at any time, and this should be an easy and accessible process. Once an individual has withdrawn consent, an APP entity can no longer rely on that past consent for any future use or disclosure of the individual's personal information. Individuals should be made aware of the potential implications of withdrawing consent, such as no longer being able to access a service.

Capacity

B.55 An individual must have the capacity to consent. This means that the individual is capable of understanding the nature of a consent decision, including the effect of giving or withholding consent, forming a view based on reasoned judgement and how to communicate a consent decision. An APP entity can ordinarily presume that an individual has the capacity to consent, unless there is something to alert it otherwise, for example, the individual is a child or young person (see below). If an entity is uncertain as to whether an individual has capacity to consent at a particular time, it should not rely on any statement of consent given by the individual at that time.

B.56 Issues that could affect an individual's capacity to consent include:

- age
- physical or mental disability
- temporary incapacity, for example during a psychotic episode, a temporary psychiatric illness, or because the individual is unconscious, in severe distress or suffering dementia
- limited understanding of English

B.57 An APP entity should consider whether any such issue could be addressed by providing the individual with appropriate support to enable them to have capacity to consent. If an individual does not have capacity to consent, even with support or the provision of additional resources such as an interpreter or alternative communication methods, and consent is required, an entity should consider who can act on the individual's behalf. Options include:

- a guardian
- someone with an enduring power of attorney
- a person recognised by other relevant laws, for example in NSW, a 'person responsible' under the Guardianship Act 1987 (NSW) (this may be an individual's spouse, partner, carer, family member or close friend), or
- a person who has been nominated in writing by the individual while they were capable of giving consent

B.58 An individual who lacks the capacity to consent should nevertheless be involved, as far as practicable, in any decision-making process. To the extent practicable in the circumstances, an APP entity should ensure that privacy issues are discussed with individuals who have impaired decision-making capacity in a way that is understandable and comprehensible.

Children and young people

B.59 The Privacy Act does not specify an age after which individuals can make their own privacy decisions. An APP entity will need to determine on a case-by-case basis whether an individual under the age of 18 has the capacity to consent.

B.60 As a general principle, an individual under the age of 18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person, for example, if the child is young or lacks the maturity or understanding to do so themselves.

B.61 If it is not practicable or reasonable for an APP entity to assess the capacity of individuals under the age of 18 on a case-by-case basis, the entity may presume that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise. An individual aged under 15 is presumed not to have capacity to consent.

De-identification

B.62 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-identified information is not 'personal information' (see paragraphs B.85–B.96).

B.63 De-identification involves removing or altering information that identifies an individual or is reasonably likely to do so. Generally, de-identification includes two steps:

- removing personal identifiers, such as an individual's name, address, date of birth or other identifying information, and
- removing or altering other information that may allow an individual to be identified, for example, because of a rare characteristic of the individual, or a combination of unique or remarkable characteristics that enable identification

B.64 De-identification may not altogether remove the risk that an individual can be re-identified. There may, for example, be a possibility that another dataset or other information could be matched with the de-identified information. The risk of re-identification must be actively assessed and managed to mitigate this risk. Relevant factors to consider when determining

whether information has been effectively de-identified could include the cost, difficulty, practicality and likelihood of re-identification.[16]

B.65 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.[17]

Disclosure

B.66 Disclosure is not defined in the Privacy Act.

B.67 An APP entity discloses personal information when it makes it accessible or visible to others outside the entity and releases the subsequent handling of the personal information from its effective control. This focuses on the act done by the disclosing party, and not on the actions or knowledge of the recipient. Disclosure, in the context of the Privacy Act, can occur even where the personal information is already known to the recipient.[18]

B.68 The release may be a proactive release, a release in response to a specific request, an accidental release or an unauthorised release by an employee.

B.69 Examples include where an APP entity:

- shares a copy of personal information with another entity or individual
- discloses personal information to themselves, but in their capacity as a different entity
- publishes personal information whether intentionally or not[19] and it is accessible to another entity or individual
- accidentally provides personal information to an unintended recipient[20]
- displays a computer screen so that the personal information can be read by another entity or individual, for example at a reception counter or in an office

B.70 Where an APP entity engages a contractor to perform services on its behalf, the provision of personal information to that contractor will in most circumstances be a disclosure (see paragraph B.144 for the limited circumstances where it will be a 'use').

B.71 '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.[21] Examples include unauthorised access following a cyber-attack[22] or a theft, including where the third party

[16] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 60.

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

[18] For a similar approach to interpreting 'disclosure', see Pratt Consolidated Holdings Pty Ltd v Commissioner of Taxation [2011] AATA 907 at [112] – 119]

[19] See OAIC, Medvet Science Pty Ltd: Own motion investigation report, July 2012, OAIC website <https://www.oaic.gov.au>; Telstra Corporation Limited: Own motion investigation report, June 2012, OAIC website <https://www.oaic.gov.au>.

[20] The APP entity may also breach APP 11 if it did not take reasonable steps to protect the information from this unauthorised disclosure (see APP 11, Chapter 11).

[21] The actions of an employee will be attributed to the APP entity where it was carried out 'in the performance of the duties of the person's employment' (s 8(1)).

[22] See OAIC, Sony PlayStation Network / Qriocity: Own motion investigation report, September 2011, OAIC website <https://www.oaic.gov.au>.

then makes that personal information available to others outside the entity. However, where a third party gains unauthorised access, the entity may breach APP 11 if it did not take reasonable steps to protect the personal information from unauthorised access (see Chapter 11 (APP 11)).

- 'use', which is discussed in paragraphs B.142–B.144 below. The concept of 'use' encompasses information handling and management activities occurring within an entity's effective control, for example, when staff of an entity access, read, exchange or make decisions based on personal information the entity holds.

B.72 In a number of APPs the same requirements apply to the 'use' or 'disclosure' of personal information (for example, APP 6.1 (see Chapter 6), APP 7 (see Chapter 7), APP 9.2 (see Chapter 9) and APP 10.2 (see Chapter 10)). For these, it is not necessary to distinguish between a 'use' and a 'disclosure'. However, the distinction is relevant to the following principles and exceptions that only apply to the 'disclosure' of personal information, and not to its 'use':

- section 16B(5) (see Chapter D)
- APP 1.4(f) and (g) (see Chapter 1)
- APP 5.2(f), (i) and (j) (see Chapter 5)
- APP 6.3 (see Chapter 6)
- APP 8 (see Chapter 8)
- APP 11.1(b) (Chapter 11)

Enforcement body

B.73 'Enforcement body' is defined to mean:

- the Australian Federal Police
- the Integrity Commissioner
- the Australian Crime Commission
- Sport Integrity Australia
- the Immigration Department
- the Australian Prudential Regulation Authority
- the Australian Securities and Investments Commission
- the Office of the Director of Public Prosecutions, or a similar body established under a law of a State or Territory
- another Commonwealth agency, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law
- another Commonwealth agency, to the extent that it is responsible for administering a law relating to the protection of the public revenue
- a police force or service of a State or a Territory
- the New South Wales Crime Commission

- the Independent Commission Against Corruption of New South Wales
- the Law Enforcement Conduct Commission of New South Wales
- the Independent Broad-based Anti-corruption Commission of Victoria
- the Crime and Corruption Commission of Queensland
- the Corruption and Crime Commission of Western Australia
- the Independent Commissioner Against Corruption of South Australia
- another prescribed authority or body that is established under a law of a State or Territory to conduct criminal investigations or inquiries
- a State or Territory authority, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law, or
- a State or Territory authority, to the extent that it is responsible for administering a law relating to the protection of the public revenue (s 6(1))

Enforcement related activities

B.74 'Enforcement related activity' is defined to mean:

- the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction
- the conduct of surveillance activities, intelligence gathering activities or monitoring activities
- the conduct of protective or custodial activities
- the enforcement of laws relating to the confiscation of the proceeds of crime
- the protection of the public revenue
- the prevention, detection, investigation or remedying of misconduct of a serious nature, or other conduct prescribed by the regulations
- the preparation for, or conduct of, proceedings before any court or tribunal, or the implementation of court/tribunal orders (s 6(1))

B.75 This definition recognises that 'enforcement related activities' can include lawful surveillance, intelligence gathering or monitoring activities where there may not be an existing investigation.[23] Those activities are distinct but may also overlap.

B.76 Examples of surveillance activities include optical surveillance of an individual or property where information obtained from that surveillance may lead to an investigation of a criminal offence. Examples of intelligence gathering include the collection of personal information about an individual to detect whether an offence has occurred, or to determine whether to initiate an investigation into that offence; the collection of information about whether an individual is planning to commit an offence and whether there are fellow criminal associates. Examples of monitoring activities include the monitoring by an enforcement

[23] Addendum to the Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 3.

body of a person who has presented themself to that body in compliance with a court order.[24]

Health information

B.77 'Health information' is defined to mean:

- information or an opinion, that is also personal information, about:
  - the health or a disability (at any time) of an individual, or
  - an individual's expressed wishes about the future provision of health services to him or her, or
  - a health service provided, or to be provided, to an individual, or
- other personal information collected to provide, or in providing, a health service, or
- other personal information about an individual collected in connection with the donation, or intended donation, by the individual of their body parts, organs or body substances, or
- genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual (s 6(1)). (Other types of genetic information that are not health information fall within the definition of 'sensitive information', discussed at paragraphs B.138–B.141.)

B.78 Examples of health information include:

- information about an individual's physical or mental health
- notes of an individual's symptoms or diagnosis and the treatment given
- specialist reports and test results
- appointment and billing details
- prescriptions and other pharmaceutical purchases
- dental records
- records held by a fitness club about an individual
- information about an individual's suitability for a job, if it reveals information about the individual's health
- an individual's healthcare identifier when it is collected to provide a health service
- any other personal information (such as information about an individual's date of birth, gender, race, sexuality, religion), collected for the purpose of providing a health service

B.79 The definition of 'sensitive information' in s 6(1) includes health information. Sensitive information, including health information, attracts additional privacy protections compared to other types of personal information (see for example, APP 3 in Chapter 3). There are also a number of provisions and APPs that deal specifically with health information, including the 'permitted health situation' exceptions set out in s 16B (see Chapter D (Permitted health situations)).

[24] Addendum to the Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 3.

Health Service

B.80 'Health service' is defined to mean:

- an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the person performing it:
  - to assess, record, maintain or improve the individual's health, or
  - to diagnose the individual's illness or disability, or
  - to treat the individual's illness or disability or suspected illness or disability, or
- the dispensing or prescription of a drug or medicinal preparation by a pharmacist (s 6(1))

B.81 The Privacy Act generally applies to all organisations that provide a health service, including an organisation that is a small business.[25] Examples of organisations that provide a health service include:

- traditional health service providers, such as private hospitals, day surgeries, medical practitioners, pharmacists and allied health professionals
- complementary therapists, such as naturopaths and chiropractors
- gyms and weight loss clinics
- child care centres, private schools and private tertiary educational institutions

Holds

B.82 An APP entity 'holds' personal information if 'the entity has possession or control of a record that contains the personal information' (s 6(1)).

B.83 The term 'record' is defined in s 6(1) and includes a document or an electronic or other device. Some items are excluded from the definition, such as anything kept in a library, art gallery or museum for the purposes of reference study or exhibition and Commonwealth records in the open access period.

B.84 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. Whether an APP entity 'holds' a particular item of personal information may therefore depend on the particular information collection, management and storage arrangements it has adopted. For example, an APP entity 'holds' personal information where:

- it physically possesses a record containing the personal information and can access that information physically or by use of an electronic device (such as decryption software)
- it has the right or power to deal with the personal information, even if it does not physically possess or own the medium on which the personal information is stored. For

[25] Small businesses – namely, those with an annual turnover of $3 million or less – are generally exempt from the operation of the Privacy Act (s 6D). However, this exemption does not apply to an individual, body corporate, partnership, unincorporated association or trust that provides a health service to another individual and holds any health information except in an employee record (s 6D(4)(b)).

example, the entity has outsourced the storage of personal information to a third party but it retains the right to deal with it, including to access and amend that information

B.85 An agency that has placed a record of personal information in the care of the National Archives of Australia, or in the custody of the Australian War Memorial, is considered to be the agency that holds the record for the purposes of the Privacy Act (s 10(4)).

Immigration Department

B.86 'Immigration Department' means 'the Department administered by the Minister administering the Migration Act 1958' (s 6(1)). Information about the particular Minister and Department that administer the Migration Act 1958 can be found on the Federal Register of Legislation.[26]

B.87 The definition of 'enforcement body' includes the 'Immigration Department' (see paragraph B.70). This means that the exception in APP 3.4(d)(i) that permits the collection of sensitive information, and the exceptions in APPS 6.2(e) and 8.2(f) that permit the use and disclosure of personal information, extend to the 'enforcement related activities' of the Immigration Department (see Chapters 3, 6 and 8).[27]

Personal information

B.88 'Personal information' is defined as any 'information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not' (s 6(1))

B.89 Common examples are an individual's name, signature, address, telephone number, date of birth, medical records, bank account details, employment details and commentary or opinion about a person.

B.90 Personal information of one individual may also be personal information of another individual. Examples include a marriage certificate that contains personal information of both parties to a marriage, and a vocational reference that includes personal information about both the author and the subject of the reference.

B.91 The personal information 'about' an individual may be broader than the item of information that identifies them. For example, a vocational reference or assessment may comment on a person's career, performance, attitudes and aptitude. Similarly, the views expressed by the author of the reference may also be personal information about the author.

B.92 Personal information that has been de-identified will no longer be personal information. Personal information is de-identified if the information is no longer about an identifiable individual or an individual who is reasonably identifiable (see paragraph B.59).

---

[26] See Federal Register of Legislation website <https://www.legislation.gov.au/Series/C1958A00062>.

[27] For examples of the functions and activities of the Immigration Department that will be covered by the 'enforcement related activity' exceptions in APPs 3.4, 6.2 and 8.2, see Addendum to the Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 2.

B.93 What constitutes personal information will vary, depending on whether an individual can be identified or is reasonably identifiable in the particular circumstances.

Meaning of 'reasonably identifiable'

B.94 Whether an individual is 'reasonably identifiable' from particular information will depend on considerations that include:[28]

- the nature and amount of information
- the circumstances of its receipt
- who will have access to the information
- other information either held by or available to the APP entity that holds the information
- whether it is possible for the individual or entity that holds the information to identify the individual, using available resources (including other information available to that individual or entity). Where it may be possible to identify an individual using available resources, the practicability, including the time and cost involved, will be relevant to deciding whether an individual is 'reasonably identifiable'[29]
- if the information is publicly released, whether a reasonable member of the public who accesses that information would be able to identify the individual

B.95 The following are given as examples of how those considerations may apply to particular items of information:

- Most entities and individuals would encounter difficulty in using a licence plate number to identify the registrant of a car, as they would not have access to the car registration database. By contrast, an agency or individual with access to that database may be able to identify the registrant. Accordingly, the licence plate number may be 'personal information' held by that agency or individual, but may not be personal information if held by another entity.
- Information that an unnamed person with a certain medical condition lives in a specific postcode area may not enable the individual to be identified, and would not therefore be personal information. By contrast, it may be personal information if held by an entity or individual with specific knowledge that could link an individual to the medical condition and the postcode.[30]
- A common surname that is shared by many people may not be personal information that would reasonably identify a particular individual. However, combined with other information, such as address or other contact information, it may be personal information

B.96 Whether a person is 'reasonably identifiable' is an objective test that has practical regard to the context in which the issue arises. Even though it may be technically possible to identify an individual from information, if doing so is so impractical that there is almost no likelihood

[28] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 61.

[29] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 61.

[30] Autism Aspergers Advocacy Australia and Department of Families, Housing, Community Services and Indigenous Affairs [2012] AICmr 28 (12 November 2012), see Information Commissioner review decisions, OAIC website <https://www.oaic.gov.au>

of it occurring, the information would not generally be regarded as 'personal information'.[31] An individual may not be reasonably identifiable if the steps required to do so are excessively time-consuming or costly in all the circumstances.

B.97 Where it is unclear whether an individual is 'reasonably identifiable', an APP entity should err on the side of caution and treat the information as personal information.

Deceased persons

B.98 The definition of 'personal information' in s 6(1) refers to information or an opinion about an 'individual.' An 'individual' means 'a natural person' (s 6(1)). The ordinary meaning of 'natural person' does not include deceased persons.[32]

B.99 Information about a deceased person may include information about a living individual and be 'personal information' for the purposes of the Privacy Act. For example, information that a deceased person had an inheritable medical condition may indicate that the deceased person's descendants have an increased risk of that condition. If the descendants are identifiable, that information would be personal information about the descendants. The privacy interests of family members could therefore be considered when handling information about deceased persons.

Purpose

B.100 The purpose of an action is the reason why it is done. The purpose for which an APP entity collects, holds, uses and discloses personal information can be relevant to:

- whether the entity is permitted to collect, use, disclose and retain personal information (APPs 3, 4, 6, 7, and 11)
- the matters that must be included in the entity's APP Privacy Policy (APP 1) and in any collection notice to the individual (APP 5)
- the steps that must be taken to ensure the quality of personal information (APP 10) and to correct incorrect information (APP 13)

Primary purpose and secondary purpose

B.101 The purpose for which an APP entity collects personal information is known as the 'primary purpose' of collection. This is the specific function or activity for which the entity collects the personal information. If an APP entity uses or discloses the personal information for another purpose this is known as a 'secondary purpose'. APP 6 sets out when an APP entity may use or disclose personal information for a secondary purpose (see Chapter 6 (APP 6)).

B.102 Where an APP entity collects personal information directly from an individual, the context will help in identifying the primary purpose of collection. For example, the individual may provide the personal information for a particular purpose, such as buying a particular

[31] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 61.

[32] However, for the purposes of Part VIA, which deals with personal information in emergencies and disasters, the definition of 'individual' in s 6(1)) is taken to include an individual who is not living (s 80G(2)).

product or receiving a particular service. This is the primary purpose of collection, even if the entity has additional secondary purposes in mind.

B.103 Where an APP entity receives unsolicited personal information or collects personal information about an individual from a third party, the context will again be relevant in identifying the primary purpose of collection. It will also be relevant to consider the function or activity which the personal information is reasonably necessary for, or to which it directly relates. In some instances, an APP entity that receives unsolicited personal information and retains it will have no primary purpose of collection. For example, where the entity could not have collected personal information under APP 3.1 but nevertheless retains it under APP 4, because the information is contained in a Commonwealth record, or because it is not lawful or reasonable for the entity to destroy it (see APP 4, Chapter 4).

Describing the primary purpose

B.104 How broadly a purpose can be described will depend on the circumstances and should be determined on a case-by-case basis. In cases of ambiguity, and with a view to protecting individual privacy, the primary purpose for collection, use or disclosure should be construed narrowly rather than expansively.

B.105 The primary purpose may nevertheless be described in general terms, as long as the description is adequate to inform an individual of how the APP entity may use or disclose their personal information. A description – the information will be used 'for the functions of the entity' – would generally be considered too broad. Instead, the primary purpose of collection could be described as to:

- provide a particular banking service
- market particular goods or services , or types of goods or services, to the individual
- assess an applicant's suitability for a job
- assess an applicant's eligibility for a loan
- resolve a complaint
- provide further information about a particular service
- enable an agency to give someone a particular benefit or service

B.106 An APP entity does not need to include in its description internal purposes that form part of normal business practices, such as auditing, business planning, billing or de-identifying personal information.

Reasonable, Reasonably

B.107 The terms 'reasonable' and 'reasonably' are used in the Privacy Act and APPs to qualify a test or obligation. Examples include that 'personal information' is information about an individual who is 'reasonably' identifiable (s 6(1)) and an APP entity must not collect personal information unless it is 'reasonably necessary' for one or more of the entity's functions or activities (APP 3).

B.108 'Reasonable' and 'reasonably' are not defined in the Privacy Act. The terms bear their ordinary meaning, as being based upon or according to reason and capable of sound explanation. What is reasonable is a question of fact in each individual case. It is an objective test that has regard to how a reasonable person, who is properly informed, would be

expected to act in the circumstances. What is reasonable can be influenced by current standards and practices.[33] It is the responsibility of an APP entity to be able to justify that its conduct was reasonable. In a related context, the High Court has observed that whether there are 'reasonable grounds' to support a course of action 'requires the existence of facts which are sufficient to [persuade] a reasonable person';[34] it 'involves an evaluation of the known facts, circumstances and considerations which may bear rationally upon the issue in question'.[35] As that indicates, there may be a conflicting range of objective circumstances to be considered, and the factors in support of a conclusion should outweigh those against.

B.109 The terms 'reasonable' and 'reasonably' are discussed further in the APP guidelines, as they arise in the context of each of the relevant APPs.

Reasonable steps

B.110 A number of the APPs require an APP entity to 'take such steps as are reasonable in the circumstances' (for example, APP 1.2 (see Chapter 1), APP 8.1 (see Chapter 8) and APP 11(see Chapter 11). The shorthand expression used in the APP guidelines is 'reasonable steps'.[36]

B.111 The 'reasonable steps' test is an objective test, and is to be applied in the same manner as 'reasonable' and 'reasonably'. It is the responsibility of an APP entity to be able to justify that reasonable steps were taken.

B.112 Some APPs require an APP entity to take 'such steps (if any) as are reasonable in the circumstances' (for example, APP 5.1 (see Chapter 5), APP 10 (see Chapter 10), APP 12.5 (see Chapter 12), APPs 13.1 and 13.2 (see Chapter 13). The inclusion of '(if any)' acknowledges that it in some circumstances an entity will satisfy the requirement to take reasonable steps by taking no steps.

Reasonably believes

B.113 A number of the exceptions to the APPs require an APP entity to have a 'reasonable belief' about a particular matter (see for example, APP 3.4 (Chapter 3), APP 6.2(e) (Chapter 6), APP 8.2 (Chapter 8), Permitted general situations, (Chapter C)).

B.114 The phrase 'reasonable belief' is to be applied in the same manner as 'reasonable' and 'reasonably'. That is, the APP entity must have a reasonable basis for the belief, and not merely a genuine or subjective belief. The requirement for a reasonable belief precludes arbitrary action, but may still leave something to surmise or conjecture.[37] It is the responsibility of an entity to be able to justify its reasonable belief.

[33] For example, Jones v Bartlett [2000] HCA 56 [57] – [58] (Gleeson CJ); Bankstown Foundry Pty Ltd v Braistina [1986] HCA 20 [12] (Mason, Wilson and Dawson JJ).

[34] George v Rockett (1990) 170 CLR 104 at 112 (Mason CJ, Brennan, Deane, Dawson, Toohey, Gaudron & McHugh JJ).

[35] McKinnon v Secretary, Department of Treasury (2006) 228 CLR 423 at 430 (Gleeson CJ & Kirby J).

[36] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 54.

[37] George v Rockett (1990) 170 CLR 104 at 112, 116.

Reasonably necessary and necessary

B.115 A number of APPs require a collection, use or disclosure to be 'reasonably necessary' for a particular purpose – see APPs 3, 6, 8 and 9. Certain permitted general situations and permitted health situations refer to a collection, use or disclosure being 'necessary' for a particular purpose (see Chapters C and D), and APP 7 refers to a use or disclosure being 'necessary' to meet a contractual obligation (see Chapter 7).

B.116 The term 'reasonable' is discussed at paragraphs B.104–B.106. 'Necessary' is not defined in the Privacy Act. The High Court of Australia has noted that 'there is, in Australia, a long history of judicial and legislative use of the term 'necessary', not as meaning essential or indispensable, but as meaning reasonably appropriate and adapted'.[38] However, in the context of the Privacy Act, it would not be sufficient if the collection, use or disclosure is merely helpful, desirable or convenient.

B.117 The 'reasonably necessary' test is an objective test: whether a reasonable person who is properly informed would agree that the collection, use or disclosure is necessary. It is the responsibility of an APP entity to be able to justify that the particular collection, use or disclosure is reasonably necessary.

B.118 The test must be applied in a practical sense. For example, under APP 3 if an entity cannot in practice effectively pursue a function or activity without collecting personal information, the collection would usually be considered reasonably necessary for that function or activity. However, a collection, use or disclosure of personal information will not usually be considered reasonably necessary if there are reasonable alternatives available, for example, if de-identified information would be sufficient for the function or activity.

B.119 An APP entity cannot rely solely on normal business practice in assessing whether a collection, use or disclosure is reasonably necessary. The primary issue is whether, in the circumstances of a particular entity, a collection, use or disclosure is reasonably necessary for a particular function or activity.

B.120 The term 'necessary' rather than 'reasonably necessary' is used in certain permitted general situations and permitted health situations, and in APP 7. The context explains this different usage. For example, a permitted health situation may exist if the collection of personal information is 'necessary' for public health research that is conducted in accordance with relevant guidelines. Similarly, APP 7.5 refers to the use or disclosure of personal information for the purpose of direct marketing where that is 'necessary' to meet a contractual obligation. In some of the permitted general situations and permitted health situations the test is whether an APP entity 'reasonably believes' that the collection, use or disclosure of personal information is 'necessary' for a particular purpose, such as lessening or preventing a serious threat to a person's health or safety.

Recognised external dispute resolution scheme

B.121 'Recognised external dispute resolution scheme' is defined as 'an external dispute resolution scheme recognised under section 35A' (s 6(1)).

B.122 Section 35A(1) gives the Information Commissioner power to recognise an external dispute resolution scheme for an entity or a class of entities, or for a specified purpose. A register of

[38] Mulholland v Australian Electoral Commissioner [2004] HCA 41 [39] (Gleeson CJ).

recognised external dispute resolution schemes is maintained on the Office of the Australian Information Commissioner website.[39]

B.123 An individual who considers that an APP entity has interfered with their privacy may complain to a recognised EDR scheme of which the entity is a member, if the complaint falls within the scope of the EDR scheme's recognition. For further discussion of recognised EDR schemes, and their role in handling privacy-related complaints, see Guidelines for Recognising External Dispute Resolution Schemes under s 35A of the Privacy Act.[40]

Registered APP code

B.124 A 'registered APP code' is defined as an APP code that is included on the Codes Register and that is in force (s 26B(1)). A registered APP code is a legislative instrument (s 26B(2)). The requirements in relation to registered APP codes are set out in Division 2 of Part IIIB.

B.125 An 'APP code' is defined as a written code of practice about information privacy (s 26C). It can be developed by an APP entity, either on its own initiative or on request from the Information Commissioner, or by the Information Commissioner directly (ss 26E and 26G). A code may be expressed to apply to all or a specified type of personal information, a specified activity or class of activities of an APP entity, a specified industry sector or professions or specified class of industry sectors or professions, or APP entities that use technology of a specified kind (s 26C(4)).

B.126 The Information Commissioner has power to approve and register an APP code (provided certain conditions are met) by including it on the Codes Register (s 26H).

B.127 Once an APP code is registered, an APP entity bound by the code must not do an act, or engage in a practice, that breaches that code. A breach of a registered APP code will be 'an interference with the privacy of an individual' by the entity under s 13(1)(b).

B.128 A registered APP code does not replace the APPs for the entities which it binds, but operates in addition to the requirements of the APPs.[41] For further discussion about the development of APP codes, and the requirements and process for recognition, see the Guidelines for Developing Codes.[42]

Related body corporate

B.129 Section 6(8) provides that 'the question whether bodies corporate are related to each other is determined in the manner in which that question is determined under the Corporations Act 2001'.

B.130 Section 13B(1) permits related bodies corporate to share personal information (other than sensitive information) in certain circumstances. The effect of s 13B(1) is discussed further in Chapter 3 (APP 3) and Chapter 6 (APP 6).

---

[39] See OAIC website <https://www.oaic.gov.au>.

[40] OAIC, Guidelines for Recognising External Dispute Resolution Schemes, OAIC website <https://www.oaic.gov.au>.

[41] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 199.

[42] OAIC, Guidelines for Developing Codes, OAIC website <https://www.oaic.gov.au>.

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

B.131 A number of the APPs provide an exception if an APP entity is 'required or authorised by or under an Australian law or a court/tribunal order' to act differently (for example, APP 3.4(a) (Chapter 3), APP 6.2(b) (Chapter 6) and APP 12.3(g) (Chapter 12)). Some other provisions refer more narrowly to an act that is 'required by or under an Australian law (other than this Act)' (s 16B(2) (Chapter D)) or 'required by or under an Australian law, or a court order' (APP 11.2(d) (Chapter 11)), and do not include an act that is 'authorised'.

Meaning of 'required'

B.132 An APP entity that is 'required' by an Australian law or a court/tribunal order to handle information in a particular way has a legal obligation to do so, and cannot choose to act differently. The obligation will usually be indicated by words such as 'must' or 'shall', and may be accompanied by a sanction for non-compliance.

Meaning of 'authorised'

B.133 An APP entity that is 'authorised' under an Australian law or a court/tribunal order has discretion as to whether it will handle information in a particular way. The entity is permitted to take the action but is not required to do so. The authorisation may be indicated by a word such as 'may', but may also be implied rather than expressed in the law or order.

B.134 An APP entity may be impliedly authorised by law to handle personal information in a particular way, where a law requires or authorises a function or activity, and this directly entails the information handling practice. For example, a statute that authorises an APP entity to collect personal information about an individual from a third party implicitly authorises the entity to disclose the individual's identity to the third party.

B.135 An act or practice is not 'authorised' solely because there is no law or court/tribunal order prohibiting it. Nor can an act or practice rely solely on a general or incidental authority conferred by statute upon an agency to do anything necessary or convenient for, or incidental to or consequential upon, the specific functions and powers of the agency. The reason is that the purpose of the APPs is to protect the privacy of individuals by imposing obligations on APP entities in handling personal information. A law will not authorise an exception to those requirements unless it does so by clear and direct language.[43]

Meaning of 'Australian law'

B.136 'Australian law' is defined as:

- an Act of the Commonwealth, or of a State or Territory
- regulations or any other instrument made under such an Act
- a Norfolk Island enactment, or
- a rule of common law or equity (s 6(1))

[43] See Coco v The Queen (1994) 179 CLR 427.

B.137 The definition of Australian law does not include a contract.[44] Consequently, an obligation imposed by contract upon a party to handle information in a particular way will not provide authority for the purposes of the 'required or authorised by or under an Australian law or court/tribunal order' exception.

Meaning of 'court/tribunal order'

B.138 'Court/tribunal order' is defined as an order, direction or other instrument made by a court, a tribunal, a judge, a magistrate, a person acting as a judge or magistrate, a judge or magistrate acting in a personal capacity, and a member or an officer of a tribunal (s 6(1)).

B.139 The definition applies to orders and the like issued by Commonwealth, State and Territory courts, tribunals and members and officers. The definition includes an order, direction or other instrument that is of an interim or interlocutory nature.

B.140 The reference to a judge or a magistrate acting in a personal capacity means that the definition applies to an order or direction issued by a judge or magistrate who has been appointed by government to an office or inquiry that involves the exercise of administrative or executive functions, including functions that are quasi-judicial in nature.[45] An example is a judge who is appointed by government to conduct a royal commission.

Sensitive information

B.141 'Sensitive information' is a subset of personal information and is defined as:

- information or an opinion (that is also personal information) about an individual's:
  - racial or ethnic origin
  - political opinions
  - membership of a political association
  - religious beliefs or affiliations
  - philosophical beliefs
  - membership of a professional or trade association
  - membership of a trade union
  - sexual orientation or practices, or
  - criminal record
- health information about an individual (see paragraphs B.74–B.78)
- genetic information (that is not otherwise health information)
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or
- biometric templates (s 6(1))

B.142 Information may be sensitive information where it clearly implies one of these matters. For example, many surnames have a particular racial or ethnic origin, but that alone will not

[44] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 55.

[45] Drake v Minister for Immigration & Ethnic Affairs (1979) 2 ALD 60; 46 FLR 409; Grollo v Palmer (1995) 184 CLR 348.

constitute sensitive information that clearly indicates the racial or ethnic origin of an individual with that surname.

B.143 Terms such as 'political opinions' and 'philosophical beliefs' are not defined in the Privacy Act. They take their ordinary meaning and should be interpreted broadly. However, not every value, belief or opinion of an individual will be considered to be a political opinion or philosophical belief.

B.144 Sensitive information is generally afforded a higher level of privacy protection under the APPs than other personal information (for example, see APPs 3, 6 and 7). This recognises that inappropriate handling of sensitive information can have adverse consequences for an individual or those associated with the individual. For example, discrimination or mistreatment is sometimes based on a person's race or ethnic origin or union membership. Mishandling of sensitive information may also cause humiliation or embarrassment or undermine an individual's dignity.

Use

B.145 'Use' is not defined in the Privacy Act. Use is a separate concept from disclosure, which is discussed at paragraphs B.63–B.68. As noted at paragraph B.69, many APP requirements apply to both the 'use' and 'disclosure' of personal information, and in those situations it is not necessary to distinguish both concepts.

B.146 Generally, an APP entity uses personal information when it handles and manages that information within the entity's effective control. Examples include:

- the entity accessing and reading the personal information
- the entity searching records for the personal information
- the entity making a decision based on the personal information
- the entity passing the personal information from one part of the entity to another
- unauthorised access by an employee of the entity.[46]

B.147 In limited circumstances, providing personal information to a contractor to perform services on behalf of the APP entity may be a use, rather than a disclosure (see paragraph B.63–B.68). This occurs where the entity does not release the subsequent handling of personal information from its effective control. For example, if an entity provides personal information to a cloud service provider for the limited purpose of performing the services of storing and ensuring the entity may access the personal information, this may be a 'use' by the entity in the following circumstances:

- a binding contract between the entity and the provider requires the provider only to handle the personal information for these limited purposes
- the contract requires any subcontractors to agree to the same obligations, and
- the contract gives the entity effective control of how the information is handled by the provider. Issues to consider include whether the entity retains the right or power to access, change or retrieve the information, who else will be able to access the information and for what purposes, the security measures that will be used for the

[46] An APP entity is taken to have 'used' personal information where an employee gains unauthorised access 'in the performance of the duties of the person's employment' (see s 8(1)).

storage and management of the personal information (see also APP 11.1, Chapter 11) and whether the information can be retrieved or permanently deleted by the entity when no longer required or at the end of the contract.[47]

[47] For further discussion of cloud computing considerations for agencies, see Secure Cloud Strategy, Digital Transformation Agency website <https://www.dta.gov.au>.

Chapter C:
Permitted general situations

Version 1.1, July 2019

OAIC

Contents

What are permitted general situations? 3

Lessening or preventing a serious threat to life, health or safety 3

Unreasonable or impracticable to obtain consent 3

Reasonably believes collection, use or disclosure is necessary 4

Lessen or prevent a serious threat 4

Taking appropriate action in relation to suspected unlawful activity or serious misconduct 5

Locating a person reported as missing 6

Reasonably necessary for establishing, exercising or defending a legal or equitable claim 7

Reasonably necessary for a confidential alternative dispute resolution process 7

Necessary for a diplomatic or consular function or activity 8

Necessary for certain Defence Force activities outside Australia 9

What are permitted general situations?

C.1 The information handling requirements imposed by some APPs do not apply if a 'permitted general situation' exists. This exception applies in relation to the collection of sensitive information (APP 3), the use or disclosure of personal information (APPs 6 and 8) and the use or disclosure of a government related identifier (APP 9). It is nevertheless open to an APP entity to comply with the APP requirements even though an exception applies.

C.2 There are seven permitted general situations listed in s 16A:

- lessening or preventing a serious threat to the life, health or safety of any individual, or to public health or safety (see APPs 3.4(b), 6.2(c), 8.2(d) and 9.2(d))
- taking appropriate action in relation to suspected unlawful activity or serious misconduct (see APPs 3.4(b), 6.2(c), 8.2(d) and 9.2(d))
- locating a person reported as missing (see APPs 3.4(c), 6.2(c) and 8.2(d))
- asserting a legal or equitable claim (see APPs 3.4(c) and 6.2(c))
- conducting an alternative dispute resolution process (see APPs 3.4(b) and 6.2(c))
- performing diplomatic or consular functions – this permitted general situation only applies to agencies (see APP 3.4(b), 6.2(c) and 8.2(d))
- conducting specified Defence Force activities – this permitted general situation only applies to the Defence Force (see APP 3.4(b), 6.2(c) and 8.2(d))

C.3 These permitted general situations are discussed generally below. Specific examples relevant to each APP are also given in the chapter relating to that APP.

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

C.4 This permitted general situation applies when an APP entity is collecting, using or disclosing personal information or a government related identifier, and:

- it is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure, and
- the entity reasonably believes that the collection, use or 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 (s 16A, Item 1)

Unreasonable or impracticable to obtain consent

C.5 Consent is defined as 'express consent or implied consent' (s 6(1)) and is discussed in Chapter B (Key concepts). The main criteria for establishing consent are:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent

C.6 An APP entity should be able to point to one or more clear reasons that make it unreasonable or impracticable to obtain an individual's consent. Relevant considerations may include:

- the nature of, and potential consequences associated with, the serious threat. For example, the urgency of a situation and level of threatened harm may require collection, use or disclosure before it is possible to seek consent
- the possible adverse consequences for an individual if their consent is not obtained before the collection, use or disclosure. It may be more difficult for an entity to establish that it was unreasonable or impracticable to obtain the individual's consent as the risk of adversity increases
- the source of the threat. For example, it may be unreasonable to seek consent from the individual posing the threat where that individual could reasonably be anticipated to withhold consent, or where the act of seeking that individual's consent could increase the threat
- the ability to contact the individual to obtain consent. For example, it may be impracticable to obtain consent if the individual's location is unknown after reasonable enquiries have been made, or if they cannot be contacted for another reason
- the capacity of the individual to give consent. For example, it may be unreasonable or impracticable to obtain consent where an individual is incapable of communicating consent because of their physical or psychological state or their age (capacity is discussed as part of 'consent' in Chapter B (Key concepts))
- the number of individuals whose personal information is to be collected, used or disclosed. For example, it may be impracticable to obtain consent from a very large number of individuals (though see below as to the relevance of inconvenience, time and costs)
- the inconvenience, time and cost involved in obtaining consent. However, an entity is not excused from obtaining consent by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it impracticable to obtain consent will depend on whether the burden is excessive in all the circumstances.

Reasonably believes collection, use or disclosure is necessary

C.7 Where it is unreasonable or impracticable to obtain consent, an APP entity must reasonably believe the collection, use or disclosure is necessary to lessen or prevent a serious threat. The terms 'reasonably believes' and 'necessary' are discussed in Chapter B (Key concepts).

C.8 In summary, there must be a reasonable basis for the belief, and not merely a genuine or subjective belief. It is the responsibility of an APP entity to be able to justify its reasonable belief. A collection, use or disclosure would not be considered necessary where it is merely helpful, desirable or convenient.

Lessen or prevent a serious threat

C.9 This permitted general situation applies to a serious threat to the life, health or safety of any individual, or to public health or safety. The permitted general situation would not apply after the threat has passed. A 'serious' threat is one that poses a significant danger to an individual or individuals. The likelihood of a threat occurring as well as the consequences if the threat materialises are both relevant. A threat that may have dire consequences but is

highly unlikely to occur would not normally constitute a serious threat. On the other hand, a potentially harmful threat that is likely to occur, but at an uncertain time, may be a serious threat, such as a threatened outbreak of infectious disease. This allows an APP entity to take preventative action to stop a serious threat from escalating before it materialises.

C.10 The permitted general situation applies to a threat to life, health or safety. This can include a threat to a person's physical or mental health and safety. It could include a potentially life threatening situation or one that might reasonably result in other serious injury or illness. The permitted general situation would not ordinarily extend to a threat to an individual's finances or reputation.

C.11 The threat may be to an individual the APP entity is dealing with or to another person. It may also be a threat of serious harm to an unspecified individual, such as a threat to inflict harm randomly.

C.12 A 'serious threat to public health or safety' relates to broader safety concerns affecting a number of people. Examples include:

- the potential spread of a communicable disease
- harm, or threatened harm, to a group of people due to a terrorist incident
- harm caused by an environmental disaster

C.13 If time permits, attempts could be made to seek the consent from the relevant individuals for the collection, use or disclosure, before relying on this permitted general situation.

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

C.14 This permitted general situation applies when an APP entity is collecting, using or disclosing personal information or a government related identifier, and 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 collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter (s 16A, Item 2).

C.15 This permitted general situation is intended to apply to an APP entity's internal investigations about activities within or related to the entity.[1] It applies when the entity has reason to suspect unlawful activity, as well as misconduct of a serious nature that does not necessarily amount to unlawful activity.

C.16 'Unlawful activity' is not defined in the Privacy Act. The core meaning is activity that is criminal, illegal or prohibited or proscribed by law, and can include unlawful discrimination or harassment, but does not include breach of a contract. Examples of unlawful activity include criminal offences, unlawful discrimination, and trespass. The unlawful activity must relate to the APP entity's functions or activities. For example, harassment or discrimination within an entity would be an unlawful activity.

[1] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 67.

C.17 'Misconduct' is defined in s 6(1) to include 'fraud, negligence, default, breach of trust, breach of duty, breach of discipline or any other misconduct in the course of duty'. 'Serious' misconduct does not cover minor breaches and transgressions. The serious misconduct must relate to the APP entity's functions or activities. For example, a serious breach by a staff member of the Australian Public Service Code of Conduct, or fraudulent conduct by a professional adviser or a client in relation to the entity's functions or activities.

C.18 An APP entity must have 'reason to suspect' that unlawful activity or serious misconduct is being, or may be engaged in. Though only a reasonable suspicion is required, it is the responsibility of the entity to be able to justify the suspicion.

C.19 An APP entity must 'reasonably believe' that the collection, use or disclosure of personal information is 'necessary' for the entity to take 'appropriate action'. 'Reasonably believes' and 'necessary' are discussed further in Chapter B (Key concepts). In summary, there must be a reasonable basis for the belief that the collection, use or disclosure is necessary, and not merely a genuine or subjective belief. A collection, use or disclosure would not be considered necessary where it is merely helpful, desirable or convenient. It is the responsibility of an entity to be able to justify its reasonable belief.

C.20 Whether action is 'appropriate' will depend on the nature of the suspected unlawful activity or misconduct and the nature of the action that the APP entity proposes to take. Appropriate action may include investigating an unlawful activity or serious misconduct and reporting these matters to the police or another relevant person or authority.[2] For example, if an entity reasonably believes that it cannot effectively investigate serious misconduct without collecting, using or disclosing personal information, this permitted general situation may apply.

Locating a person reported as missing

C.21 This permitted general situation applies when an APP entity reasonably believes that the collection, use or disclosure of personal information is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing. The collection, use or disclosure must comply with the rules made by the Information Commissioner under s 16A(2) (s 16A, Item 3) .

C.22 The terms 'reasonably believes' and 'reasonably necessary' are discussed further in Chapter B (Key concepts). In summary, the APP entity must have a reasonable basis for the belief that the collection, use or disclosure is reasonably necessary, and not merely a genuine or subjective belief. 'Reasonably necessary' has regard to whether a reasonable person who is properly informed would agree that the collection, use or disclosure is necessary. It is the responsibility of an entity to be able to justify that the entity reasonably believes that the collection, use or disclosure is reasonably necessary.

C.23 The rules made by the Commissioner under s 16A(2) are a legislative instrument that are available on the Federal Register of Legislation.[3]

---

[2] Where an APP entity seeks to disclose personal information to an 'enforcement body', such as the Australian Federal Police or the police force or service of a State or Territory, it may be able to rely on the exception at APP 6.2(e). APP 6.2(e) permits the use or disclosure of personal information where an APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body (see Chapter 6).

[3] See the Federal Register of Legislation website <https://www.legislation.gov.au/>.

Reasonably necessary for establishing, exercising or defending a legal or equitable claim

C.24 This permitted general situation applies if an APP entity collects, uses or discloses personal information that is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim (s 16A, Item 4).

C.25 The term 'reasonably necessary' is discussed further in Chapter B (Key concepts). In summary, it is an objective test that has regard to whether a reasonable person, who is properly informed, would agree that the collection, use or disclosure is necessary. A collection, use or disclosure would not be considered necessary where it is merely helpful, desirable or convenient. It is the responsibility of the APP entity to be able to justify that the particular collection, use or disclosure is reasonably necessary.

C.26 This permitted general situation applies to the collection, use or disclosure of personal information in relation to existing or anticipated legal proceedings in a court or tribunal. Where legal proceedings have not yet commenced, this situation will usually only apply to a collection, use or disclosure involving a real possibility of legal proceedings, for example where professional legal advice is sought about commencing legal proceedings. By contrast, this permitted general situation does not compel an APP entity to disclose personal information in response to a request from a third party, and it may be difficult for an entity to be satisfied that it is reasonably necessary to do so solely on the basis that a third party has requested the information in connection with existing or anticipated legal proceedings.

C.27 An APP should not rely on this permitted general situation to disclose personal information if doing so would be contrary to an Australian law (for example, a statutory secrecy provision) or a legal order or principle (for example, if disclosure would be a breach of legal professional privilege).

Reasonably necessary for a confidential alternative dispute resolution process

C.28 This permitted general situation applies if an APP entity collects, uses or discloses personal information that is reasonably necessary for the purposes of a confidential alternative dispute resolution process (s 16A, Item 5).

C.29 The term 'reasonably necessary' is discussed further in Chapter B (Key concepts). In summary, it is an objective test that has regard to whether a reasonable person, who is properly informed, would agree that the collection, use or disclosure is necessary. A collection, use or disclosure would not be considered necessary where it is merely helpful, desirable or convenient. It is the responsibility of the APP entity to be able to justify that the particular collection, use or disclosure is reasonably necessary.

C.30 The phrase 'alternative dispute resolution process' (or ADR) is not defined in the Privacy Act. ADR covers processes, other than judicial determinations, in which an impartial person assists those in a dispute to resolve the issues between them. That person may, but is not required to, have any particular form of accreditation. Examples of ADR processes include

mediation, conciliation, facilitation, expert assessment, determination, or neutral evaluation.[4]

C.31 For the exception to apply, the parties to the dispute and the ADR provider must be bound by confidentiality obligations such that any personal information collected, used or disclosed for the purpose of that ADR process will not be used or disclosed for any purpose outside the ADR process, including use or disclosure in subsequent proceedings. The confidentiality obligations may be imposed through contractual agreements or legislative provisions.

C.32 This permitted general situation extends to a disclosure of personal information by an APP entity to an ADR provider, a collection, use or disclosure by an entity for the purpose of participating in the ADR, and the collection, use or disclosure by an entity in relation to a complaint of professional misconduct against an ADR practitioner.

Necessary for a diplomatic or consular function or activity

C.33 This permitted general situation applies when an agency reasonably believes that the collection, use or disclosure of personal information is necessary for the agency's diplomatic or consular functions or activities (s 16A, Item 6). This permitted general situation applies only to agencies, and not to organisations. The terms 'reasonably believes' and 'necessary' are discussed further in Chapter B (Key concepts).

C.34 The terms 'diplomatic' and 'consular' are not defined in the Privacy Act. An agency can rely on this permitted general situation only if it has diplomatic or consular functions or powers, conferred either by legislation or an executive instrument (such as the Administrative Arrangements Order). The following are given as examples of when this permitted general situation might apply:

- Diplomatic functions or activities: where an agency collects, uses or discloses personal information to grant a diplomatic visa to a foreign national accredited as a member of the diplomatic staff of a mission to Australia.
- Consular functions or activities: where an agency collects, uses or discloses personal information to:
    - assist Australian citizens who are in distress overseas, including 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, or to provide assistance in response to a crisis or emergency overseas
    - provide information to the next of kin of an Australian individual who is overseas where, for example, the individual is seriously injured or is suffering serious physical or mental illness, and the agency considers that there are likely to be significant, serious or undesirable consequences for the individual or their next of kin if it does not disclose the personal information

[4] Attorney-General's Department and National Alternative Dispute Resolution Advisory Council (NADRAC), Your Guide to Dispute Resolution, viewed 6 February 2014, Attorney-General's Department website <https://www.ag.gov.au>.

Necessary for certain Defence Force activities outside Australia

C.35 This permitted general situation applies to the collection, use or disclosure of personal information by the Defence Force, where it reasonably believes that the collection, use or disclosure is necessary for any of the following occurring outside Australia and the external Territories:

- war or warlike operations
- peacekeeping or peace enforcement
- civil aid, humanitarian assistance, medical or civil emergency or disaster relief (s 16A, Item 7)

C.36 For a discussion of 'reasonably believes' and 'necessary', see Chapter B (Key concepts).

C.37 The following are given as examples of when this permitted general situation might apply:

- War or warlike operations/peacekeeping or peace enforcement: where the Defence Force collects sensitive information, such as biometric information, about an enemy or other hostile adversary and uses and discloses this and other personal information in order to support Defence Force military operations.
- Civil aid, humanitarian assistance, medical or civil emergency or disaster relief: where the Defence Force collects sensitive information about an individual in the immediate aftermath of a natural or man-made disaster outside Australia and the external Territories, and uses or discloses this and other personal information in order to trace the individual or relatives of the individual, or assist in the provision of proper medical care.

Chapter D:
Permitted health situations

Version 1.1, July 2019

OAIC

Contents

What are permitted health situations? 3

Collection — providing a health service 3

Collection — conducting research; compiling or analysing statistics; management, funding or monitoring of a health service 4

Public health or public safety 4

Management, funding or monitoring of a health service 4

De-identified information 5

Impracticable to obtain consent 5

Guidelines approved under s 95A 5

Disclosure of personal information collected under this permitted health situation 5

Use or disclosure — conducting research; compiling or analysing statistics 6

Use or disclosure — necessary to prevent a serious threat to the life, health or safety of a genetic relative 6

Disclosure — responsible person for an individual 7

Incapacity to give consent 8

Cannot communicate consent 8

Carer 8

Wishes of the individual 9

What are permitted health situations?

D.1 The information handling requirements imposed by APP 3 and APP 6 do not apply to an organisation if a 'permitted health situation' exists. This exception applies to the collection, use or disclosure of health information or genetic information by an organisation. The exception applies only to organisations, and not to agencies. It is open to an organisation to comply with the APP requirements even though an exception applies.

D.2 There are five permitted health situations listed in s 16B:

- the collection of health information to provide a health service (s 16B(1)) (see APP 3.4(c))
- the collection of health information for certain research and other purposes (s 16B(2)) (see APP 3.4(c))
- the use or disclosure of health information for certain research and other purposes (s 16B(3)) (see APP 6.2(d))
- the use or disclosure of genetic information (s 16B(4)) (see APP 6.2(d))
- the disclosure of health information for a secondary purpose to a responsible person for an individual (s 16B(5)) (see APP 6.2(d))

D.3 'Health information' is defined in s 6(1). It is a type of sensitive information and is discussed in more detail in Chapter B (Key concepts). Genetic information is not defined in the Privacy Act, and is discussed in paragraphs D.26–D.27 below.

D.4 The permitted health situations are discussed generally below. For specific examples that are relevant to APPs 3 and 6, see Chapters 3 and 6.

Collection — providing a health service

D.5 This permitted health situation applies when an organisation is collecting health information about an individual, if the information is necessary to provide a health service to the individual, and either:

- the collection is required or authorised by or under an Australian law (other than the Privacy Act), or
- the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation (s 16B(1))

D.6 The terms 'necessary', 'health service' and 'required or authorised by or under Australian law' are discussed in Chapter B (Key concepts).

D.7 This permitted health situation overlaps with another exception stated in APP 3.4(a), namely the collection of sensitive information (which includes health information) as required or authorised by or under law or a court/tribunal order.

D.8 In deciding whether the collection of health information is 'necessary' to provide a health service, an organisation should consider if there are reasonable alternatives available. Further, an organisation should collect only the minimum amount of health information needed to provide a health service.

D.9 The Privacy Act does not specify which bodies qualify as 'competent health or medical bodies'. Common examples include medical boards and other rule-making bodies

recognised in an applicable Australian law. An important requirement is that the organisation collecting the information does so in accordance with rules established by such a body, is bound by those rules, and those rules impose obligations of professional confidentiality. Generally, a binding rule is one that will attract a sanction or adverse consequence if breached.

Collection — conducting research; compiling or analysing statistics; management, funding or monitoring of a health service

D.10 This permitted health situation applies when an organisation is collecting health information about an individual, if the collection is necessary for research relevant to public health or public safety, the compilation or analysis of statistics relevant to public health or public safety, or the management, funding or monitoring of a health service, and:

- the particular purpose cannot be served by collecting de-identified information
- it is impracticable to obtain the individual's consent, and
- the collection is either:
  - required by or under an Australian law (other than the Privacy Act)
  - in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation, or
  - in accordance with guidelines approved under s 95A (s 16B(2))

D.11 The terms 'necessary', 'de-identified', 'consent' and 'required by or under an Australian law' are discussed in Chapter B (Key concepts). Collection in accordance with rules of a competent health or medical body is discussed in paragraph D.9 of this chapter.

D.12 This permitted health situation overlaps with another exception stated in APP 3.4(a), namely the collection of sensitive information (which includes health information) as required or authorised by or under law or a court/tribunal order.

Public health or public safety

D.13 The phrase 'relevant to public health or public safety' is not defined in the Privacy Act. Illustrative examples include research or the compilation or analysis of statistics relating to communicable diseases, cancer, heart disease, mental health, injury control and prevention, diabetes and the prevention of childhood diseases.

Management, funding or monitoring of a health service

D.14 Examples of where health information about an individual may be collected for the 'management, funding or monitoring of a health service' include collection by:

- a quality assurance body, of data about the quality of a health service provided by a nursing home or hostel
- an oversight body, of information from a private hospital about an incident occurring in an individual's health treatment

- a health insurer, of information relevant to possible fraud or an incorrect payment

De-identified information

D.15 An organisation should consider whether the purposes listed in s 16B(2)(a) can be achieved by collecting de-identified information, rather than personal information. If they can, this permitted health situation will not apply.

Impracticable to obtain consent

D.16 The following are given as examples of where it may be impracticable for an organisation to obtain an individual's consent to the collection of health information for one of the purposes listed in this permitted health situation:

- the integrity or validity of health research could be impaired, for example, because the organisation is conducting a participant observation study and obtaining the consent of participants may alter their behaviour and the research results. Consideration could be given to consulting a human research ethics committee as to whether obtaining consent would have this effect
- where obtaining the individual's consent would adversely impact an investigation or monitoring activity
- there are no current contact details for the individual and the organisation has insufficient information to obtain up-to-date contact details

D.17 It is the responsibility of an organisation relying on this permitted health situation to be able to justify why it would be impracticable to obtain an individual's consent. Incurring some expense or doing extra work to obtain consent would not by itself make it impracticable to obtain consent.

Guidelines approved under s 95A

D.18 The 'guidelines approved under s 95A' are issued by the National Health and Medical Research Council (NHMRC) or a 'prescribed authority', and approved by the Information Commissioner.[1]

Disclosure of personal information collected under this permitted health situation

D.19 An organisation that collects personal information under this permitted health situation, must take reasonable steps to ensure that the information is de-identified before it is disclosed (APP 6.4 (Chapter 6)).

[1] See National Health and Medical Research Council (NHMRC), Guidelines Approved Under Section 95A of the Privacy Act 1988, NHMRC website <https://www.nhmrc.gov.au>.

Use or disclosure — conducting research; compiling or analysing statistics

D.20 This permitted health situation applies when an organisation is using or disclosing health information about an individual, if the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety, and:

- it is impracticable to obtain the individual's consent to the use or disclosure
- the use or disclosure is conducted in accordance with guidelines approved under s 95A, and
- in the case of disclosure — the organisation reasonably believes that the recipient of the information will not disclose the information, or personal information derived from that information (s 16B(3))

D.21 The terms 'necessary' and 'reasonably believes' are discussed in Chapter B (Key concepts); 'relevant to public health or public safety' is discussed in paragraph D.13; 'impracticable to obtain an individual's consent' is discussed in paragraph D.16–D.17; and 'guidelines approved under s 95A' is discussed in paragraph D.18.

D.22 When considering whether a use or disclosure is 'necessary' under this permitted health situation, an organisation should consider whether the research or statistical compilation or analysis could be undertaken using or disclosing de-identified information. If so, the use or disclosure of personal information would not be considered necessary. De-identification is discussed in Chapter B (Key concepts).

D.23 An organisation cannot rely on this permitted health situation to disclose health information unless it reasonably believes that the recipient will not disclose the information or personal information derived from that information. It is the responsibility of the organisation to be able to justify its reasonable belief.

Use or disclosure — necessary to prevent a serious threat to the life, health or safety of a genetic relative

D.24 This permitted health situation applies when an organisation is using or disclosing genetic information about an individual, if:

- the organisation has obtained the information in the course of providing a health service to the individual
- the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another individual who is a genetic relative of the individual
- the use or disclosure is conducted in accordance with guidelines approved under s 95AA, and
- in the case of disclosure — the recipient of the information is a genetic relative of the individual (s 16B(4))

D.25 The terms 'health service', 'necessary' and 'reasonably believes' are discussed in Chapter B (Key concepts). The phrase 'serious threat to life, health or safety' is discussed in Chapter C (Permitted general situations).

D.26 'Genetic information' is not defined in the Privacy Act. Genetic information about an individual is, however, included in the definition of 'sensitive information' (s 6(1)). Genetic information that is 'about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual' is also covered by the definition of 'health information' (s 6(1)).' This permitted health situation applies to genetic information whether it is sensitive information or health information.

D.27 This permitted health situation applies to genetic information about an individual that an organisation has obtained from any source in the course of providing a health service to the individual. For example, the genetic information may include the results of a parentage test, or information from other sources that confirms a condition that is clinically apparent or that may predict the likelihood of an individual developing a condition.

D.28 A 'genetic relative' is defined in s 6(1) to mean an individual who is related by blood, including but not limited to a sibling, a parent or a descendant.

D.29 A serious threat to the life, health or safety of a genetic relative could include a threat to their physical or mental health. Whether a threat is serious can include consideration of both the likelihood of a threat occurring as well as the consequences if the threat materialises.

D.30 The 'guidelines approved under s 95AA' are issued by the NHMRC and approved by the Information Commissioner.[2]

Disclosure — responsible person for an individual

D.31 This permitted health situation applies when an organisation discloses health information about an individual, and:

- the organisation provides a health service to the individual
- the recipient of the information is a responsible person for the individual
- the individual is either physically or legally incapable of giving consent to the disclosure, or physically cannot communicate consent to the disclosure
- another individual providing the health service for the organisation (the 'carer') is satisfied that either the disclosure is necessary to provide appropriate care or treatment of the individual, or the disclosure is made for compassionate reasons
- the disclosure is not contrary to any wish expressed by the individual before the individual became unable to give or communicate consent of which the carer is aware or of which the carer could reasonably be expected to be aware, and

[2] See National Health and Medical Research Council (NHMRC), Use and Disclosure of Genetic Information to a Patient's Genetic Relatives under Section 95AA of the Privacy Act 1988: Guidelines for Health Practitioners in the Private Sector, NHMRC website <https://www.nhmrc.gov.au>.

- the disclosure is limited to the extent reasonable and necessary to provide appropriate care or treatment of the individual or to fulfil the purpose of making a disclosure for compassionate reasons (s 16B(5))

D.32 The terms 'health service', 'consent' (including capacity), 'reasonable' and 'necessary' are discussed in Chapter B (Key concepts). A 'responsible person' is defined in s 6AA and includes for example, a parent, adult child, spouse, partner, relative, guardian or nominee of an individual.

Incapacity to give consent

D.33 An individual may be 'physically or legally incapable of giving consent' if they cannot understand the nature of a consent decision, including the effect of giving or withholding consent, forming a view based on reasoned judgement and how to communicate a consent decision. Issues that may affect an individual's capacity to give consent include:

- age
- physical or mental disability
- temporary or incremental incapacity, for example, during a psychotic episode, a temporary psychiatric illness, or because the person is unconscious, in severe distress, or suffering dementia
- limited understanding of English

D.34 An organisation should consider whether any such issue could be addressed by providing the individual with appropriate support to enable them to have capacity.

Cannot communicate consent

D.35 Where an individual physically cannot communicate consent to the disclosure, an organisation may disclose the individual's personal information to a responsible person, without having to form a view as to the individual's capacity (provided the other criteria in this permitted health situation are satisfied).

Carer

D.36 For the purposes of this permitted health situation, a 'carer' is an individual who is providing the health service for the organisation, such as a doctor, nurse, pharmacist, locum, visiting medical officer or qualified employee of the organisation. This is different to the use of the term 'carer' in other situations, as referring for example to a family member, close friend or other person who cares for the individual but does not provide a health service.

D.37 The carer must be satisfied that it is necessary to disclose the individual's health information to a responsible person for the individual in order to provide appropriate care or treatment or for compassionate reasons. This requires a practical judgement by the carer. For example, the carer may be satisfied that ongoing care cannot be guaranteed without the disclosure occurring.

D.38 A compassionate reason for disclosure may include an update about the condition or progress of an unconscious patient to family members or an emergency contact.

Wishes of the individual

D.39 The disclosure must not be contrary to any wish expressed by the individual before they were unable to give or communicate consent. An individual's wish or preference need not have been communicated in writing but may have been earlier communicated in anticipation of the individual no longer being able to make decisions about their health information, for example, where an individual has a degenerative condition which will lead to a lack of capacity.

D.40 An example of where a carer could be reasonably aware of an individual's wishes is where they are noted on the individual's medical record. An individual's wishes may also have been expressed verbally during clinician-patient consultations, prior to the individual losing capacity to consent.

D.41 An individual's wishes would be unlikely to override a guardianship order or other relevant legal authority, unless that guardianship order or other legal authority is limited or makes reference to the patient's wishes. In these circumstances, an organisation should consider whether it can disclose the information under APP 6.2(b).

Chapter 1:

Australian Privacy Principle 1 —

Open and transparent management of personal information

Version 1.2, October 2025

Contents

Key points 3

What does APP 1 say? 3

Implementing practices, procedures and systems to ensure APP compliance 4

Developing an APP Privacy Policy 5

Information that must be included in an APP Privacy Policy 6
Other matters for inclusion in an APP Privacy Policy 10

Making an APP Privacy Policy publicly available 10

Making an APP Privacy Policy available free of charge and in an appropriate form 10
Making an APP Privacy Policy available in a requested form 11

Key points

- APP 1 outlines the requirements for an APP entity to manage personal information in an open and transparent way.
- An APP entity must take reasonable steps to implement practices, procedures and systems that will ensure it complies with the APPs and any binding registered APP code, and is able to deal with related inquiries and complaints.
- An APP entity must have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information.
- An APP entity must take reasonable steps to make its APP Privacy Policy available free of charge and in an appropriate form (usually on its website).
- An APP entity must, upon request, take reasonable steps to provide a person or body with a copy of its APP Privacy Policy in the particular form requested.

From 10 December 2026, an APP entity must include additional information in its APP Privacy Policy if it arranges for a computer program to use personal information to make decisions that could reasonably be expected to significantly affect the rights or interests of an individual.[1]

What does APP 1 say?

1.1 The declared object of APP 1 is 'to ensure that APP entities manage personal information in an open and transparent way' (APP 1.1). This enhances the accountability of APP entities for their personal information handling practices and can build community trust and confidence in those practices.

1.2 APP 1 imposes obligations upon an APP entity to:

- take reasonable steps to implement practices, procedures and systems that will ensure the entity complies with the APPs and any binding registered APP code, and is able to deal with related inquiries and complaints (APP 1.2)
- have a clearly expressed and up-to-date APP Privacy Policy about how the entity manages personal information (APP 1.3 and 1.4)
- take reasonable steps to make its APP Privacy Policy available free of charge in an appropriate form (APP 1.5) and, upon request, in a particular form (APP 1.6)

[1] APPs 1.7, 1.8 and 1.9 were introduced by the *Privacy and Other Legislation Amendment Act 2024* (Cth) and commence on 10 December 2026. These APP 1 amendments apply in relation to decisions made from this date, regardless of whether the arrangement for a computer program to make the decision was made before or after this date, and regardless of whether the personal information was used, or acquired or created in the operation of the computer program before or after this date.

From 10 December 2026, APP entities will have additional obligations to ensure APP Privacy Policies contain specified information if the APP entity arranges for a computer program to use personal information to make decisions that could reasonably be expected to significantly affect the rights or interests of an individual (APP 1.7, APP 1.8 and APP 1.9).[2]

1.3 APP 1 lays down the first step in the information lifecycle – planning and explaining how personal information will be handled before it is collected. APP entities will be better placed to meet their privacy obligations under the Privacy Act if they embed privacy protections in the design of their information handling practices.

Implementing practices, procedures and systems to ensure APP compliance

1.4 APP 1.2 requires an APP entity to take reasonable steps to implement practices, procedures and systems relating to the entity's functions or activities that will:

- ensure the entity complies with the APPs and any binding registered APP code (see Part IIIB), and
- enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the APPs and any binding registered APP code.

1.5 APP 1.2 imposes a distinct and separate obligation upon an APP entity, in addition to being a general statement of its obligation to comply with other APPs. The purpose of APP 1.2 is to require an entity to take proactive steps to establish and maintain internal practices, procedures and systems that ensure compliance with the APPs. The obligation is a constant one. An entity could consider keeping a record of the steps taken to comply with APP 1.2, to demonstrate that personal information is managed in an open and transparent way.

1.6 The requirement to implement practices, procedures and systems is qualified by a 'reasonable steps' test. The reasonable steps that an APP entity should take will depend upon circumstances that include:

- the nature of the personal information held. More rigorous steps may be required as the amount and sensitivity of personal information handled by an APP entity increases
- the possible adverse consequences for an individual if their personal information is not handled as required by the APPs. More rigorous steps may be required as the risk and severity of possible adverse consequences increases
- the nature of the APP entity. Relevant considerations include an entity's size, resources and its business model. For example, the reasonable steps expected of an entity that operates through franchises or dealerships, or gives database and network access to contractors, may differ from the reasonable steps required of a centralised entity, and

[2] APPs 1.7, 1.8 and 1.9 were introduced by the *Privacy and Other Legislation Amendment Act 2024* (Cth) and commence on 10 December 2026. These APP 1 amendments apply in relation to decisions made from this date, regardless of whether the arrangement for a computer program to make the decision was made before or after this date, and regardless of whether the personal information was used, or acquired or created in the operation of the computer program before or after this date.

- the practicability, including time and cost of implementing practices, procedures and systems. The 'reasonable steps' test recognises that privacy protection must be viewed in the context of the practical options available to an APP entity. However, an entity is not excused from implementing particular practices, procedures or systems 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.

1.7 The following are given as examples of practices, procedures and systems that an APP entity should consider implementing:

- procedures for identifying and managing privacy risks at each stage of the information lifecycle, including collection, use, disclosure, storage, destruction or de-identification
- security systems for protecting personal information from misuse, interference and loss and from unauthorised access, modification or disclosure (such as IT systems, internal access controls and audit trails) (see also Chapter 11 (APP 11))
- a commitment to conducting a Privacy Impact Assessment (PIA) for new projects in which personal information will be handled, or when a change is proposed to information handling practices. Whether a PIA is appropriate will depend on a project's size, complexity and scope, and the extent to which personal information will be collected, used or disclosed[3]
- procedures for identifying and responding to privacy breaches, handling access and correction requests and receiving and responding to complaints and inquiries[4]
- procedures that give individuals the option of not identifying themselves, or using a pseudonym, when dealing with the entity in particular circumstances (see also Chapter 2 (APP 2))
- governance mechanisms to ensure compliance with the APPs (such as designated privacy officers and regular reporting to the entity's governance body)
- regular staff training and information bulletins on how the APPs apply to the entity, and its practices, procedures and systems developed under APP 1.2
- appropriate supervision of staff regularly handling personal information, and reinforcement of the entity's APP 1.2 practices, procedures and systems
- mechanisms to ensure that agents and contractors in the service of, or acting on behalf of, the entity comply with the APPs, and
- a program of proactive review and audit of the adequacy and currency of the entity's APP Privacy Policy and of the practices, procedures and systems implemented under APP 1.2.

Developing an APP Privacy Policy

1.8 APP 1.3 requires an APP entity to have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information. At a minimum, a clearly expressed policy should be easy to understand (avoiding jargon, legalistic and in-house terms), easy to

[3] Further information about Privacy Impact Assessments is contained in OAIC, Guide to Undertaking Privacy Impact Assessments, OAIC website <https://www.oaic.gov.au>.

[4] For example, see OAIC, Data Breach Preparation and Response, OAIC website <https://www.oaic.gov.au>.

navigate, and only include information that is relevant to the management of personal information by the entity. As the policy will usually be available on the entity's website (see paragraph 1.37), it should be written in a style and length that makes it suitable for web publication.[5]

1.9 An APP entity should regularly review and update its APP Privacy Policy to ensure that it reflects the entity's information handling practices. This review could, at a minimum, be undertaken as part of an entity's annual planning processes. An entity could also:

- include a notation on the policy indicating when it was last updated
- invite comment on the policy to evaluate its effectiveness, and explain how any comments will be dealt with

1.10 An APP Privacy Policy should explain how the APP entity manages the personal information it collects, and the information flows associated with that personal information. This reflects the central object of APP 1, which is to ensure that entities manage personal information in an open and transparent manner. The policy is not expected to contain detail about all the practices, procedures and systems adopted to ensure APP compliance. The policy also differs from a collection notice provided to an individual under APP 5.1, which will provide specific information relevant to a particular collection of personal information (see Chapter 5 (APP 5)).

1.11 It is open to an APP entity to choose the style and format for its APP Privacy Policy, so long as the policy is clearly expressed, up-to-date and otherwise complies with the requirements of APP 1.

1.12 Where an APP Privacy Policy is made available online, using a layered approach to the provision of the information may assist an individual's understanding of the information in the policy. A layered approach means providing a condensed version of the full policy to outline key information, with direct links to the more detailed information in the full policy.[6]

1.13 An APP Privacy Policy should be tailored to the specific information handling practices of an entity. For example, for a large APP entity where distinct business units handle personal information differently, it may be appropriate for the entity to have a set of policies to cover the different types of personal information handled or different information handling practices.

1.14 The APP Privacy Policy should be directed to the different audiences who may consult it. Primarily this will be individuals whose personal information is, or is likely to be, collected or held by the APP entity. If personal information relevant to particular classes of people or segments of the community is handled differently within the entity, this could be explained and signposted by headings. For example, different practices may be adopted in the entity for handling personal information relating to young people or people with a disability.

Information that must be included in an APP Privacy Policy

1.15 APP 1.4 contains a non-exhaustive list of information that an APP entity must include in its APP Privacy Policy:

[5] The OAIC has developed a guide to help mobile device application (app) developers embed better privacy practices in their products and services, see OAIC, Mobile Privacy: A Better Practice Guide for Mobile App Developers, OAIC website <https://www.oaic.gov.au>.

[6] For an example of a layered approach, see OAIC, Privacy Policy Summary, OAIC website <https://www.oaic.gov.au>.

- the kinds of personal information collected and held by the entity (APP 1.4(a))
- how personal information is collected and held (APP 1.4(b))
- the purposes for which personal information is collected, held, used and disclosed (APP 1.4(c))
- how an individual may access their personal information and seek its correction (APP 1.4(d))
- how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled (APP 1.4(e)), and
- whether the entity is likely to disclose personal information to overseas recipients (APP 1.4(f)), and if so, the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy (APP 1.4(g)).

1.16 Further guidance is set out below.

Kinds of personal information collected and held

1.17 An APP Privacy Policy must describe in general terms the kinds of personal information an APP entity usually collects and holds (APP 1.4(a)). The terms 'collects' and 'holds' are discussed in Chapter B (Key concepts). For example, the policy may list personal information holdings as 'contact details', 'employment history', 'educational qualifications' and 'complaint details'.

1.18 'Sensitive information' collected or held by the entity could be separately listed ('sensitive information' is defined in s 6(1) and discussed in Chapter B (Key concepts)). For example, a policy may list sensitive information relating to 'health information about an individual', 'racial or ethnic origin', 'criminal records', 'religious affiliation' and 'political opinions.'

How personal information is collected and held

1.19 An APP Privacy Policy must explain an APP entity's usual approach to collecting personal information (APP 1.4(b)). For example, the policy may explain whether personal information is collected directly from individuals or from list purchases, competitions, or referrals from individuals or other entities.

1.20 The policy must describe an APP entity's usual approach to holding personal information. This should include how the entity stores and secures personal information. For example, the policy may explain that personal information is stored by a third party data storage provider, or is combined or linked to other information held about an individual. The description of security measures should not provide details that jeopardise the effectiveness of those measures.

Purposes for which the entity collects, holds, uses and discloses personal information

1.21 An APP Privacy Policy must describe the purposes for which personal information is usually collected, held, used and disclosed (APP 1.4(c)). An APP entity is not expected to publish details of purposes that form part of normal internal business practices, such as auditing, business planning, billing, and de-identifying personal information. The description of purposes could indicate the range of people or entities to which personal information is usually disclosed, and details about an entity's functions or activities that involve personal

information that are contracted out. An organisation could also indicate if personal information is shared with a related body corporate.[7] Discussion of the terms 'purpose', 'collects', 'holds', 'uses' and 'discloses' is in Chapter B (Key concepts).

Accessing and seeking correction of personal information

1.22 An APP Privacy Policy must explain the procedure an individual can follow to gain access to or seek correction of personal information the APP entity holds (APP 1.4(d)). At a minimum, the policy should state:

- that individuals have a right to request access to their personal information and to request its correction (APPs 12 and 13), and
- the position title, telephone number, postal address and email address of a contact person for requests to access and correct personal information. An APP entity could establish a generic telephone number and email address that will not change with staff movements (for example privacy@agency.gov.au).[8]

1.23 If an APP entity wishes an individual to follow a particular procedure in requesting access to or correction of their personal information, the entity could publish that procedure and draw attention to it, for example, by providing a link in the entity's APP Privacy Policy. However, an APP entity cannot require the individual to follow a particular procedure to make the access or correction request (see Chapter 12 (APP 12) and Chapter 13 (APP 13)).

1.24 An agency's APP Privacy Policy could also refer to the *Freedom of Information Act 1982* (FOI Act) and explain that the access and correction requirements in the Privacy Act operate alongside and do not replace other informal or legal procedures by which an individual can be provided with access to, or correction of, their personal information, including the FOI Act (this is discussed in more detail in Chapter 12 (APP 12) and Chapter 13 (APP 13)).

1.25 An APP entity may have other specific access or correction obligations outside the Privacy Act (for example the Consumer Data Right under Part IVD of the *Competition and Consumer Act 2010).* In such cases, the APP entity could also refer or explain those obligations where appropriate.

Complaints about a breach of the APPs or a binding registered APP code

1.26 An APP Privacy Policy must explain how an individual can complain about an APP entity's breach of the APPs or a binding registered APP code (APP 1.4(e)). It is implicit in this requirement that an entity which is bound by a binding, registered APP code should clearly state that fact and name the code.

1.27 Details that should also be included in the APP Privacy Policy are the procedure and contact details for complaining directly to the APP entity (see for example, the generic contact details in paragraph 1.22) and, where applicable, the procedure for complaining to an

[7] Section 13B of the Privacy Act permits 'related bodies corporate' to share personal information in some circumstances. Related bodies corporate are discussed in Chapter B (Key concepts). The sharing of information between related bodies corporate is discussed in Chapter 3 (APP 3) and Chapter 6 (APP 6).

[8] The OAIC has published guidance for agencies about developing their access to information webpages. This includes recommendations about adopting an 'Access to information' icon. This guidance may assist agencies in developing online access and correction processes, which could then be explained in the APP Privacy Policy under APP 1.4(d). See OAIC, Guidance for Agency Websites: 'Access to Information' Web Page, OAIC website <https://www.oaic.gov.au>.

external complaint body (such as an external dispute resolution scheme of which the entity is a member and that is recognised by the Information Commissioner).[9] The policy could inform individuals of the different stages in complaint handling: in most cases, a complaint should first be made in writing to the entity, as required by s 40(1A), and that the entity should be given a reasonable time (usually 30 days) to respond; following engagement with the entity, a complaint may be taken to a recognised external dispute resolution scheme of which the entity is a member; and, after those avenues have been considered, a complaint may be taken to the OAIC.

1.28 The policy could refer to other complaint avenues that operate alongside the Privacy Act. For example, banks are required to provide information to customers about complaint handling and dispute resolution in relation to the bank's obligations under the *Corporations Act 2001*, the Code of Banking Practice, and the Electronic Funds Transfer Code of Conduct. In these circumstances, the APP Privacy Policy could note the different procedures for privacy and non-privacy complaints (or link to other explanatory material the APP entity has published).

Likely overseas disclosures

1.29 An APP Privacy Policy must set out whether personal information is likely to be disclosed to overseas recipients and the countries in which such recipients are likely to be located 'if it is practicable to specify those countries in the policy' (APP 1.4(f) and 1.4(g)). This includes a likely disclosure to a related body corporate located overseas, and the country in which that body is located. An APP entity can be regarded as likely to disclose personal information to an overseas recipient if it is the entity's current practice or it has established plans to do so.

1.30 An APP entity is required to set out in the policy only likely disclosures of personal information to overseas recipients, and not likely uses of personal information by the entity. For example, routing personal information, in transit, through a server located outside Australia would usually be considered a 'use'.[10] Similarly, it would also be a use and not a disclosure for an entity to make personal information accessible to an overseas office of the entity, such as a consular office.[11] For further discussion of the requirements applying to a cross-border disclosure of personal information, and what is considered a disclosure, see Chapter 8 (APP 8).

1.31 An example of when it may be impracticable to specify the countries in which overseas recipients of personal information are likely to be located is where personal information is likely to be disclosed to numerous overseas recipients and the burden of determining where those recipients are likely to be located is excessively time-consuming, costly or inconvenient in all the circumstances. However, an APP entity is not excused from specifying the countries by reason only that it would be inconvenient, time-consuming or impose some cost to do so. As in other examples, it is the responsibility of the entity to be able to justify that this is impracticable.

1.32 If personal information is disclosed to numerous overseas locations, one practical option may be to list those countries in an appendix to the APP Privacy Policy rather than in the body of the policy. Another option in these circumstances may be to include a link in the APP

[9] Further information about external dispute resolution schemes recognised by the Information Commissioner is available in OAIC, Guidelines for Recognising External Dispute Resolution Schemes, OAIC website <https://www.oaic.gov.au>.

[10] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.

[11] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.

Privacy Policy to a regularly updated list of those countries, accessible from the APP entity's website. Where it is not practicable to specify the countries, the entity could instead identify general regions (such as European Union countries).

1.33 This requirement to describe overseas disclosure practices in an APP Privacy Policy complements the obligation on an APP entity under APP 5.2(j) and (i) to notify an individual when personal information is being collected if the personal information is likely to be disclosed to overseas recipients and the location of those recipients (see Chapter 5 (APP 5)).

Other matters for inclusion in an APP Privacy Policy

1.34 The list of matters that must be included in an APP Privacy Policy, as discussed above, is not exhaustive. In all cases, the policy should contain sufficient information to describe how the APP entity manages personal information.

1.35 The following are examples of other information that could be included:

- any exemptions under the Privacy Act that apply to personal information held by the entity or to any of its acts or practices
- whether the APP entity retains a record of personal information about all individuals (or categories of persons) with whom it deals
- who, other than the individual, can access personal information, and the conditions for access
- the entity's process or schedule for updating its APP Privacy Policy, and how changes will be publicised
- if the entity interacts with and collects personal information about a vulnerable segment of the community (such as children), the criteria that will be applied and the procedure that will be followed in collecting and holding that personal information
- the situations in which a person can deal with the entity by not identifying themselves or by using a pseudonym (see APP 2, Chapter 2), and
- information retention or destruction practices or obligations that are specific to the entity.

Making an APP Privacy Policy publicly available

Making an APP Privacy Policy available free of charge and in an appropriate form

1.36 APP 1.5 requires an APP entity to take reasonable steps to make its APP Privacy Policy available free of charge, and in an appropriate form. This furthers the objective of APP 1 of ensuring that personal information is managed in an open and transparent way.

1.37 An APP entity is generally expected to make its policy available by publishing it on its website (see Note to APP 1.5). The information in the policy may be provided using a layered approach (see paragraph 1.12 above). The policy should be prominently displayed, accessible and easy to download. For example, a prominent link or privacy icon, displayed on each page of the entity's website, could provide a direct link to the APP Privacy Policy. If it is foreseeable that the policy may be accessed by individuals with special needs (such as

individuals with a vision impairment, or individuals from a non-English speaking background), appropriate accessibility measures should be available. Agencies are also required to comply with any applicable government or statutory accessibility requirements.[12]

1.38 Online publication may not be appropriate in some circumstances, for example, where the APP entity does not have an online presence or, where individuals who regularly interact with the entity may not have internet access. In these circumstances, options that an entity should consider include:

- displaying the policy on a stand at the entity's premises, so that it can be seen by members of the public
- distributing a printout of the policy on request
- including details about how to access the policy at the bottom of all correspondence to individuals, and
- where the entity interacts with individuals by telephone, informing them during the telephone call of how the policy may be accessed in a particular form.

Making an APP Privacy Policy available in a requested form

1.39 APP 1.6 requires an APP entity, upon request, to take reasonable steps to provide a person or body with a copy of its APP Privacy Policy in the form requested. This should be done as soon as reasonably practicable after the request is received.

1.40 The reference to a 'body' requesting a copy of a policy makes it clear that a request may be made other than by an individual or entity that is subject to the Privacy Act.

1.41 An APP entity can decline to provide a copy of its APP Privacy Policy in a particular form if it would not be reasonable in the circumstances to meet the request. The steps that are reasonable will depend upon:

- other steps taken by the entity to make its policy publicly available and accessible
- the practicability, including time and cost involved. However, an entity is not excused from providing a copy in a particular form 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
- the sensitivity of the personal information held. More rigorous steps may be required where the entity holds 'sensitive information' (defined in s 6(1) and discussed in Chapter B (Key concepts)) or information of a sensitive nature
- whether the entity has unique or unusual information handling practices
- any reasons given by the body or person for requesting the policy in a particular form, and
- any accessibility or other specific needs of the body or person requesting the policy. For example, it may be reasonable to provide the policy in a form that can be accessed via assistive technology where appropriate.

[12] See, for example, Digital Service Standard Criteria — 9. Make It Accessible, DTA website <https://www.dta.gov.au>.

1.42 Inherent in the obligation to take 'reasonable steps' is an expectation that an APP Privacy Policy will usually be made available free of charge. The cost of doing so should be treated as part of an APP entity's normal operating costs. If a charge is imposed, the reason for the charge and the basis of calculation should be clearly communicated and explained before the policy is made available in the requested form, and the charge should be calculated at the lowest reasonable cost.

1.43 If a request for access in a particular form is declined, the APP entity should explain this decision to the person or body making the request. The entity should be prepared to undertake reasonable consultation with the requester about the request.

New obligations about automated decisions from December 2026

From 10 December 2026, there will be additional obligations for APP entities to include information in an APP Privacy Policy (APP 1.7) if:

- the APP entity has arranged for a computer program to make, or do a thing that is substantially and directly related to making, a decision
- where that decision could reasonably be expected to significantly affect the rights or interests of an individual, and
- personal information about the individual is used in the operation of the computer program to make the decision or do the thing.

What information will need to be included in an APP Privacy Policy regarding automated decision making?

The APP Privacy Policy will need to contain information (APP 1.8) about:

- the kinds of personal information used in the operation of computer programs
- the kinds of decisions made solely by the operation of computer programs, and
- the kinds of decisions for which a thing, that is substantially and directly related to making the decision, is done by the operation of such computer programs.

What is a 'decision' that may affect the rights or interests of an individual?

APP 1.9 outlines that 'making a decision' for the purposes of APP 1.8 and APP 1.9 includes refusing or failing to make a decision. These obligations also apply regardless of whether the decision is beneficial or adverse to the individual.

Examples of the kinds of decisions that may affect the rights or interests of an individual include:

- a decision made under a provision of an Act or a legislative instrument to grant (or refuse to grant) a benefit to the individual, such as a decision about granting admission to a country or entitlement to a housing benefit
- a decision that affects the individual's rights under a contract, agreement or arrangement, such as a contract for a life insurance policy, and
- a decision that affects the individual's access to a significant service or support, such as access to healthcare services.

The OAIC will be publishing detailed guidance about these new APP 1 obligations for automated decisions in 2026.

In the meantime, for more information, including examples of the kinds of arrangements and decisions that would apply, please refer to Part 15—Automated decisions and privacy policies in the *Privacy and Other Legislation Amendment Act 2024* (Cth) and the explanatory memoranda.

Chapter 2:

Australian Privacy Principle 2 —

Anonymity and pseudonymity

Version 1.1, July 2019

OAIC

Contents

Key points 3

What does APP 2 say? 3

The difference between anonymity and pseudonymity 3

Anonymity 3

Pseudonymity 4

Why anonymity and pseudonymity are important 4

Providing anonymous and pseudonymous options 5

Requiring identification — required or authorised by law 5

Requiring identification — impracticability 6

Key points

- APP 2 provides that individuals must have the option of dealing anonymously or by pseudonym with an APP entity.
- An APP entity is not required to provide those options where:
  - the entity is required or authorised by law or a court or tribunal order to deal with identified individuals, or
  - it is impracticable for the entity to deal with individuals who have not identified themselves
- Anonymity means that an individual dealing with an APP entity cannot be identified and the entity does not collect personal information or identifiers.
- A pseudonym is a name, term or descriptor that is different to an individual's actual name. Where applicable, an APP entity must ensure that individuals are made aware of their opportunity to deal anonymously or by pseudonym with the entity.

What does APP 2 say?

2.1 APP 2 provides that individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

2.2 That principle does not apply in relation to a particular matter if:

- the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves (APP 2.2(a)), or
- it is impracticable for the APP entity to deal with individuals who have not identified themselves or used a pseudonym (APP 2.2(b))

2.3 'Anonymity' and 'pseudonymity' are different concepts. APP 2 requires that both options be made available to individuals dealing with an APP entity unless one of the two exceptions applies. Both options must also be made available each time an individual interacts with the entity, that is, when a person is 'dealing with an APP entity in relation to a particular matter' (APP 2.1). Similarly, the exceptions ('required or authorised by law' and 'impracticability') apply to the particular dealing between an individual and the entity.

The difference between anonymity and pseudonymity

Anonymity

2.4 Anonymity requires that an individual may deal with an APP entity without providing any personal information or identifiers. The entity should not be able to identify the individual at the time of the dealing or subsequently.

2.5 Examples of anonymous dealings include an unidentified individual telephoning an APP entity to inquire generally about its goods or services, and an individual completing a retail transaction and paying for goods in cash.

Pseudonymity

2.6 Pseudonymity requires that an individual may deal with an APP entity by using a name, term or descriptor that is different to the person's actual name. Examples include an email address that does not contain the person's actual name, a user name that a person uses when participating in an online forum, or an artist who uses a 'pen-name' or 'screen-name'.

2.7 The use of a pseudonym does not necessarily mean that an individual cannot be identified. The individual may choose to divulge their identity, or to volunteer personal information necessary to implement a particular transaction, such as credit information or an address at which goods can be delivered. Similarly, an APP entity may have in place a registration system that enables a person to participate by pseudonym in a moderated online discussion forum, on condition that the person is identifiable to the forum moderator or the entity.

2.8 An APP entity should bear in mind that the object of APP 2 is to provide individuals with the opportunity to deal with the entity without revealing their identity. Personal information should only be linked to a pseudonym if this is required or authorised by law, it is impracticable for the entity to act differently, or the individual has consented to providing or linking the additional personal information. An entity could also restrict access to personal information that is linked to a pseudonym to authorised personnel (for a discussion of the security requirements for personal information, see Chapter 11 (APP 11)).

Why anonymity and pseudonymity are important

2.9 Anonymity and pseudonymity are important privacy concepts. They enable individuals to exercise greater control over their personal information and decide how much personal information will be shared or revealed to others.

2.10 An individual may prefer to deal anonymously or pseudonymously with an APP entity for various reasons, including:

- a preference not to be identified or to be 'left alone'
- to avoid subsequent contact such as direct marketing from that entity or other entities
- to keep their whereabouts secret from a former partner or family member
- to access services (such as counselling or health services) without this becoming known to others
- to express views in the public arena without being personally identified

2.11 There can be wider benefits too:

- Individuals may be more likely to inquire about products and services that an APP entity provides if able to do so without being identified, meaning the community is better informed.
- Freedom of expression is enhanced if individuals can express controversial or minority opinions without fear of reprisal.
- The risk of identity fraud is minimised when less personal information is collected, linked and stored by entities.

- An APP entity can lessen its compliance burden under the APPs by reducing the quantity of personal information it collects.
- Client feedback may be more forthcoming and robust if individuals have the option of making an unattributed compliment or complaint to an entity.

Providing anonymous and pseudonymous options

2.12 It is implicit in APP 2 that an APP entity should ensure that, if applicable, individuals are made aware of their opportunity to deal anonymously or by pseudonym with the entity. If anonymity or pseudonymity is the default setting, this does not apply.

2.13 The steps an APP entity should take to draw both options to the attention of individuals will depend on the nature of the dealing between the entity and an individual. For example, an entity's APP Privacy Policy could explain the circumstances in which an individual may deal anonymously or by pseudonym with the entity, and the procedures for doing so (see Chapter 1 (APP 1)). The policy could go further and explain how the entity manages pseudonyms and any linked personal information, and if there will be any consequences for an individual if they deal with the entity anonymously or through a pseudonym (for example, where only a limited service can be provided).

2.14 Other measures that could be adopted by an APP entity to facilitate anonymous and pseudonymous dealings include:

- if the entity provides a facility on its website for online communication, stating prominently that an individual may use that facility without providing personal information
- if telephone calls to the entity are routed through an automated message, informing callers in that message that they are not required to provide personal information
- if individuals can contact the entity by using an online or printed form, stating on the form that personal identification boxes (such as name and address) are not mandatory fields
- if the entity solicits public submissions or comments from individuals, allowing participants to use a pseudonym that will be published, even if the individual's name is supplied confidentially to the entity
- in other dealings between the entity and individuals, informing individuals at the beginning of a dealing that they may interact anonymously or by pseudonym

Requiring identification — required or authorised by law

2.15 APP 2.2(a) provides that an individual may not have the option of dealing anonymously or by pseudonym with an APP entity if the entity 'is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves'. The meaning of 'required or authorised by or under an Australian law or court/tribunal order' is discussed in Chapter B (Key concepts).

2.16 If an APP entity is 'required' by a law or order to deal only with an identified individual it will be necessary for the individual to provide adequate identification. If an entity is 'authorised' by a law or order to deal with an identified individual, the entity can require the individual to identify themselves, but equally will have discretion to allow the individual to deal with the entity anonymously or pseudonymously. The nature of any discretion, and whether it is appropriate to rely upon it, will depend on the terms of the law or order and the nature of the dealing.

2.17 The following are given as examples of where a law or order may require or authorise an APP entity to deal only with an identified individual:

- Processing an individual's application for an identity document (such as a passport, licence or security pass).
- Issuing a tax file number to an individual.
- Paying a social security or healthcare benefit to an eligible individual.
- Providing assistance to an individual who has been diagnosed with a disease that must be recorded and notified under a public health law.
- Providing assistance to a suspected victim of child abuse, whose injury is covered by a mandatory reporting requirement.
- Opening a bank account for an individual, or providing other financial services where legislation requires the individual to be identified.
- Supplying a pre-paid mobile phone to an individual where legislation requires identification.
- Discussing the individual's personal information with them, such as the individual's account information.
- Giving access to the individual's personal information under the Privacy Act or Freedom of Information Act 1982.[1]

2.18 An APP entity that relies on APP 2.2(a) to collect personal information should ensure that the collection does not go beyond the requirements of the law or court or tribunal order. For example, the legal requirement may be satisfied by sighting, but not collecting, the personal information, or by collecting an individual's name but not their address, gender or date of birth. APP 3 imposes a complementary requirement, that generally an entity can only collect personal information that is reasonably necessary for one or more of its functions or activities.

Requiring identification — impracticability

2.19 APP 2.2(b) provides that an individual may not have the option of dealing anonymously or by pseudonym with an APP entity if 'it is impracticable for the APP entity to deal with individuals who have not identified themselves'.

2.20 The following are given as examples of where it may be impracticable to deal with an individual who is not identified:

[1] It may be practicable to deal with a pseudonymous request for personal information under the Privacy Act or the Freedom of Information Act 1982 if the individual has previously transacted under that pseudonym and can establish their identity as that individual (see APP 12, Chapter 12).

- In dispute resolution, it may be impracticable to investigate and resolve an individual's particular complaint about how their case was handled or how the staff of an APP entity behaved unless the complainant provides their name or similar information.
- Where an entity is delivering purchased goods to an individual, it may not be able to do so without knowing that individual's address, or their name (for example, where the individual needs to sign for delivery of the goods).

2.21 In special circumstances it may be open to an APP entity to rely on the 'impracticability' exception where the burden of the inconvenience, time and cost of dealing with an unidentified or pseudonymous individual, or of changing an existing system or practice to include the option of anonymous or pseudonymous dealings, would be excessive in all the circumstances. However, this is more likely to be a transitional rather than an ongoing justification. Unless an entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves (see paragraphs 2.15–2.18 above), entities are expected to design and maintain information collection systems that incorporate anonymous and pseudonymous options.

2.22 An APP entity that is relying on APP 2.2(b) should not collect more personal information than is required to facilitate the dealing with an individual (see paragraph 2.18 above).

Chapter 3:

Australian Privacy Principle 3 —

Collection of solicited personal information

Version 1.1, July 2019

OAIC

Contents

Key points 3
What does APP 3 say? 3
'Solicit' and 'collect' 4
Collecting for an APP entity's 'functions or activities' 5
Identifying the functions or activities of an agency 5
Identifying the functions or activities of an organisation 5
Collecting personal information that is 'directly related' to an agency's functions or activities 6
Collecting personal information that is 'reasonably necessary' for an APP entity's functions or activities 6
Collecting sensitive information 7
Collecting sensitive information as required or authorised by law 8
Collecting sensitive information where a permitted general situation exists 8
Collecting sensitive information where a permitted health situation exists 10
Collecting sensitive information for an enforcement related activity 11
Collection of sensitive information by a non-profit organisation 12
Collecting by lawful and fair means 13
Collecting by lawful means 13
Collecting by fair means 14
Collecting directly from the individual 14
Unreasonable or impracticable to collect directly from the individual 14
Consent by the individual — for agencies only 15
Required or authorised by law or a court or tribunal order — for agencies only 15
Collecting personal information from a related body corporate 15

Key points

- APP 3 outlines when an APP entity may collect solicited personal information.
- An APP entity solicits personal information if it explicitly requests another entity to provide personal information, or it takes active steps to collect personal information.
- APP 3 deals with when an APP entity can collect personal information, and how an APP entity must collect personal information.
- For personal information (other than sensitive information), an APP entity that is:
  - an agency, may only collect this information where it is reasonably necessary for, or directly related to, the agency's functions or activities
  - an organisation, may only collect this information where it is reasonably necessary for the organisation's functions or activities
- APP 3 contains different requirements for the collection of sensitive information compared to other types of personal information. Unless an exception applies, an APP entity may only collect sensitive information where the above conditions are met and the individual concerned consents to the collection.
- Personal information must only be collected by lawful and fair means.
- Personal information must be collected from the individual concerned, unless this is unreasonable or impracticable (additional exceptions apply to agencies).

What does APP 3 say?

3.1 The APPs distinguish between an APP entity collecting solicited personal information (APP 3) and receiving unsolicited personal information (APP 4).

3.2 APP 3 deals with two aspects of collecting solicited personal information:

- when an APP entity can collect personal information — the requirements vary according to whether the personal information is or is not sensitive information, and whether the APP entity is an agency or an organisation
- how an APP entity must collect personal information — the same requirements apply to all APP entities and to all kinds of personal information

3.3 In summary, the principles that apply are:

- an agency may only solicit and collect personal information that is reasonably necessary for, or directly related to, one or more of its functions or activities (APP 3.1)
- an organisation may only solicit and collect personal information that is reasonably necessary for one or more of its functions or activities (APP 3.2)
- in addition to the above requirements, an APP entity may only solicit and collect sensitive information if the individual consents to the sensitive information being collected, unless an exception applies (APP 3.3)
- an APP entity must solicit and collect personal information:
  - only by lawful and fair means (APP 3.5), and
  - directly from the individual, unless an exception applies (APP 3.6)

‘Solicit’ and ‘collect’

3.4 APP 3 applies when an APP entity ‘solicits’ and ‘collects’ personal information, while APP 4 applies when an APP entity receives personal information that it ‘did not solicit’. Examples of solicited personal information collected by an entity are given in paragraph 3.7 below; examples of unsolicited personal information received by an entity are given in Chapter 4 (APP 4).

3.5 An APP entity ‘collects’ personal information ‘only if the entity collects the personal information for inclusion in a record or generally available publication’ (s 6(1)). This concept applies broadly, and includes gathering, acquiring or obtaining personal information from any source and by any means. In practice, all personal information that is held by an entity will generally be treated as information that was collected by the entity. ‘Collect’ is discussed in more detail in Chapter B (Key concepts).

3.6 An APP entity ‘solicits’ personal information ‘if the entity requests another entity to provide the personal information, or to provide a kind of information in which that personal information is included’ (s 6(1)). The request may be made to an agency, organisation, individual or a small business operator.[1] A ‘request’ is an active step taken by an entity to collect personal information, and may not involve direct communication between the entity and an individual.

3.7 Examples of solicited personal information collected by an APP entity include the following, where they are collected for inclusion in a record or generally available publication:

- personal information provided by an individual in response to a request, direction or order
- personal information about an individual provided by another entity in response to a request, direction, order or arrangement for sharing or transferring information between both entities
- personal information provided at a business meeting, where it relates to the subject matter of the meeting, including business cards exchanged at the meeting
- a completed form or application submitted by an individual
- a complaint letter sent in response to a general invitation on an APP entity’s website to individuals to complain to the entity
- an employment application sent in response to either a job advertisement published by an entity or an expression of interest register maintained by the entity
- a form completed to enter a competition being conducted by an entity
- personal information provided to a ‘fraud hotline’ that is designed to capture ‘tip-offs’ from the public
- an entry in an APP entity’s visitors book
- a record of a credit card payment
- CCTV footage that identifies individuals

[1] An ‘entity’ is defined in s 6(1) to mean an agency, organisation or small business operator. ‘Organisation’ is defined in s 6C to include an individual.

Collecting for an APP entity's 'functions or activities'

3.8 An APP entity must only collect personal information which is reasonably necessary for one or more of the entity's functions or activities (APPs 3.1 and 3.2).[2] Agencies may, in addition, collect personal information that is directly related to one or more of the agency's functions or activities.

3.9 Determining whether a particular collection of personal information is permitted involves a two-step process:

- identifying an APP entity's functions or activities — different criteria apply for ascertaining the functions and activities of agencies and organisations
- determining whether the particular collection of personal information is reasonably necessary for (or, for agencies, directly related to) one of those functions or activities

Identifying the functions or activities of an agency

3.10 An agency's functions will be conferred either by legislation (including a subordinate legislative instrument) or an executive scheme or arrangement established by government. Identifying an agency's functions involves examining the legal instruments that confer or describe the agency's functions. These include:

- Acts and subordinate legislative instruments
- the Administrative Arrangements Order made by the Governor-General
- government decisions or ministerial statements that announce a new government function[3]

3.11 The activities of an agency will be related to its functions. The activities of an agency include incidental and support activities, such as human resource, corporate administration, property management and public relations activities.

3.12 One resource that describes an agency's functions is that agency's Information Publication Scheme (IPS) entry.[4] Agencies to which the Freedom of Information Act 1982 (FOI Act) applies are required to publish on a website 'details of the functions of the agency'. This forms part of the IPS established by the FOI Act (FOI Act, ss 8(2)(c), 8D(3)). The IPS entries of most agencies are readily accessible through a link on the homepage of the agency's website. Another resource that describes agency functions and activities is the annual report of an agency, usually accessible from the agency's website.

Identifying the functions or activities of an organisation

3.13 An organisation's functions or activities include:

---

[2] See Chapter 9 (APP 9) for a discussion of particular issues relating to the lawful collection of government related identifiers by organisations.

[3] The source and scope of government functions are discussed at greater length in OAIC, FOI Guidelines at [13.38]–[13.49], OAIC website <https://www.oaic.gov.au>.

[4] An agency's incidental functions (described in paragraph 3.11) are not required to be published in its IPS entry: see OAIC, FOI Guidelines at [13.47]–[13.49], OAIC website <https://www.oaic.gov.au>.

- current functions or activities of the organisation
- proposed functions or activities the organisation has decided to carry out and for which it has established plans
- activities the organisation carries out in support of its other functions and activities, such as human resource, corporate administration, property management and public relations activities

3.14 The functions and activities of an organisation will commonly be described (though not necessarily exhaustively) on a website, in an annual report, and in corporate brochures, advertising, product disclosure statements and client and customer letters and emails.

3.15 The functions and activities of an organisation (for which it may collect personal information under APP 3) are limited to those in which it may lawfully engage.

Collecting personal information that is 'directly related' to an agency's functions or activities

3.16 An agency may collect personal information that is 'directly related to' one or more of the agency's functions or activities (APP 3.1). To be 'directly related to', a clear and direct connection must exist between the personal information being collected and an agency function or activity.

Collecting personal information that is 'reasonably necessary' for an APP entity's functions or activities

3.17 An APP entity may collect personal information that is 'reasonably necessary for' a function or activity of the entity (APP 3.1 and APP 3.2).[5]

3.18 The 'reasonably necessary' test is an objective test: whether a reasonable person who is properly informed would agree that the collection is necessary. It is the responsibility of an APP entity to be able to justify that the particular collection is reasonably necessary. 'Reasonably necessary' is also discussed in Chapter B (Key concepts).

3.19 Factors relevant to determining whether a collection of personal information is reasonably necessary for a function or activity include:

- the primary purpose of collection ('purpose' is discussed further in Chapter B (Key concepts)
- how the personal information will be used in undertaking a function or activity of the APP entity (for example, in most circumstances collection on the basis that personal information could become necessary for a function or activity in the future, would not be reasonably necessary)
- whether the entity could undertake the function or activity without collecting that personal information, or by collecting a lesser amount of personal information

3.20 The following are instances in which the OAIC has previously ruled that a collection of personal information was not reasonably necessary for an entity's function or activity:

[5] An APP entity may also collect the personal information of an individual (other than sensitive information) from a related body corporate (s 13B(1)(a)).

- a job applicant being asked to advise if they had suffered a work-related injury or illness, when this was not relevant to the position being advertised[6]
- a person applying to open a bank account being asked to complete a standard form application that included a question about marital status, when this had no bearing on the applicant's eligibility to open an account[7]
- a medical practitioner photographing a patient for the patient's medical file, when this was not necessary to provide a health service[8]

3.21 Other examples of personal information collection that may not be reasonably necessary for an APP entity's functions or activities include:

- collecting personal information about a group of individuals, when information is only required for some of those individuals
- collecting more personal information than is required for a function or activity. For example, collecting all information entered on an individual's driver licence when the purpose is to establish if the individual is aged 18 years or over
- collecting personal information that is not required for a function or activity but is being entered in a database in case it might be needed in the future (this is to be distinguished from the situation where personal information is required for a function or activity, but is not being used immediately)
- an organisation collecting personal information for or on behalf of a related body corporate where the collection of that personal information is not reasonably necessary for the organisation's own functions or activities

Collecting sensitive information

3.22 APP 3.3 imposes an additional requirement for collecting sensitive information about an individual. Unless an exception applies, an APP entity must:

- satisfy the criteria above, i.e. the collection of the sensitive information must be reasonably necessary for (or, for agencies, directly related to) one or more of the entity's functions or activities, and
- the individual about whom the sensitive information relates must consent to the collection (APP 3.3(a))

3.23 'Sensitive information' is defined in s 6(1), and is discussed in more detail in Chapter B (Key concepts). '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 individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific, and

[6] Own Motion Investigation v Australian Government Agency [2007] PrivCmrA 4, Australasian Legal Information Institute website <www.austlii.edu.au>.

[7] D v Banking Institution [2006] PrivCmrA 4, Australasian Legal Information Institute website <www.austlii.edu.au>.

[8] M v Health Service Provider [2007] PrivCmrA 15, Australasian Legal Information Institute website <www.austlii.edu.au>.

- the individual has the capacity to understand and communicate their consent

3.24 APP 3.4 lists five exceptions to the requirements of APP 3.3(a). These are considered below.

Collecting sensitive information as required or authorised by law

3.25 An APP entity may collect sensitive information if the collection 'is required or authorised by or under an Australian law or a court/tribunal order' (APP 3.4(a)). The meaning of 'required or authorised by or under an Australian law or a court/tribunal order' is discussed in more detail in Chapter B (Key concepts).

3.26 An example of where a law or order may require or authorise collection of sensitive information is the collection by an authorised officer under the Migration Act 1958 of personal identifiers (that may include biometric information) from a non-citizen who is in immigration detention.[9]

Collecting sensitive information where a permitted general situation exists

3.27 An APP entity may collect sensitive information if a 'permitted general situation' exists in relation to the collection (APP 3.4(b)).

3.28 Section 16A lists seven permitted general situations (two of which apply only to agencies). The seven situations are set out below, and are discussed in Chapter C (Permitted general situations), including the meaning of relevant terms.

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

3.29 An APP entity may collect sensitive information if:

- it is unreasonable or impracticable to obtain the individual's consent to the collection, and
- the entity reasonably believes 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 (s 16A(1), Item 1)

3.30 Examples of where this permitted general situation might apply are:

- collecting health information about an individual who is seriously injured, requires treatment and, due to their injuries, cannot give informed consent, on the basis that it is impracticable to obtain the individual's consent
- collecting sensitive information about a parent that is required to provide assistance to a child who may be at risk of physical or sexual abuse by the parent, on the basis that it would be unreasonable to obtain the parent's consent

[9] See Migration Act 1958, ss 5A, 261AA.

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

3.31 An APP entity may collect sensitive 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
- reasonably believes that the collection is necessary in order for the entity to take appropriate action in relation to the matter (s 16A(1), Item 2)

3.32 Examples of where this permitted general situation might apply are the collection of sensitive information by:

- an APP entity that is investigating fraudulent conduct by a professional adviser or a client in relation to the entity's functions or activities
- an agency that is investigating a suspected serious breach by a staff member of the Australian Public Service Code of Conduct

Locating a person reported as missing

3.33 An APP entity may collect sensitive information if:

- 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, and
- the collection complies with rules made by the Information Commissioner under s 16A(2) (s 16A(1), Item 3)

Reasonably necessary for establishing, exercising or defending a legal or equitable claim

3.34 An APP entity may collect sensitive information if the collection is reasonably necessary to establish, exercise or defend a legal or equitable claim (s 16A(1), Item 4).

3.35 An example of where this permitted general situation might apply is an insurer collecting health information about an individual who has made an insurance compensation claim but is suspected of misrepresenting their claim or the extent of their injuries.[10]

Reasonably necessary for a confidential alternative dispute resolution process

3.36 An APP entity may collect sensitive information if the collection is reasonably necessary for the purposes of a confidential alternative dispute resolution (ADR) process (s 16A(1), Item 5).

3.37 An example of where this permitted general situation might apply is an alternative dispute resolution practitioner making a record of a party recounting their version of events, where that account includes the disclosure of sensitive information about an individual who is directly or indirectly involved in the dispute. This permitted general situation will only apply

[10] N and Law Firm [2011] AICmrCN 8, Australasian Legal Information Institute website <www.austlii.edu.au>. See also B v Law Firm [2011] PrivCmrA 2 (3 May 2011), viewed 6 March 2013, Australasian Legal Information Institute website <www.austlii.edu.au>.

where the parties to the dispute and the ADR provider are bound by confidentiality obligations.

Necessary for a diplomatic or consular function or activity

3.38 An agency may collect sensitive information if the agency reasonably believes the collection is necessary for the agency's diplomatic or consular functions or activities (s 16A(1), Item 6). This permitted general situation applies only to agencies, and not to organisations.

3.39 An example of where this permitted general situation might apply is where an agency with diplomatic or consular functions collects sensitive information about an individual who is overseas and in need of consular assistance because the individual has been hospitalised, is suffering a psychiatric illness, has been arrested or is missing.

Necessary for certain Defence Force activities outside Australia

3.40 The Defence Force (as defined in s 6(1)) may collect sensitive information if it reasonably believes the collection to be 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).

Collecting sensitive information where a permitted health situation exists

3.41 An organisation may collect sensitive information if a 'permitted health situation' exists in relation to the collection (APP 3.4(c)). This exception applies only to organisations, and not to agencies.

3.42 Section 16B lists two permitted health situations that relate to the collection of health information by an organisation. The two situations are set out below, and are discussed in Chapter D (Permitted health situations), including the meaning of relevant terms.

Providing a health service

3.43 An organisation may collect health information about an individual if the health information is necessary to provide a health service to the individual, and either:

- the collection is required or authorised by or under an Australian law (other than the Privacy Act), or
- the health information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation (s 16B(1))

3.44 An example of where this permitted health situation might apply is where a participant in the My Health Record system collects health information included in a consumer's My Health Record as authorised by the My Health Records Act 2012.[11]

3.45 'Health information' is defined in s 6(1) and discussed in more detail in Chapter B (Key concepts).

[11] See My Health Records Act 2012, ss 63, 64, 65, 66 and 68.

Conducting research; compiling or analysing statistics; management, funding or monitoring of a health service

3.46 An organisation may collect health information about an individual if the collection is necessary for research relevant to public health or public safety, the compilation or analysis of statistics relevant to public health or public safety, or the management, funding or monitoring of a health service, and:

- the particular purpose cannot be served by collecting de-identified information
- it is impracticable to obtain the individual's consent, and
- the collection is either:
  - required by or under an Australian law (other than the Privacy Act)
  - in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation, or
  - in accordance with guidelines approved under s 95A (s 16B(2))[12]

3.47 An example of where this permitted health situation might apply is an organisation conducting longitudinal research into heart disease and requiring health information about a large number of individuals from different data sources for research linkage. In this case, the collection must be required by an Australian law or carried out in accordance with the rules or guidelines referred to in s 16B(2).

3.48 'Health information' is defined in s 6(1) and discussed in more detail in Chapter B (Key concepts).

Collecting sensitive information for an enforcement related activity

3.49 An enforcement body may collect sensitive information where:

- if the body is the Immigration Department[13], the Department reasonably believes that collecting the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the Department (APP 3.4(d)(i))
- for other enforcement bodies, the body reasonably believes that collecting the information is reasonably necessary for, or directly related to, one or more of the body's functions or activities (APP 3.4(d)(ii))

3.50 'Enforcement body' is defined in s 6(1) as a list of specific bodies and is discussed in Chapter B (Key concepts). 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,[14] the

[12] See National Health and Medical Research Council (NHMRC), Guidelines Approved Under Section 95A of the Privacy Act 1988, NHMRC website <https://www.nhmrc.gov.au>.

[13] 'Immigration Department' is defined in s 6(1) as the Department administered by the Minister administering the Migration Act 1958 and is discussed in Chapter B (Key concepts). This is now the Department of Home Affairs.

[14] In July 2016, the former Australian Crime Commission and CrimTrac were merged to form the Australian Criminal Intelligence Commission.

Integrity Commissioner,[15] the Immigration Department, Australian Prudential Regulation Authority, Australian Securities and Investments Commission and AUSTRAC.

3.51 For an enforcement body to collect sensitive information using this exception, it must:

- for the Immigration Department, identify the 'enforcement related activities' it conducts or that are conducted on its behalf, and for other enforcement bodies, identify their 'functions or activities', and
- 'reasonably believe' that the collection is either 'reasonably necessary for' or 'directly related to' one or more of those functions or activities

3.52 'Reasonably believes' is discussed in more detail in Chapter B (Key concepts). Identifying the 'functions or activities' of an agency is discussed above at paragraphs 3.10–3.12, while 'reasonable necessary for' and 'directly related to' are discussed above at paragraphs 3.16–3.21.

3.53 'Enforcement related activities' are defined in s 6(1) and discussed in Chapter B (Key concepts). Where applied to the Immigration Department, the activities could include assessing and enforcing compliance with visa and citizenship requirements, and detecting, preventing, investigating and prosecuting breaches of visa, immigration and citizenship laws. Non-enforcement related activities of the Department do not fall within this exception.[16]

3.54 An example of where the Immigration Department may collect sensitive information from an individual using this exception is where it reasonably believes that the sensitive information directly relates to the function of investigating whether a person has breached an immigration law.

Collection of sensitive information by a non-profit organisation

3.55 A non-profit organisation may collect sensitive information if:

- the information relates to the activities of the organisation, and
- the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities (APP 3.4(e)).

3.56 'Non-profit organisation' is defined in s 6(1) as an organisation 'that is a non-profit organisation; and that engages in activities for cultural, recreational, political, religious, philosophical, professional, trade or trade union purposes'. The term 'cultural purposes' includes both racial and ethnic purposes.

3.57 There are three criteria a non-profit organisation must meet to rely on this exception to collect sensitive information:

- Firstly, the non-profit organisation can rely on this exception only when collecting sensitive information for an activity that is undertaken for one of the specified purposes in the definition of 'non-profit organisation' (s 6(1)). An organisation conducting activities

[15] 'Integrity Commissioner' is defined in s 6(1) as having the same meaning as in the Law Enforcement Integrity Commissioner Act 2006.

[16] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 76.

for some other purpose cannot rely on this exception to collect sensitive information for that purpose.

- Secondly, the sensitive information that is collected must 'relate' to the activity that is being conducted for a specified purpose. A clear relationship, assessed objectively, must exist between the information collected and that activity. For example, the information may relate to a fundraising activity undertaken by a non-profit organisation to support its cultural, recreational, political, religious, philosophical, professional, trade or trade union purpose.
- Thirdly, the sensitive information must relate solely to a member of the organisation, or an individual who has regular contact with the organisation in connection with its activities. Collection of sensitive information about a relative of a member of the organisation would not be covered unless the relative was also a member or person in regular contact with the non-profit organisation.

3.58 An example of where a non-profit organisation may be permitted to collect sensitive information is where a religious organisation collects information about the views of its members on religious or moral issues.

Collecting by lawful and fair means

3.59 An APP entity must collect personal information 'only by lawful and fair means' (APP 3.5). This requirement applies to all APP entities.

Collecting by lawful means

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

3.61 Examples of collection that would not be lawful include:

- collecting in breach of legislation, for example:
  - collecting via computer hacking[17]
  - collecting using telephone interception or a listening device except under the authority of a warrant[18]
  - requesting or requiring information in connection with, or for the purpose of, an act of discrimination[19]
- collecting by a means that would constitute a civil wrong, for example, by trespassing on private property or threatening damage to a person unless information is provided
- collecting information contrary to a court or tribunal order, for example, contrary to an injunction issued against the collector

[17] For example, Criminal Code Act 1995, Part 10.7.

[18] For example, Telecommunications (Interception) Act 1979 (Cth) s 7; Surveillance Devices Act 2004 (Cth) s 14.

[19] See for example, the Disability Discrimination Act 1992, s 30 and the Sex Discrimination Act 1984, s 27.

Collecting by fair means

3.62 A 'fair means' of collecting information is one that does not involve intimidation or deception, and is not unreasonably intrusive.[20] Whether a collection uses unfair means will depend on the circumstances. For example, it would usually be unfair to collect personal information covertly without the knowledge of the individual. However, this may be a fair means of collection if undertaken in connection with a fraud investigation.

3.63 The following are given as examples of where a collection of personal information may be unfair (some may also be unlawful):

- collecting from a file dumped by accident on a street, or from an electronic device which is lost or left unattended
- collecting from an individual who is traumatised, in a state of shock or intoxicated
- collecting in a way that disrespects cultural differences
- misrepresenting the purpose or effect of collection, or the consequences for the individual of not providing the requested information
- collecting by telephoning an individual in the middle of the night
- collecting by deception, for example, wrongly claiming to be a police officer, doctor or trusted organisation

Collecting directly from the individual

3.64 APP 3.6 provides that an APP entity 'must collect personal information about an individual only from the individual', unless one of the following exceptions apply:

- for all APP entities, it is unreasonable or impracticable for the entity to collect personal information only from the individual
- for agencies, the individual consents to the personal information being collected from someone other than the individual
- for agencies, the agency is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual

Unreasonable or impracticable to collect directly from the individual

3.65 Whether it is 'unreasonable or impracticable' to collect personal information only from the individual concerned will depend on the circumstances of the particular case. Considerations that may be relevant include:

- whether the individual would reasonably expect personal information about them to be collected directly from them or from another source
- the sensitivity of the personal information being collected

[20] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 77.

- whether direct collection would jeopardise the purpose of collection or the integrity of the personal information collected
- any privacy risk if the information is collected from another source
- the time and cost involved of collecting directly from the individual. However, an APP entity is not excused from collecting from the individual rather than another source by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable or impracticable will depend on whether the burden is excessive in all the circumstances.

3.66 The following are given as examples of when it may be unreasonable or impracticable to collect personal information only from the individual concerned:

- collection by a law enforcement agency of personal information about an individual who is under investigation, where the collection may jeopardise the investigation if the personal information is collected only from that individual[21]
- if a legal or official document that is mailed to an individual is returned to the sender, the individual's current contact details may need to be obtained from another source

Consent by the individual — for agencies only

3.67 The term 'consent' is discussed at paragraph 3.23 above and in Chapter B (Key concepts). As noted in those sections, consent can be express or implied, and must be voluntary, informed, current and specific, and the individual must have capacity to consent.

3.68 An example of where an agency might collect personal information from someone other than the individual is where an individual consents to one agency disclosing their personal information (such as contact details) to the other agency.

Required or authorised by law or a court or tribunal order — for agencies only

3.69 The meaning of 'required or authorised by or under an Australian law or a court/tribunal order' is discussed in Chapter B (Key concepts). It is a common feature of legislation that an agency, for the purpose of performing a function or exercising a power, is authorised to require a person or body to provide personal information.

3.70 An example of where collection by an agency from someone other than the individual concerned might be required or authorised by law is s 44 of the Privacy Act, which provides that the Information Commissioner may issue a notice to a person requiring them to provide specified information for the purpose of an investigation under the Act (and that information may include personal information).

Collecting personal information from a related body corporate

3.71 Section 13B(1)(a) provides that the collection of personal information about an individual (other than sensitive information) by a body corporate from a related body corporate is

[21] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 77.

generally not 'an interference with the privacy of an individual' (interferences with privacy are discussed in Chapter A (Introductory matters)). This provision applies to collection of information from related bodies corporate and not to other corporate relationships such as a franchise or joint-venture relationship.[22]

3.72 The effect of s 13B(1)(a) is that an APP entity may collect personal information (other than sensitive information) from a related body corporate without satisfying the requirements of APP 3.1 or 3.2 (see paragraphs 3.8–3.21 above). However, s 13B(1A) sets out some exceptions to this, including where the related body corporate is not an organisation.

[22] Section 6(8) states 'for the purposes of this Act, the question of whether bodies corporate are related to each other is determined in the manner in which that question is determined under the Corporations Act 2001'.

Chapter 4:

Australian Privacy Principle 4 —

Dealing with unsolicited personal information

Version 1.1, July 2019

OAIC

Contents

Key points 3

What does APP 4 say? 3

'Unsolicited' personal information 4

Determining whether unsolicited personal information could have been collected under APP 3 5

Dealing with unsolicited personal information that could not have been collected under APP 3 5

- Unsolicited personal information received by an agency 5
- Unsolicited personal information received by an organisation 6

Dealing with unsolicited personal information that could have been collected under APP 3, or is not destroyed or de-identified 7

Key points

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

What does APP 4 say?

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

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

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

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

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

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

'Unsolicited' personal information

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Unsolicited personal information received by an agency

4.15 The term 'Commonwealth record' in s 6(1) has the same meaning as in s 3 of the Archives Act 1983 (the Archives Act) and is discussed in more detail in Chapter B (Key concepts).[1] The

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

term is likely to include all or most personal information received by agencies. It may also include personal information received by contracted service providers.

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

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

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

Unsolicited personal information received by an organisation

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

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

Destruction or de-identification that is 'lawful'

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

4.22 Examples of where destruction may not be lawful include:

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

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

Destruction or de-identification that is 'reasonable'

4.24 Whether destruction or de-identification is reasonable is a question of fact in each individual case. It is an objective standard that has regard to how a reasonable person, who is properly

informed, would be expected to act in the circumstances. It is the responsibility of the organisation to be able to justify that its conduct was reasonable.

4.25 Relevant considerations may include:

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

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

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

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

4.28 An APP entity may retain unsolicited personal information if the entity has determined that it could have collected the personal information under APP 3, or the personal information is contained in a Commonwealth record, or the entity is not required to destroy or de-identify the personal information under APP 4.3 because it would be unlawful or unreasonable to do so. The personal information must then be dealt with in accordance with APPs 5–13 (APP 4.4). This means, for example, that a notice of collection may be required (see Chapter 5

(APP 5)), the personal information may only be used or disclosed for the primary purpose for which it was collected unless an exception applies (see paragraph 4.29 below and Chapter 6 (APP 6)), the security of the personal information must be protected (see Chapter 11 (APP 11)), an individual can request access to the personal information (see Chapter 12 (APP 12)) and an individual can request the entity to correct the personal information (see Chapter 13 (APP 13)).

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

4.30 Secondly, APP 11.2 requires an APP entity to destroy or de-identify personal information it holds but which it no longer needs for any purpose permitted by the APPs, unless the personal information is contained in a Commonwealth record or the entity is required by or under an Australian law, or a court/tribunal order, to retain the information. Consequently, personal information that is retained under APP 4.4 may nevertheless need to be destroyed or de-identified in accordance with APP 11.2 (see Chapter 11 (APP 11)).

Chapter 5:

Australian Privacy Principle 5 —

Notification of the collection of personal information

Version 1.2, July 2019

OAIC

Contents

Key points 3

What does APP 5 say? 3

Taking reasonable steps to notify or ensure awareness 3

When not taking any steps might be reasonable 5

Matters about which an individual must be notified or made aware 6

The APP entity's identity and contact details 6
The facts and circumstances of collection 6
If the collection is required or authorised by law 7
The purposes of collection 7
The consequences for the individual if personal information is not collected 7
Other APP entities, bodies or persons to which the personal information is usually disclosed 8
Information about access and correction in the APP entity's APP Privacy Policy 8
Likely cross-border disclosures of the personal information 8

When notification is to occur 9

Key points

- An APP entity that collects personal information about an individual must take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters.
- The matters include:
  - the APP entity's identity and contact details
  - the fact and circumstances of collection
  - whether the collection is required or authorised by law
  - the purposes of collection
  - the consequences if personal information is not collected
  - the entity's usual disclosures of personal information of the kind collected by the entity
  - information about the entity's APP Privacy Policy
  - whether the entity is likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located
- An APP entity must take reasonable steps, before, or at the time it collects personal information. If this is not practicable, reasonable steps must be taken as soon as practicable after collection.

What does APP 5 say?

5.1 APP 5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters (generally referred to in this chapter as 'APP 5 matters'). The term 'collects' is discussed in Chapter B (Key concepts). Reasonable steps must be taken at or before the time of collection, or as soon as practicable afterwards.

5.2 The requirement to notify or ensure awareness of the APP 5 matters applies to all personal information 'collected' about an individual, either directly from the individual or from a third party. It applies to solicited personal information (APP 3) and also unsolicited personal information that is not destroyed or de-identified by the APP entity (APP 4) (see Chapter 3 (APP 3), Chapter 4 (APP 4) and Chapter B (Key concepts)).

Taking reasonable steps to notify or ensure awareness

5.3 An APP entity must take reasonable steps either to notify an individual of the APP 5 matters or to ensure the individual is aware of those matters (APP 5.1).

5.4 The reasonable steps for an APP entity will depend upon circumstances that include:

- the sensitivity of the personal information collected. More rigorous steps may be required when collecting 'sensitive information' (defined in s 6(1) and discussed in Chapter B (Key concepts)) or information of a sensitive nature

- the possible adverse consequences for an individual as a result of the collection. More rigorous steps may be required as the risk of adversity increases
- any special needs of the individual. More rigorous steps may be required if personal information is collected from an individual from a non-English speaking background who may not readily understand the APP 5 matters
- the practicability, including time and cost involved. However, an entity is not excused from taking particular steps 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.

5.5 An individual may be notified or made aware of APP 5 matters through a variety of formats, provided the matters are expressed clearly. A notice may be prepared in advance (paper, online, telephone script) and staff should be trained to understand their obligation to take reasonable steps to notify or ensure awareness under APP 5. A notice may also be provided in layers, from a full explanation to a brief refresher as individuals become more familiar with how the APP entity operates and how personal information is handled. Brief privacy notices on forms or signs may be supplemented by longer notices made available online or in brochures.

5.6 Examples of reasonable steps that an APP entity could consider taking to notify or ensure awareness of the APP 5 matters include:

- if the entity collects personal information directly from an individual who completes a form or uses an online facility, clearly and prominently displaying the APP 5 matters in the form, or providing a readily accessible and prominent link to an APP 5 notice
- if personal information is collected by telephone, explaining the APP 5 matters to the individual at the commencement of the call (perhaps following a template script or using an automated message). Where this is not practicable, an entity should give the individual information about the APP 5 matters as soon as possible afterwards, such as in any subsequent electronic or paper-based communication, or directing the individual to the relevant notice on the entity's website
- if the entity collects personal information from another entity, ensuring that the other entity has notified or made the individual aware of the relevant APP 5 matters on its behalf (such as through an enforceable contractual arrangement)
- where it is not reasonable to notify or ensure awareness of the full range of APP 5 matters, an entity could alert the individual to specific sections of its APP Privacy Policy (see Chapter 1 (APP 1)), such as parts of the Policy about likely overseas disclosures (APP 5.2(i)), or other general documents containing relevant information.[1] However, before doing so the entity should consider whether information in the APP Privacy Policy sufficiently covers the APP 5 matters as they relate to the particular collection, as the APP Privacy Policy may describe only the general information handling practices of the entity.

[1] See Tenants' Union of Queensland Inc, Tenants' Union of NSW Co-op Ltd v TICA Default Tenancy Control Pty Ltd [2004] PrivCmrACD 4 (16 April 2004) [80], [82], which states 'if an organisation provides the information required to meet its obligations on different forms or in different locations it would generally need to alert individuals to the fact the other information was available…it should [also] seek to ensure that there are appropriate references to that information in the primary form'.

When not taking any steps might be reasonable

5.7 APP 5.1 acknowledges that it may be reasonable for an APP entity to not take any steps to provide a notice or ensure awareness of all or some of the APP 5 matters. It is the responsibility of the entity to be able to justify not taking any steps. The following are given as examples of when this may be reasonable:

- The individual is aware that personal information is being collected, the purpose of collection and other APP 5 matters relating to the collection, for example, a doctor has informed a patient that a specialist to whom the patient is referred for treatment will obtain the patient's health information from the doctor.
- An entity collects personal information from an individual on a recurring basis in relation to the same matter. However, if a long period of time has elapsed since the notice was provided and the individual may no longer be aware of the APP 5 matters, the entity may need to take steps to notify or ensure awareness. Similarly, if a change in circumstances as to how personal information is collected affects any of the APP 5 matters, the entity should take reasonable steps to ensure an individual is aware of those matters.
- Notification may pose a serious threat to the life, health or safety of an individual or pose a threat to public health or safety, for example, a law enforcement agency obtaining personal information from a confidential source for the purpose of an investigation.
- Notification may jeopardise the purpose of collection or the integrity of the personal information collected and there is a clear public interest in the purpose of collection, for example, a law enforcement agency undertaking lawful covert surveillance of an individual in connection with a criminal investigation.
- Notification would be inconsistent with another legal obligation, for example, by breaching a statutory secrecy provision, a client's legal professional privilege, or a legal obligation of confidence.
- An entity collects personal information about a person who poses (or is alleged to pose) a risk of committing family violence and this collection is permitted by a legislated family violence information sharing scheme, such as that established by the Family Violence Protection Act 2008 (Vic).
- The impracticability of notification, including the time and cost, outweighs the privacy benefit of notification. For example:
    - where an entity collects personal information about the individual's next of kin for emergency contact purposes, it would generally be reasonable for the entity to take no steps to notify the next of kin of the collection of their personal information
    - where an individual provides unsolicited personal information to an entity about a third party for the purposes of a confidential alternative dispute resolution process, and the entity is not required to destroy or de-identify the information under APP 4 (see Chapter 4), it would generally be reasonable for the entity to take no steps to notify the third party. This is especially so where the entity will not rely on the personal information in investigating or resolving the matter, or does not have the contact details of the third party.

Matters about which an individual must be notified or made aware

5.8 APP 5.2 lists the matters (discussed separately below) that must be notified to an individual or of which they must be made aware. For each matter, an APP entity must consider whether notifying the individual is reasonable in the circumstances. This means that it may be reasonable for an entity to notify some but not all of the APP 5 matters. For example, it may be reasonable not to notify an individual of the collecting entity's identity where this is obvious from the circumstances.

The APP entity's identity and contact details

5.9 The matter set out in APP 5.2(a) is the identity and contact details of the APP entity. This could include the position title, telephone number and email address of a contact who handles enquiries and requests relating to the Privacy Act. Consideration could also be given to establishing a generic telephone number and email address (for example, privacy@agency.gov.au) that will not change with staff movements. This ensures awareness of a contact if an individual chooses to exercise any available rights such as to request access to, or correction of, personal information later (see Chapter 12 (APP 12) and Chapter 13 (APP 13)).

The facts and circumstances of collection

5.10 The matter set out in APP 5.2(b) is the fact and circumstances of collection. This may include how, when and from where the personal information was collected. This requirement applies where either the personal information has been collected from a third party or the individual may not be aware that the entity has collected their personal information.

5.11 The following examples illustrate matters that can be notified:

- Where the individual's personal information was or will be collected from another entity, the individual should be made aware of the name of the entity. If this is not practicable because, for instance, the APP entity collects information from a wide variety of entities and it would not be practicable to give a separate notice in relation to each entity, the APP entity should instead indicate the kinds of entities from which it collects that information.
- Where the individual's personal information was or will be collected from an individual, the name of that individual should be provided, unless doing so would be an interference with the privacy of that individual (for example, the use or disclosure breaches APP 6 because that individual would not reasonably expect their personal information to be disclosed in an APP 5 notice and no other exception in APP 6 applies) (see Chapter 6 (APP 6)).
- Where the individual may not be aware of their personal information being collected, the individual should be made aware of the method of collection, for example, that personal information is collected through use of a hidden radio-frequency identification tag (RFID tags), software (such as cookies), or biometric technology (such as voice or facial recognition).

If the collection is required or authorised by law

5.12 The matter set out in APP 5.2(c) is the fact (if applicable) that a collection is required or authorised by or under an Australian law or a court/tribunal order. The phrase 'required or authorised by or under an Australian law or court/tribunal order' is discussed in Chapter B (Key concepts).

5.13 The name of the Australian law (or, if applicable, the regulation or other instrument), or details of the particular court or tribunal order, that requires or authorises the collection, must also be included. If practicable, the notice could include the provision of the law, regulation or other instrument relied upon for collection.

5.14 If it is not reasonable to name the particular law relied upon (for example, multiple Australian laws authorise or require the collection) the more practical option may be to include a generic description of the laws under which personal information is collected (for example, 'taxation laws').

The purposes of collection

5.15 The matter set out in APP 5.2(d) is the purposes for which the APP entity collects the personal information. This includes the primary purpose of collection, that is, the specific function or activity for which particular personal information is collected.

5.16 If the APP entity may use or disclose personal information for purposes other than the primary purpose (known as a 'secondary purpose'), these could also be included. This may create a reasonable expectation that the personal information will be used or disclosed for a secondary purpose, of relevance to the exception in APP 6.2(a) (this exception is discussed in Chapter 6 (APP 6)). The entity does not need to include in its description internal purposes that form part of normal business practices, such as auditing, business planning, billing or de-identifying personal information.

5.17 The term 'purpose', including 'primary purpose', 'secondary purpose' and how a purpose should be described, are discussed in Chapter B (Key concepts) and Chapter 6 (APP 6)).

The consequences for the individual if personal information is not collected

5.18 The matter set out in APP 5.2(e) is the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity.

5.19 An APP entity is not required to list all possible or remote consequences or those that would be obvious to a reasonable person. Instead, it should describe significant consequences that could be expected to result. If the individual can avoid or lessen those consequences by providing some but not other personal information, this should be explained.

5.20 The following are given as examples of consequences that may result if personal information is not collected:

- An application for a licence, benefit, allowance or concession cannot be processed.
- An APP entity cannot properly investigate or resolve an individual's complaint.
- A different level of service will be provided to the individual. For example, the individual may not be eligible to purchase a discounted flight without providing personal information about a medical emergency in the individual's family.

Other APP entities, bodies or persons to which the personal information is usually disclosed

5.21 The matter set out in APP 5.2(f) is any other APP entity, body or person, or the types of other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity.

5.22 An APP entity is not required to include that a particular disclosure has occurred or will occur. Rather, APP 5.2(f) requires an entity to notify or ensure awareness of the 'usual' practices of the entity in disclosing personal information of that 'kind' to other APP entities, bodies or persons or 'types' of APP entities, bodies or persons.

5.23 A 'usual' disclosure is one that occurs regularly, under an agreed arrangement, or that can reasonably be predicted or anticipated. It does not include a disclosure that may occur in exceptional or special circumstances (such as a disclosure under a lawful warrant to a law enforcement agency).

5.24 The 'kind' of personal information that is usually disclosed may be described, for example, as 'contact details', 'employment history', 'educational qualifications' or 'complaint details'.

5.25 If the personal information is usually disclosed to a particular APP entity (including a related body corporate), body or person, it should be named, unless it would be impracticable to include a long list of APP entities, bodies or persons. In that case, the 'type' of APP entity, body or person should be described, for example, as 'health insurers' or 'State Government motor vehicle licensing authorities' or 'related bodies corporate.' An APP entity is not required to describe the disclosure practices of the APP entity, body or person to which the information is disclosed. However, if it is known that that APP entity, body or person usually discloses the personal information to other entities, this could be noted.

Information about access and correction in the APP entity's APP Privacy Policy

5.26 The matters set out in APP 5.2(g) and (h) are that the APP entity's APP Privacy Policy contains information about how the individual may:

- access and seek correction of their personal information held by the entity (APP 5.2(g))
- complain to the entity about a breach of the APPs, or any registered APP code that binds the entity, and how the entity will deal with such a complaint (APP 5.2(h))

5.27 Where practicable, an APP 5 notice could include a prominent and accessible link to the APP Privacy Policy on the entity's website or explain how it may be accessed. The APP Privacy Policy requirements are discussed in Chapter 1 (APP 1).

Likely cross-border disclosures of the personal information

5.28 The matters set out in APP 5.2(i) and (j) are:

- whether the APP entity is likely to disclose the personal information to overseas recipients (APP 5.2(i)), and
- if so, the countries in which such recipients are likely to be located if it is practicable to specify those counties in the notice or to otherwise make the individual aware of them (APP 5.2(j))

5.29 This requirement only applies to a likely disclosure of personal information to an overseas recipient. It does not apply to a use of personal information by an APP entity that does not constitute a disclosure. For example, routing personal information, in transit, through servers located outside Australia would usually be considered a 'use' and not a 'disclosure'.[2] Similarly, if an entity makes personal information accessible to an overseas office of the entity (for example, a consular office), this is a use and not a disclosure.[3] For further discussion of the requirements applying to a cross-border disclosure of personal information, and what is considered a disclosure, see Chapter 8 (APP 8).

5.30 An example of when it may be impracticable to specify the countries in which overseas recipients of personal information are likely to be located is where personal information is likely to be disclosed to numerous overseas recipients and the burden of determining where those recipients are located is excessively time-consuming, costly or inconvenient in all the circumstances. However, an APP entity is not excused from specifying the countries by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it impracticable to specify the countries will depend on whether the burden is excessive in all the circumstances. In this, as in other examples, it is the responsibility of the entity to be able to justify that this is impracticable.

5.31 The requirement to notify an individual or ensure awareness if information being collected is likely to be disclosed to overseas recipients, and the location of those recipients, complements the obligation on APP entities under APP 1.4(f) and (g) to describe overseas disclosure practices in an APP Privacy Policy (see Chapter 1 (APP 1)).

5.32 If the personal information is disclosed to numerous overseas locations, one practical option may be to list those countries in an appendix to the notice rather than in the body of the notice. Where it is not practicable to specify the countries, the entity could instead identify general regions (such as European Union countries).

5.33 An APP entity that regularly discloses personal information overseas could consider including additional information in an APP 5 notice about these disclosures, to ensure transparent handling of personal information. For example, the APP 5 notice could explain:

- how the overseas recipient might use, disclose and protect the personal information, including whether the overseas recipient may be required to disclose the personal information under a foreign law (see discussion of s 6A(4) in Chapter 8 (APP 8))
- how the individual can request further information about laws or binding schemes that protect privacy in the country of receipt (this information may be particularly relevant if an entity intends to rely on the exception in APP 8.2(a) (see Chapter 8 (APP 8))
- how the individual can access personal information held by the overseas recipient

When notification is to occur

5.34 An APP entity must take any reasonable steps to comply with APP 5:

- at or before the time an APP entity collects an individual's personal information, or
- if that is not practicable, as soon as practicable after the collection occurs

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

[3] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.

5.35 This requirement recognises that it is preferable that an individual can make an informed choice about whether to provide personal information to an APP entity.

5.36 Examples of when it may not be practicable to take reasonable steps at or before the time of collection include where:

- urgent collection of the personal information is required and giving a notice or ensuring awareness would unreasonably delay the collection, for example, where there is a serious threat to an individual's life or health or to public safety
- the medium through which personal information is collected makes it impracticable to provide a detailed APP 5 notice or ensure awareness at or before the time of collection. For example, where personal information is collected by telephone, it may be impracticable to notify or ensure the individual is aware of all of the APP 5 matters at the time of collection (see paragraph 5.5).[4]

5.37 The test of practicability is an objective test. It is the responsibility of the APP entity to be able to justify that it is not practicable to give notification or ensure awareness before or at the time of collection. Options for providing early notification or ensuring awareness should, so far as practicable, be built into information collection processes and systems – for example, by including relevant information in standard forms and online collection mechanisms (see APP 1.2, Chapter 1).

5.38 If notification does not occur before or at the time of collection, the APP entity must take reasonable steps to provide notification, or ensure the individual is aware, as soon as practicable after the collection. In adopting a timetable that is 'practicable', an entity can take technical and resource considerations into account. However, it is the responsibility of the entity to be able to justify any delay in notification.

[4] See also OAIC, Mobile Privacy: A Better Practice Guide for Mobile App Developers, section "4. Timing of user notice and consent is critical", OAIC website <https://www.oaic.gov.au>.

Chapter 6:

Australian Privacy Principle 6 —

Use or disclosure of personal information

Version 1.1, July 2019

OAIC

Contents

Key points **3**
What does APP 6 say? **3**
'Holds', 'use', 'disclose' and 'purpose' **4**
'Holds' 4
'Use' 4
'Disclose' 5
'Purpose' of collection 6
Using or disclosing personal information for a secondary purpose **6**
Using or disclosing personal information with the individual's consent 6
Using or disclosing personal information where reasonably expected by the individual and related to the primary purpose of collection 7
Using or disclosing personal information as required or authorised by law 9
Using or disclosing personal information where a permitted general situation exists 10
Using or disclosing personal information where a permitted health situation exists 12
Using or disclosing personal information for an enforcement related activity 14
Disclosing biometric information to an enforcement body 15
De-identifying certain health information before disclosure **16**
Related bodies corporate **16**
Disclosing personal information to a related body corporate 16
Using or disclosing personal information collected from a related body corporate 17

Key points

- APP 6 outlines when an APP entity may use or disclose personal information.
- An APP entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies.
- The exceptions include where:
  - the individual has consented to a secondary use or disclosure
  - the individual would reasonably expect the APP entity to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose
  - the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order
  - a permitted general situation exists in relation to the secondary use or disclosure
  - the APP entity is an organisation and a permitted health situation exists in relation to the secondary use or disclosure
  - the APP entity reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body, or
  - the APP entity is an agency (other than an enforcement body) and discloses biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner for the purposes of APP 6.3

What does APP 6 say?

6.1 APP 6 outlines when an APP entity may use or disclose personal information. The intent is that an entity will generally use and disclose an individual's personal information only in ways the individual would expect or where one of the exceptions applies.

6.2 An APP entity that holds personal information about an individual can only use or disclose the information for a particular purpose for which it was collected (known as the 'primary purpose' of collection), unless an exception applies. Where an exception applies the entity may use or disclose personal information for another purpose (known as the 'secondary purpose'). Exceptions include:

- the individual consented to a secondary use or disclosure (APP 6.1(a))
- the individual would reasonably expect the secondary use or disclosure, and that is related to the primary purpose of collection or, in the case of sensitive information, directly related to the primary purpose (APP 6.2(a))
- the secondary use or disclosure of the personal information is required or authorised by or under an Australian law or a court/tribunal order (APP 6.2(b))
- a permitted general situation exists in relation to the secondary use or disclosure of the personal information by the APP entity (APP 6.2(c))

- the APP entity is an organisation and a permitted health situation exists in relation to the secondary use or disclosure of the personal information by the organisation (APP 6.2(d))
- the APP entity reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body (APP 6.2(e))
- the APP entity is an agency (other than an enforcement body) and discloses personal information that is biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner for the purposes of APP 6.3 (APP 6.3)

6.3 An APP entity may disclose personal information, other than sensitive information, to a related body corporate (s 13B(1)(b)).

6.4 APP 6 does not apply to the use or disclosure by an organisation of:

- personal information for the purpose of direct marketing (this is covered by APP 7), or
- government related identifiers (this is covered by APP 9) (APP 6.7)

'Holds', 'use', 'disclose' and 'purpose'

6.5 Each of the terms 'holds', 'use', 'disclose' and 'purpose' which are used in APP 6 and other APPs, are discussed in more detail in Chapter B (Key concepts). The following is a brief analysis of the meaning of these terms in the context of APP 6.

'Holds'

6.6 APP 6 only applies to personal information that an APP entity 'holds'. An APP entity 'holds' personal information 'if the entity has possession or control of a record that contains the personal information' (s 6(1)).

6.7 The term 'holds' extends beyond physical possession of a record to include a record that an entity has the right or power to deal with. For example, an APP 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. The term 'holds' is discussed further in Chapter B (Key concepts).

'Use'

6.8 The term 'use' is not defined in the Privacy Act. An APP entity 'uses' information where it handles or undertakes an activity with the information, within the entity's effective control. For further discussion of use, see Chapter B (Key concepts). Examples include:

- the entity accessing and reading the personal information
- the entity searching records for the personal information
- the entity making a decision based on the personal information
- the entity passing the personal information from one part of the entity to another

- unauthorised access by an employee of the entity[1]

'Disclose'

6.9 The term 'disclose' is not defined in the Privacy Act. An APP entity 'discloses' personal information where it makes it accessible to others outside the entity and releases the subsequent handling of the information from its effective control. This focuses on the act done by the disclosing party. The state of mind or intentions of the recipient does not affect the act of disclosure. Further, there will be a disclosure in these circumstances even where the information is already known to the recipient. For further discussion of disclosure, see Chapter B (Key concepts).

6.10 The release may be a proactive release or publication, a release in response to a specific request, an accidental release or an unauthorised release by an employee.[2] Examples include where an APP entity:

- shares the personal information with another entity or individual
- discloses personal information to themselves, but in their capacity as a different entity
- publishes the personal information on the internet, whether intentionally or not,[3] and it is accessible by another entity or individual
- accidentally provides personal information to an unintended recipient[4]
- reveals the personal information in the course of a conversation with a person outside the entity
- displays a computer screen so that the personal information can be read by another entity or individual, for example, at a reception counter or in an office

6.11 '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.[5] Examples include unauthorised access following a cyber-attack[6] or a theft, including where the third party then makes that personal 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 Chapter 11 (APP 11))

---

[1] An APP entity is taken to have 'used' personal information where an employee gains unauthorised access 'in the performance of the duties of the person's employment' (see s 8(1)).

[2] An APP entity is taken to have 'disclosed' personal information where an employee carries out an unauthorised disclosure 'in the performance of the duties of the person's employment' (s 8(1)).

[3] See OAIC, Medvet Science Pty Ltd: Own Motion Investigation Report, July 2012, OAIC website <https://www.oaic.gov.au>; Telstra Corporation Limited: Own Motion Investigation Report, June 2012, OAIC website <https://www.oaic.gov.au>.

[4] The APP entity may also breach APP 11 if it did not take reasonable steps to protect the information from this unauthorised disclosure (see APP 11, Chapter 11).

[5] The actions of an employee will be attributed to the APP entity where it was carried out 'in the performance of the duties of the person's employment' (s 8(1)).

[6] See OAIC, Sony PlayStation Network / Qriocity: Own Motion Investigation Report, September 2011, OAIC website <https://www.oaic.gov.au>.

- 'use', which is discussed in paragraph 6.8 above. APP 6 generally imposes the same obligations on an APP entity for uses and disclosures of personal information. Therefore, this distinction is not relevant in interpreting this principle (except in relation to APP 6.3). However, the distinction is relevant to APP 8, which applies to the disclosure of personal information to an overseas recipient (see Chapter 8 (APP 8))

'Purpose' of collection

6.12 The purpose for which an APP entity collects personal information is known as the 'primary purpose' of collection. This is the specific function or activity for which the entity collects the personal information. 'Purpose', including how to identify and describe the primary purpose, is discussed in more detail in Chapter B (Key concepts).

6.13 The notification requirements in APP 5 complement the limitations on use and disclosure under APP 6. APP 5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. This includes the primary purpose of collection and could also include other purposes for which the entity collects the information (known as secondary purposes) (see APP 5.2(d)). The notification requirements are discussed in Chapter 5 (APP 5).

Using or disclosing personal information for a secondary purpose

6.14 A 'secondary purpose' is any purpose other than the primary purpose for which the APP entity collected the personal information.

6.15 The grounds on which an APP entity may use or disclose personal information for a secondary purpose are outlined below. It is nevertheless open to an entity not to rely on any such ground and to decide not to use or disclose personal information, unless the use or disclosure is required by law (see paragraphs 6.29–6.31 below).

Using or disclosing personal information with the individual's consent

6.16 APP 6.1(a) permits an APP entity to use or disclose personal information for a secondary purpose where the individual has consented to the use or disclosure.

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

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent

Using or disclosing personal information where reasonably expected by the individual and related to the primary purpose of collection

6.18 APP 6.2(a) permits an APP entity to use or disclose personal information for a secondary purpose if the individual would reasonably expect the entity to use or disclose the information for that secondary purpose, and:

- if the information is sensitive information, the secondary purpose is directly related to the primary purpose of collection, or
- if the information is not sensitive information, the secondary purpose is related to the primary purpose of collection

6.19 This exception creates a two-limb test which focuses both on the reasonable expectations of the individual, and the relationship between the primary and secondary purposes.

Reasonably expect

6.20 The 'reasonably expects' test is an objective one that has regard to what a reasonable person, who is properly informed, would expect in the circumstances. This is a question of fact in each individual case. It is the responsibility of the APP entity to be able to justify its conduct.

6.21 An APP entity should consider whether an individual would reasonably expect it to use or disclose for a secondary purpose only some of the personal information it holds about the individual, rather than all of the personal information it holds. The entity should only use or disclose the minimum amount of personal information sufficient for the secondary purpose. For example, an individual may not reasonably expect an entity that is investigating their complaint against a contractor to disclose the individual's residential address and home contact details to the contractor as part of its investigation. The individual would reasonably expect the entity to give the contractor only the minimum amount of personal information necessary to enable them to respond to the complaint.[7]

6.22 Examples of where an individual may reasonably expect their personal information to be used or disclosed for a secondary purpose include where:

- the individual makes adverse comments in the media about the way an APP entity has treated them. In these circumstances, it may be reasonable to expect that the entity may respond publicly to these comments in a way that reveals personal information specifically relevant to the issues that the individual has raised[8]
- an agency discloses to another agency a query, view or representation that an individual has made to the first-mentioned agency[9]
- the entity has notified the individual of the particular secondary purpose under APP 5.1 (see Chapter 5 (APP 5))

[7] For another example of where an individual would not reasonably expect disclosure, see W v Telecommunications Company [2007] PrivCmrA 25, Australasian Legal Information Institute website <www.austlii.edu.au>.

[8] See L v Commonwealth Agency [2010] PrivCmrA 14 (24 December 2010), Australasian Legal Information Institute website <www.austlii.edu.au>.

[9] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 78.

- the secondary purpose is a normal internal business practice, such as as auditing, business planning, billing or de-identifying the personal information

Relationship between the primary and secondary purpose

6.23 This exception is limited to using or disclosing personal information for a secondary purpose that is 'related', or for sensitive information 'directly related', to the primary purpose of collection.

Related secondary purpose

6.24 A related secondary purpose is one which is connected to or associated with the primary purpose. There must be more than a tenuous link.[10]

6.25 Examples of where a secondary purpose is related to the primary purpose of collection include:

- An organisation collects personal information about an individual for the primary purpose of collecting a debt. A law firm, acting on behalf of that organisation in relation to the debt collection, contacts the individual's neighbour and seeks information from the neighbour about the individual's whereabouts (but does not disclose any specific information about the debt). This disclosure to the neighbour, for the secondary purpose of locating the individual, is related to the primary purpose of debt collection and would be within the individual's reasonable expectations[11]
- An agency collects personal information to include in an employee's personnel file for the primary purpose of administering that individual's employment.[12] It then uses this personal information as part of an investigation into complaints by the individual about working conditions. In these circumstances, the use for the secondary purpose of investigating a complaint in the workplace is related to the primary purpose of collection, and would be within the individual's reasonable expectations[13]
- An APP entity uses personal information for the purpose of de-identifying the information.

Directly related secondary purpose

6.26 For the use or disclosure of sensitive information, the secondary purpose must be 'directly related' to the primary purpose of collection. A directly related secondary purpose is one which is closely associated with the primary purpose, even if it is not strictly necessary to achieve that primary purpose. This requirement for a direct relationship recognises that the use and disclosure of sensitive information can have serious ramifications for the individual or their associates, including humiliation, embarrassment or loss of dignity.

---

[10] For examples of where disclosure of personal information for a secondary purpose is not related to the primary purpose of collection, see B v Hotel [2008] PrivCmrA 2, Australasian Legal Information Institute website <www.austlii.edu.au>. E v Insurance Company [2011] PrivCmrA 5, Australasian Legal Information Institute website <www.austlii.edu.au>.

[11] This example is adapted from M and Law Firm [2011] AICmrCN 7 (available at Australasian Legal Information Institute website <www.austlii.edu.au>), where the Commissioner also referred the complaint to the Australian Competition and Consumer Commission to consider whether the debt collection practices were consistent with its debt collection guidelines.

[12] The exemption relating to employee records in s 7B(3) only applies to organisations.

[13] N v Commonwealth Agency [2009] PrivCmrA 17, Australasian Legal Information Institute website <www.austlii.edu.au>.

6.27 An example of where a secondary purpose is directly related to the primary purpose of collection is:

- A health service provider collects health information about an individual for the purpose of providing treatment, and then decides, for ethical and therapeutic reasons, that they cannot treat the individual. The health service provider then advises another provider at the medical clinic of the individual's need for treatment and of the provider's inability to provide that treatment. This disclosure to the other provider is directly related to the purpose for which the information was collected, and would be within the individual's reasonable expectations.[14]

6.28 The use of sensitive information for the purpose of de-identifying the information will also be directly related to the primary purpose of collection.

Using or disclosing personal information as required or authorised by law

6.29 An APP entity may use or disclose personal information for a secondary purpose if the use or disclosure is required or authorised by or under an Australian law or a court/tribunal order (APP 6.2(b)).

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

6.31 Examples of where an APP entity may be required or authorised by law to use or disclose personal information include where:

- a warrant, order or notice issued by a court requires the entity to provide information, or produce records or documents that are held by the entity
- the entity is subject to a statutory requirement to report certain matters to an agency or enforcement body, for example, specific financial transactions, notifiable diseases and suspected cases of child abuse
- a law applying to the entity clearly and specifically authorises it to use or disclose the personal information, for example:
    - to give a record to the Private Health Insurance Ombudsman,[15] or to disclose matters to a trustee conducting a bankruptcy investigation[16]
    - a specified use or disclosure of personal information by an Agency Head, the Merit Protection Commissioner or the Australian Public Service Commissioner[17]
    - a specified use or disclosure of personal information under the Privacy Act, for example, to de-identify personal information as required by APP 11

[14] F v Medical Specialist [2009] PrivCmrA 8, Australasian Legal Information Institute website <www.austlii.edu.au>.

[15] Private Health Insurance Act 2007, s 250.10.

[16] Bankruptcy Act 1966, s 77A.

[17] Public Service Act 1999, s 72E and Public Service Regulations 1999, regulation 9.2.

Using or disclosing personal information where a permitted general situation exists

6.32 An APP entity may use or disclose personal information for a secondary purpose if a 'permitted general situation' exists in relation to the use or disclosure of the information by the entity (APP 6.2(e)).

6.33 Section 16A lists seven permitted general situations (two of which only apply to agencies). The seven situations are set out below, and are discussed in Chapter C (Permitted general situations), including the meaning of relevant terms.

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

6.34 An APP entity may use or disclose personal information for a secondary purpose where:

- it is unreasonable or impracticable to obtain the individual's consent to the use or disclosure, and
- the entity reasonably believes the use or 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 (s 16A(1), Item 1)

6.35 Examples of where this permitted general situation might apply include:

- where an individual is seriously injured while interstate and, due to their injuries, cannot give informed consent, the individual's usual health service provider may be able to disclose personal information about the individual to another health service provider who is treating the individual's serious injuries on the basis that it is impracticable to obtain the individual's consent
- where an APP entity that provides child protection services has evidence that a child is at risk of physical or sexual abuse by their parent, the entity may be able to disclose the personal information of the parent to another child protection service on the basis that it would be unreasonable to obtain the parent's consent

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

6.36 An APP entity may use or disclose personal information for a secondary purpose 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 collection use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter (s 16A(1), Item 2)

6.37 Examples of where this permitted general situation might apply are the use of personal information by:

- an APP entity that is investigating fraudulent conduct by a professional adviser or a client in relation to the entity's functions or activities
- an agency that is investigating a suspected serious breach by a staff member of the Australian Public Service Code of Conduct

Locating a person reported as missing

6.38 An APP entity may use or disclose personal information for a secondary purpose where the entity:

- reasonably believes that the use or disclosure is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing, and
- the use or disclosure complies with rules made by the Commissioner under s 16A(2) (s 16A(1), Item 3)

Reasonably necessary for establishing, exercising or defending a legal or equitable claim

6.39 An APP entity may use or disclose personal information for a secondary purpose where the use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim (s 16A(1) Item 4).

6.40 An example of where this permitted general situation might apply is where an individual has made a claim under their life insurance policy and the insurer is preparing to dispute the claim. The insurer may use or disclose personal information about the individual to establish its defence of the claim.

Reasonably necessary for a confidential alternative dispute resolution processes

6.41 An APP entity may use or disclose personal information for a secondary purpose where the use or disclosure is reasonably necessary for the purposes of a confidential alternative dispute resolution (ADR) process (s 16A(1), Item 5).

6.42 An example of where this permitted general situation might apply is where an APP entity discloses their version of events during a confidential ADR process, where that account includes the disclosure of personal information about an individual who is directly or indirectly involved in the dispute. This permitted general situation will only apply where the parties to the dispute and the ADR provider are bound by confidentiality obligations.

Necessary for a diplomatic or consular function or activity

6.43 An agency may use or disclose personal information for a secondary purpose where the agency reasonably believes that the use or disclosure is necessary for the agency's diplomatic or consular functions or activities (s 16A(1), Item 6). This permitted general situation applies only to agencies, and not to organisations.

6.44 An example of where this permitted general situation might apply is where an agency with diplomatic or consular functions uses or discloses personal information to grant a diplomatic visa to a foreign national accredited as a member of the diplomatic staff of a mission to Australia.

Necessary for certain Defence Force activities outside Australia

6.45 The Defence Force (as defined in s 6(1)) may use or disclose personal information for a secondary purpose where it reasonably believes that the use or 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).

6.46 An example of where this permitted general situation might apply is where the Defence Force uses and discloses personal information about an enemy or other hostile adversary in order to support military operations.

Using or disclosing personal information where a permitted health situation exists

6.47 An organisation may use or disclose personal information if a 'permitted health situation' exists in relation to the use or disclosure (APP 6.2(d)). This exception applies only to organisations, and not to agencies.

6.48 Section 16B lists three permitted health situations that relate to the use or disclosure of health information or genetic information by an organisation. The three situations are set out below, and are discussed in Chapter D (Permitted health situations), including the meaning of relevant terms.

Conducting research; compiling or analysing statistics; management, funding or monitoring of a health service

6.49 An organisation may use or disclose health information about an individual for a secondary purpose if the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety, and:

- it is impracticable to obtain the individual's consent to the use or disclosure
- the use or disclosure is conducted in accordance with guidelines approved under s 95A,[18] and
- in the case of disclosure, the organisation reasonably believes that the recipient of the information will not disclose the information, or personal information derived from that information (s 16B(3))

6.50 An example of where this permitted health situation might apply is where an organisation discloses health information to a researcher who is conducting public health research in circumstances where the age of the information makes it impracticable to obtain consent. The disclosing organisation should have a written agreement with the researcher which requires the researcher not to disclose the health information, or any personal information that is derived from that health information. The disclosure must be carried out in accordance with guidelines approved under s 95A.

Necessary to prevent a serious threat to the life, health or safety of a genetic relative

6.51 An organisation may use or disclose genetic information about an individual for a secondary purpose if:

- the organisation has obtained the information in the course of providing a health service to the individual

[18] See National Health and Medical Research Council (NHMRC), Guidelines Approved Under Section 95A of the Privacy Act 1988, NHMRC website <https://www.nhmrc.gov.au>.

- the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another individual who is a genetic relative of the individual
- the use or disclosure is conducted in accordance with guidelines approved under s 95AA,[19] and
- in the case of disclosure, the recipient of the information is a genetic relative of the individual (s 16B(4))

6.52 An example of where this permitted health situation might apply is:

- in the course of providing a health service, an organisation obtains information that a patient has a pathogenic mutation in the Huntington disease gene, and
- the individual refuses to consent to the organisation disclosing any information to their genetic relatives, even after the individual has participated in discussions and counselling, and received information about the implications of the diagnosis for the individual's genetic relatives
- despite this refusal, the organisation may disclose the genetic information to genetic relatives under this exception, providing any disclosure is in accordance with the guidelines approved under s95AA

Disclosure to a responsible person for the individual

6.53 An organisation may disclose health information about an individual for a secondary purpose if:

- the organisation provides a health service to the individual
- the recipient of the information is a 'responsible person' for the individual
- the individual is either physically or legally incapable of giving consent to the disclosure, or physically cannot communicate consent to the disclosure
- the individual providing the health service (the 'carer') is satisfied that either the disclosure is necessary to provide appropriate care or treatment of the individual, or the disclosure is made for compassionate reasons
- the disclosure is not contrary to any wish expressed by the individual before the individual became unable to give or communicate consent of which the carer is aware or of which the carer could reasonably be expected to be aware
- the disclosure is limited to the extent reasonable and necessary for providing appropriate care or fulfilling compassionate reasons (s 16B(5))

6.54 An example of where this permitted health situation might apply is where an individual who cannot give consent is released from hospital into the care of family members. The health service provider (referred to in this exception as the 'carer') discloses health information to the family members to enable them to monitor the individual's progress and administer medication. In these circumstances, the exception would apply where the carer is satisfied

[19] See National Health and Medical Research Council (NHMRC), Use and Disclosure of Genetic Information to a Patient's Genetic Relatives Under Section 95AA of the Privacy Act 1988: Guidelines for Health Practitioners in the Private Sector, NHMRC website <https://www.nhmrc.gov.au>.

that the disclosure is necessary to provide appropriate care for the individual. The disclosure must be limited to the extent reasonable and necessary to provide appropriate care.

6.55 Another example is where a carer discloses health information to an unconscious patient's family members about the patient's condition. In these circumstances, the exception would apply where the carer is satisfied that the disclosure is necessary for compassionate reasons. The disclosure must be limited to the extent reasonable and necessary for the compassionate reasons.

Using or disclosing personal information for an enforcement related activity

6.56 An APP entity may use or disclose personal information for a secondary purpose where the entity reasonably believes that the use or disclosure of the personal information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body (APP 6.2(e)).

6.57 'Enforcement body' is defined in s 6(1) as a list of specific bodies and is discussed in Chapter B (Key concepts). 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 Commissioner,[20] the Immigration Department,[21] Australian Prudential Regulation Authority, the Australian Securities and Investments Commission and AUSTRAC.

6.58 'Enforcement related activities' is defined in s 6(1) and is discussed in Chapter B (Key concepts). Enforcement related activities include the prevention, detection, investigation and prosecution or punishment of criminal offences and intelligence gathering activities.

Reasonable belief

6.59 The phrase 'reasonable belief' is discussed in Chapter B (Key concepts). In summary, the APP entity must have a reasonable basis for the belief, and not merely a genuine or subjective belief. It is the responsibility of the entity to be able to justify its reasonable belief.

6.60 In some circumstances, the basis for an APP entity's 'reasonable belief' will be clear, for example, if the entity discloses personal information in response to a written request by an enforcement body and the request is dated and signed by an authorised person. In other circumstances, the basis for this belief may be less clear, and the entity will need to reflect more carefully about whether its judgment is reasonable.

Reasonably necessary

6.61 The 'reasonably necessary' test is an objective test: whether a reasonable person who is properly informed would agree that the use or disclosure is reasonable in the circumstances. Again, it is the responsibility of an APP entity to be able to justify that the particular use or disclosure is reasonably necessary.

---

[20] 'Integrity Commissioner is defined in s 6(1) as having the same meaning as in the Law Enforcement Integrity Commissioner Act 2006.

[21] 'Immigration Department' is defined in s 6(1) as the Department administered by the Minister administering the Migration Act 1958.

6.62 For example, investigators from an enforcement body suspect that a particular building is being used for drug trafficking activities. As part of the enforcement body's intelligence gathering, the investigators request an APP entity to disclose the personal information of individuals associated with the building (although the investigators do not know the extent, if any, of the involvement of the individuals). This disclosure would be 'reasonably necessary' as it forms an important part of the enforcement body's intelligence gathering about the suspected drug trafficking.

6.63 The use or disclosure does not need to relate to an existing enforcement related activity. The use or disclosure may be reasonably necessary for the initiation of an enforcement related activity. This recognises that a law enforcement body may not be in a position to prevent, detect or investigate offences or breaches of the law, unless and until certain information, including personal information, is brought to its attention.

6.64 An APP entity should ensure that it only uses or discloses the minimum amount of personal information reasonably necessary for a particular enforcement related activity. For example, an entity may hold a range of personal information about an individual, such as the person's contact details, their photograph and information about their political views and religious views. Before disclosing all of this personal information to the enforcement body, the entity should consider whether only some of it is reasonably necessary for the enforcement related activity. If so, it should disclose only that information.

Making a written note of use or disclosure for this secondary purpose

6.65 If an APP entity uses or discloses personal information in accordance with the 'enforcement related activities' exception in APP 6.2(e), the entity must make a written note of the use or disclosure (APP 6.5).

6.66 The APP entity could include the following details in that note:

- the date of the use or disclosure
- details of the personal information that was used or disclosed
- the enforcement body conducting the enforcement related activity
- if the entity used the personal information, how the personal information was used by the entity
- if the entity disclosed the personal information, who it disclosed the personal information to (this may be the enforcement body or another entity)
- the basis for the entity's 'reasonable belief'. This will help the entity assure itself that this exception applies, and it may be a useful reference if the entity later needs to justify its reasonable belief

6.67 This requirement does not apply where a law prohibits the APP entity from making such a record.

Disclosing biometric information to an enforcement body

6.68 An agency may disclose biometric information or biometric templates for a secondary purpose if:

- the agency is not an enforcement body, and

- the recipient of the information is an enforcement body, and
- the disclosure is conducted in accordance with guidelines made by the Commissioner for the purposes of APP 6.3 (see APP 6.3, Chapter 6)

6.69 This exception does not apply to organisations.

6.70 'Biometric information' and 'biometric templates' are types of 'sensitive information' (defined in s 6(1)). 'Enforcement body' is defined in s 6(1) and is discussed in more detail in Chapter B (Key concepts).

De-identifying certain health information before disclosure

6.71 APP 6.4 applies where an organisation collects health information under an exception to APP 3 in s 16B(2). Section 16B(2) outlines the permitted health situation that allows an organisation to collect health information about an individual if the collection is necessary for research relevant to public health or safety, the compilation or analysis of statistics relevant to public health or public safety, or the management, funding or monitoring of a health service and certain other criteria are satisfied (see Chapter D (Permitted health situations)).

6.72 In these circumstances, APP 6.4 requires the organisation to take reasonable steps to ensure that the information is de-identified, before it discloses the information in accordance with APPs 6.1 or 6.2.

6.73 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).[22]

6.74 The reasonable steps that an organisation should take will depend upon circumstances that include:

- the possible adverse consequences for an individual if their health information is not de-identified before it is disclosed. More rigorous steps may be required as the risk of adversity increases.
- the practicability, including time and cost involved. However, an organisation is not excused from taking particular steps to de-identify health 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.

Related bodies corporate

Disclosing personal information to a related body corporate

6.75 Section 13B(1)(b) provides that where a body corporate discloses personal information (other than sensitive information) to a related body corporate, this is generally not considered 'an interference with the privacy of an individual' under the Privacy Act

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

(interferences with privacy are discussed in Chapter A (Introductory matters)). This provision applies to related bodies corporate and not to other corporate relationships, such as a franchise or joint-venture relationship.[23]

6.76 The effect of this provision is that an APP entity may disclose personal information (other than sensitive information) to a related body corporate without relying on an exception in APP 6.2.

Using or disclosing personal information collected from a related body corporate

6.77 An APP entity that collects personal information from a related body corporate is taken to have the same primary purpose of collection as its related body corporate (APP 6.6). Under APP 6, the entity may only use or disclose the personal information for that primary purpose, unless an exception to that principle applies (see paragraph 6.2 above).

For example, an APP entity collects personal information about an applicant contractor for the purpose of assessing their suitability to perform work on its behalf. The parent company then collects that personal information from the entity. The primary purpose of this collection is taken to be the same as the original purpose of collection. The parent company may only disclose the personal information to a third party for another purpose, where an exception to APP 6 applies.

[23] Section 6(8) states 'for the purposes of this Act, the question of whether bodies corporate are related to each other is determined in the manner in which that question is determined under the Corporations Act 2001'.

Chapter 7:

Australian Privacy Principle 7 —

Direct marketing

Version 1.1, July 2019

OAIC

Contents

Key points 3
What does APP 7 say? 3
'Direct marketing' 4
When are agencies covered by APP 7? 5
Using and disclosing personal information for the purpose of direct marketing where reasonably expected by the individual 5
Reasonably expect 5
Providing a simple means for 'opting out' 6
Using and disclosing personal information for the purpose of direct marketing where no reasonable expectation of the individual, or information collected from a third party 7
Consent 7
Impracticable to obtain consent 7
Providing a prominent statement about simple means for 'opting out' 8
Using and disclosing sensitive information for the purpose of direct marketing with the individual's consent 9
Using and disclosing personal information for the purpose of direct marketing by contracted service providers 9
Requests by an individual to stop direct marketing communications 9
Requests by an individual to stop facilitating direct marketing 10
When does an organisation 'facilitate' direct marketing? 10
Requests by an individual to identify the source of the personal information 11
Interaction with other legislation 11

Key points

- APP 7 provides that an organisation must not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies. APP 7 may also apply to an agency in the circumstances set out in s 7A.
- Direct marketing involves the use or disclosure of personal information to communicate directly with an individual to promote goods and services.
- Where an organisation is permitted to use or disclose personal information for the purpose of direct marketing, it must always:
  - allow an individual to request not to receive direct marketing communications (also known as 'opting out'), and
  - comply with that request
- An organisation must, on request, provide its source for an individual's personal information, unless it is impracticable or unreasonable to do so.

What does APP 7 say?

7.1 An organisation must not use or disclose the personal information that it holds about an individual for the purpose of direct marketing (APP 7.1). The term 'holds' is discussed in Chapter B (Key concepts).

7.2 There are a number of exceptions to this requirement. The exceptions in APP 7.2 and 7.3 apply to personal information other than sensitive information. They draw a distinction between the use or disclosure of personal information by an organisation where:

- the personal information has been collected directly from an individual, and the individual would reasonably expect their personal information to be used for the purpose of direct marketing (APP 7.2), and
- the personal information has been collected from a third party, or from the individual directly but the individual does not have a reasonable expectation that their personal information will be used for the purpose of direct marketing (APP 7.3). Sources of third party data include data list providers, third party mobile applications, third party lead generation and enhancement data

7.3 Both of these exceptions require an organisation to provide a simple means by which an individual can request not to receive direct marketing communications (also known as 'opting out'). However, in the circumstances where the organisation has not obtained personal information from the individual, or the individual would not reasonably expect their personal information to be used in this way, there are additional requirements to ensure that the individual is made aware of their right to opt out of receiving direct marketing communications from the organisation.

7.4 Exceptions to this principle also apply in relation to:

- sensitive information (APP 7.4), and
- an organisation that is a contracted service provider for a Commonwealth contract (APP 7.5)

7.5 APP 7 may apply to an agency in the circumstances set out in s 7A (see paragraph 7.13 below).

7.6 An individual may request an organisation not to use or disclose their personal information for the purpose of direct marketing, or for the purpose of facilitating direct marketing by other organisations (APP 7.6). The organisation must give effect to any such request by an individual within a reasonable period of time and for free (APP 7.7).

7.7 An organisation must, on request, notify an individual of its source of the individual's personal information that it has used or disclosed for the purpose of direct marketing unless this is unreasonable or impracticable to do so (APP 7.6).

7.8 APP 7 does not apply to the extent that the Do Not Call Register Act 2006, the Spam Act 2003 or any other legislation prescribed by the regulations apply (APP 7.8). APP 7 will still apply to the acts or practices of an organisation that are exempt from these Acts.

'Direct marketing'

7.9 Direct marketing involves the use and/or disclosure of personal information to communicate directly with an individual to promote goods and services.[1] A direct marketer may communicate with an individual through a variety of channels, including telephone, SMS, mail, email and online advertising.

7.10 Organisations involved in direct marketing often collect personal information about an individual from a variety of sources, including:

- public records, such as telephone directories and land title registers
- membership lists of business, professional and trade organisations
- online, paper-based or phone surveys and competitions
- online accounts, for example, purchase history or the browsing habits of identified, or logged in, users[2]
- mail order or online purchases

7.11 Examples of direct marketing by an organisation include:

- sending an individual a catalogue in the mail addressed to them by name
- displaying an advertisement on a social media site that an individual is logged into, using personal information, including data collected by cookies relating to websites the individual has viewed[3]
- sending an email to an individual about a store sale, or other advertising material relating to the store, using personal information provided by the customer in the course of signing up for a store loyalty card

7.12 Marketing is not direct, and therefore APP 7.1 does not apply, if personal information is not used or disclosed to identify or target particular recipients, for example, where:

[1] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 81.

[2] For more information about online behavioural advertising and personal information, see OAIC, Targeted Advertising, OAIC website <https://www.oaic.gov.au>.

[3] For more information about cookies, see OAIC, Targeted Advertising, OAIC website <https://www.oaic.gov.au>.

- an organisation sends catalogues by mail to all mailing addresses in a particular location, addressed 'To the householder' (that is, where recipients are not selected on the basis of personal information)
- an organisation hand delivers promotional flyers to the mailboxes of local residents
- an organisation displays advertisements on a website, but does not use personal information to select which advertisements are displayed

When are agencies covered by APP 7?

7.13 An agency must comply with the direct marketing requirements of APP 7 in the circumstances set out in s 7A. These circumstances include where:

- the agency is listed in Part 1 of Schedule 2 to the Freedom of Information Act 1982 (the FOI Act) and is prescribed in regulations,[4] or
- the act or practice relates to the commercial activity of an agency specified in Part 2 of Schedule 2 to the FOI Act[5]

Using and disclosing personal information for the purpose of direct marketing where reasonably expected by the individual

7.14 APP 7.2 provides that an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

- the organisation collected the personal information from the individual
- the individual would reasonably expect the organisation to use or disclose the personal information for that purpose
- the organisation provides a simple way for the individual to request not to receive direct marketing communications from the organisation (also known as 'opting out'), and
- the individual has not made such a request to the organisation

Reasonably expect

7.15 The 'reasonably expect' test is an objective test that has regard to what a reasonable person, who is properly informed, would expect in the circumstances. This is a question of fact in each individual case. It is the responsibility of the organisation to be able to justify its conduct.

7.16 Factors that may be important in deciding whether an individual has a reasonable expectation that their personal information will be used or disclosed for the purpose of direct marketing include where:

[4] See the Federal Register of Legislation <https://www.legislation.gov.au> for up-to-date versions of the regulations made under the Freedom of Information Act 1982.

[5] See s 7A and OAIC, FOI Guidelines, Part 2, OAIC website <https://www.oaic.gov.au>.

- the individual has consented to the use or disclosure of their personal information for that purpose (see discussion in paragraph 7.23 below and Chapter B (Key concepts) for further information about the elements of consent)
- the organisation has notified the individual that one of the purposes for which it collects the personal information is for the purpose of direct marketing under APP 5.1 (see Chapter 5 (APP 5))
- the organisation made the individual aware that they could request not to receive direct marketing communications from the organisation, and the individual does not make such a request (see paragraph 7.21)

7.17 An organisation should not assume that an individual would reasonably expect their personal information to be used or disclosed for the purpose of direct marketing just because the organisation believes that the individual would welcome the direct marketing, for example, because of the individual's profession, interest or hobby.

7.18 An individual is not likely to have a reasonable expectation that their personal information will be used or disclosed for the purpose of direct marketing where the organisation has notified the individual that their personal information will only be used for a particular purpose unrelated to direct marketing. For example, where an individual provides personal information to their bank when setting up internet banking, and the bank tells the individual that it will only use that personal information for enabling security for internet banking, the individual is not likely to have a reasonable expectation that their personal information will then be used or disclosed for the purpose of direct marketing.[6]

Providing a simple means for 'opting out'

7.19 A simple means for opting out should include:

- a visible, clear and easily understood explanation of how to opt out, for example, instructions written in plain English and in a font size that is easy to read
- a process for opting out, which requires minimal time and effort
- an opt out process that uses a straightforward and accessible communication channel, or channels. For example, the same communication channel that the organisation used to deliver the direct marketing communication. However, in some circumstances, a straightforward and accessible communication channel may be a different channel to that used to deliver the direct marketing communication, such as telephone and email, where the original channel was post, and
- an opt out process that is free, or that does not involve more than a nominal cost for the individual, for example, the cost of a local phone call, text message or postage stamp

7.20 The individual should be able to easily find out how to opt out. For example, an organisation could provide information about how to opt out in each direct marketing communication. An organisation should also consider whether the means for opting out is accessible to a person with a disability.

7.21 If the individual has 'opted out', the organisation must not use or disclose their personal information for the purpose of direct marketing, in accordance with the individual's request

[6] A and Financial Institution [2012] AICmrCN 1 (1 May 2012).

(APP 7.2(d)). Further examples of a simple means to opt out are given in paragraphs 7.27–7.30 below.

Using and disclosing personal information for the purpose of direct marketing where no reasonable expectation of the individual, or information collected from a third party

7.22 APP 7.3 provides that an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

- the organisation collected the information from:
  - the individual, but the individual would not reasonably expect their information to be used or disclosed for that purpose, or
  - a third party, and
- the individual has consented to use or disclosure for that purpose, or it is impracticable to obtain that consent, and
- the organisation provides a simple way for the individual to opt out of receiving direct marketing communications from the organisation, and
- in each direct marketing communication with the individual, the organisation includes a prominent statement, or otherwise draws the individual's attention to the fact that the individual may make such a request (referred to as an 'opt out statement'), and
- the individual has not made such a request to the organisation

Consent

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

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent

Impracticable to obtain consent

7.24 Whether it is 'impracticable' for an organisation to obtain consent will depend on a number of factors, including the time and cost involved in seeking consent. However, an organisation is not excused from obtaining consent by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it impracticable to obtain consent will depend on whether the burden is excessive in all the circumstances.

7.25 An organisation may obtain the consent from the individual in relation to a subsequent use or disclosure of the individual's personal information for the purpose of direct marketing at the time it collects the personal information. In order to rely on this consent, the

organisation must be satisfied that it is still current at the time of the use or disclosure. 'Current' consent is discussed in Chapter B (Key concepts).

7.26 Where an organisation did not obtain the individual's consent at the time of collection, it must obtain the consent of the individual for the proposed use or disclosure, unless it is impracticable to do so. In that case, the organisation should assess whether it is impracticable to obtain consent at the time of the proposed use or disclosure.

Providing a prominent statement about simple means for 'opting out'

7.27 APP 7.3 requires that an organisation provides a simple means for an individual to opt out of receiving direct marketing communications (see discussion at paragraphs 7.19–7.21 above).

7.28 In addition, APP 7.3 requires an organisation to provide a prominent statement that the individual may request to opt out in each direct marketing communication. This statement should meet the following criteria:

- it should be written in plain English, and not use legal or industry jargon
- it should be positioned prominently, and not hidden amongst other text. Headings may be necessary to draw attention to the statement, and
- it should be published in a font size and type which is easy to read, for example, in at least the same font size as the main body of text in the communication

7.29 The following are given as examples of ways that an organisation may comply with the 'opt out' requirements of APP 7.3:

- clearly indicating in each direct marketing email that the individual can opt out of receiving future emails by replying with a single word instruction in the subject line (for example, 'unsubscribe'). Alternatively, ensuring that a link is prominently located in the email, which takes the individual to a subscription control centre
- clearly indicating that the individual can opt out of future direct marketing by replying to a direct marketing text message with a single word instruction (for example, 'STOP')
- telling the recipient of a direct marketing phone call that they can verbally opt out from any future calls
- including instructions about how to opt out from future direct marketing in each mailed communication

7.30 In each case, an organisation may use an opt out mechanism that provides the individual with the opportunity to indicate their direct marketing communication preferences, including the extent to which they wish to opt out. However, the organisation should always provide the individual with an option to opt out of all future direct marketing communications as one of these preferences.

Using and disclosing sensitive information for the purpose of direct marketing with the individual's consent

7.31 APP 7.4 provides that an organisation may use or disclose sensitive information for the purpose of direct marketing if the individual has consented to the use or disclosure for that purpose.

7.32 The requirement to obtain consent applies even if the individual and the organisation have a pre-existing relationship.[7] If consent is not obtained, the organisation cannot rely on this exception, even if obtaining consent is impracticable or impossible in the circumstances.

7.33 Consent is discussed in paragraph 7.23 below, and generally in Chapter B (Key concepts). 'Sensitive information' is defined in s 6(1) and discussed in Chapter B (Key concepts).

Using and disclosing personal information for the purpose of direct marketing by contracted service providers

7.34 APP 7.5 provides that an organisation that is a contracted service provider for a Commonwealth contract may use or disclose personal information for the purpose of direct marketing if:

- it collects the information for the purpose of meeting (directly or indirectly) an obligation under the contract, and
- the use or disclosure is necessary to meet (directly or indirectly) such an obligation

7.35 The terms 'contracted service provider' and 'Commonwealth contract' are defined in s 6(1) and discussed in Chapter A (Introductory matters).

Requests by an individual to stop direct marketing communications

7.36 If an organisation uses or discloses personal information about an individual for the purpose of direct marketing, the individual may request not to receive direct marketing communications from that organisation (APP 7.6(c)).

7.37 The organisation must not charge the individual for making or giving effect to the request (APP 7.7). It must also stop sending the direct marketing communications within a reasonable period after the request is made (APP 7.7(a)). A 'reasonable period' would generally be no more than 30 days. However, an organisation could give effect to an opt-out request in a shorter timeframe, particularly where digital communication channels are being utilised.

[7] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 82.

7.38 When the first organisation engages a second organisation to carry out, or assist in carrying out direct marketing on its behalf, it should ensure that the contractual arrangements with the second organisation reflect the first organisation's obligations under APP 7. Where the second organisation is an APP entity, it must also comply with the APPs when handling personal information (see also paragraph 7.44 below).

7.39 In particular, where an individual makes a request to the second organisation to stop the direct marketing under APP 7.6, the contractual arrangements between the two organisations could require the second organisation to give effect to or pass on the opt out request to the first organisation.

Requests by an individual to stop facilitating direct marketing

7.40 An individual may request an organisation not to use or disclose personal information about the individual for the purpose of facilitating direct marketing by a second organisation (APP 7.6(d)).

7.41 The organisation must not charge the individual for making or giving effect to the request (APP 7.7). It must also stop using or disclosing the personal information for the purpose of facilitating direct marketing by a second organisation within a reasonable period after the request is made (APP 7.7(a)). A 'reasonable period' would be no more than 30 days. However, an organisation could give effect to an opt-out request in a shorter timeframe, particularly when digital communication channels are being utilised.

7.42 Where the second organisation is an APP entity, an individual can also make a separate request to not receive direct marketing communications from that organisation (APP 7.6(c)).

When does an organisation 'facilitate' direct marketing?

7.43 An organisation (the first organisation) facilitates direct marketing where it collects personal information for the purpose of providing that personal information to another organisation (the second organisation), so that the second organisation can undertake direct marketing of its own products or services.[8] For example, an organisation facilitates direct marketing where it collects personal information and sells that personal information to the second organisation which uses or discloses the personal information to send out marketing material.

7.44 An organisation does not facilitate direct marketing where it engages a second organisation to carry out, or assist in carrying out, direct marketing on its own behalf. In these circumstances, the second organisation will usually be a contractor, or an agent of the first organisation (see paragraphs 7.38–7.39 above). The following are given as examples of where an organisation 'carries out' direct marketing through a contractor, rather than facilitates direct marketing by a second organisation:

- An organisation engages a mailing house to mail out its direct marketing communications.

[8] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 82.

- An organisation engages a second organisation to conduct door-to-door marketing or telemarketing on its behalf.

Requests by an individual to identify the source of the personal information

7.45 An individual may ask an organisation to identify the source of the personal information that it uses or discloses for the purpose of direct marketing, or for the purpose of facilitating direct marketing by other organisations (APP 7.6(e)).

7.46 The organisation must then notify the individual of its source, unless this is impracticable or unreasonable (APP 7.7(b)). It is the responsibility of the organisation to be able to justify that it is impracticable or unreasonable to provide this notification. Relevant considerations may include:

- the possible adverse consequences for the individual if they are not notified of the source
- the length of time that has elapsed since the personal information was collected by the organisation
- for personal information collected before commencement of APP 7, whether the source of the personal information was recorded
- the time and cost involved. However, an organisation is not excused from notifying an individual by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to do so will depend on whether the burden is excessive in all the circumstances.

7.47 Notification of the source of the personal information must be given within a reasonable period after the request is made (APP 7.7(b)). A 'reasonable period' would generally be 30 days unless special circumstances apply.

Interaction with other legislation

7.48 The Spam Act 2003 (Spam Act) and the Do Not Call Register Act 2006 (DNCR Act) contain specific provisions regarding direct marketing. Where the act or practice of an APP entity is subject to the Spam Act, DNCR Act, or other legislation prescribed under the regulations, APP 7 does not apply to the extent that this legislation applies (APP 7.8).

7.49 If an organisation that is an APP entity is exempt or partially exempt from the Spam Act or DNCR Act, APP 7 will still apply to the acts and practices of that organisation to the extent of that exemption.

Chapter 8:

Australian Privacy Principle 8 — Cross-border disclosure of personal information

Version 1.3, October 2025

OAIC

Contents

Key points 3
What does APP 8 say? 3
'Overseas recipient' 4
When does an APP entity 'disclose' personal information about an individual to an overseas recipient? 4
Providing personal information to a contractor 5
Taking reasonable steps to ensure an overseas recipient does not breach the APPs 6
Exception 1 — Disclosing personal information to an overseas recipient that is subject to a substantially similar law or binding scheme 8
Reasonable belief 8
Law or binding scheme 8
Substantially similar to 9
Mechanisms to enforce privacy protections 9
Exception 2 — Disclosing personal information to an overseas recipient where the country or a binding scheme is prescribed by regulations 10
Exception 3 — Disclosing personal information to an overseas recipient with the individual's consent after the individual is expressly informed 10
Expressly inform 10
Consent 11
Exception 4 — Disclosing personal information to an overseas recipient as required or authorised by law 12
Exception 5 — Disclosing personal information to an overseas recipient where a permitted general situation exists 12
Lessening or preventing a serious threat to life, health or safety 12
Taking appropriate action in relation to suspected unlawful activity or serious misconduct 13
Locating a person reported as missing 13
Necessary for a diplomatic or consular function or activity 13
Necessary for certain Defence Force activities outside Australia 13
Exception 6 — Disclosing personal information to an overseas recipient as required or authorised under an international agreement relating to information sharing 14
Exception 7 — Disclosing personal information to an overseas recipient for an enforcement related activity 15
When is an APP entity accountable for personal information that it discloses to an overseas recipient? 15
Overseas acts or practices required by a foreign law 16

Key points

- Before an APP entity discloses personal information to an overseas recipient, the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs (other than APP 1) 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. The framework generally requires an APP entity to ensure that an overseas recipient will handle an individual's personal information in accordance with the APPs, and makes the APP entity accountable if the overseas recipient mishandles the information.[1] This reflects a central object of the Privacy Act, to facilitate the free flow of information across national borders while ensuring that the privacy of individuals is respected (s 2A(f)).

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 such steps as are reasonable in the circumstances to ensure that the recipient does not breach the APPs in relation to that information. Where an 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 8.20–8.59 below).

8.4 When an APP entity discloses personal information to an overseas recipient it will also need to comply with APP 6.1. That is, it must only disclose the personal information for the primary purpose for which it was collected unless the individual has consented to the disclosure or an exception to that principle applies (see Chapter 6 (APP 6)). A note to APP 6.1 cross-references the requirements for the cross-border disclosure of personal information in APP 8. It is implicit in this note, that APP 8 only applies to personal information covered by APP 6. That is, it only applies to personal information 'held' by an APP entity. The term 'holds' is discussed in Chapter B (Key concepts).

[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 <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 <https://www.oecd.org>.

‘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 distinguished from the case where an APP entity in Australia sends personal information to a ‘related body corporate’ located outside of Australia.[3] 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.[4]

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.

8.8 An APP entity discloses personal information where it makes it accessible to others outside the entity and releases the subsequent handling of the information from its effective control. The release of the information may be a proactive release or publication, a release in response to a specific request, an accidental release or an unauthorised release by an employee.[5] This focuses on the act done by the disclosing party. The state of mind or intentions of the recipient does not affect the act of disclosure. Further, there will be a disclosure in these circumstances even where the information is already known to the overseas recipient.

8.9 In the context of APP 8, an APP entity will disclose personal information to an overseas recipient where it, for example:

- shares the personal information with an overseas recipient
- reveals the personal information at an international conference or meeting overseas

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

[3] Section 6(8) provides ‘for the purposes of this Act, the question whether bodies corporate are related to each other is determined in the manner in which that question is determined under the Corporations Act 2001.’

[4] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 states ‘APP 8 will apply where an organisation sends personal information to a ‘related body corporate’ located outside Australia’ (p 83). While s 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.

[5] An APP entity is taken to have ‘disclosed’ personal information where an employee carries out an unauthorised disclosure ‘in the performance of the duties of the person’s employment’ (s 8(1)).

- sends a hard copy document or email containing an individual's personal information to an overseas client, or
- publishes the personal information on the internet, whether intentionally or not, and it is accessible to an overseas recipient.

8.10 '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 personal information. Examples include unauthorised access following a cyber-attack[6] or a theft, including where the third party then makes that personal information available to others outside the entity.[7] 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 personal information from unauthorised access (see Chapter 11 (APP 11)), and
- 'use'. An APP entity uses personal information where it handles, or undertakes an activity with the personal information, within the entity's effective control. For example, where an entity provides personal information to an overseas recipient, via a server in a different overseas location, there would not usually be a disclosure until the personal information is able to be accessed or modified by the overseas recipient. That is, routing personal information, in transit, through servers located outside Australia, would usually be considered a 'use'.[8] In limited circumstances, the provision of personal information to a contractor may also be a 'use' of that personal information (see paragraphs 8.12–8.15 below).

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

Providing personal information to a contractor

8.12 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 personal information.[9]

8.13 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

[6] See OAIC, Sony PlayStation Network / Qriocity: Own Motion Investigation Report, September 2011, OAIC website <https://www.oaic.gov.au>.

[7] The actions of an employee will be attributed to the APP entity where it was carried out 'in the performance of the duties of the person's employment' (s 8(1)).

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

[9] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.

- 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, or
- 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).

8.14 However, in limited circumstances providing personal information to an overseas contractor to perform services on behalf of the APP entity may be a use, rather than a disclosure. This occurs where the entity does not release the subsequent handling of personal information from its effective control. 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 performing the services of storing and ensuring the entity may access the personal information, this may be a 'use' by the entity in the following circumstances:

- a binding contract between the entity and the provider requires the provider only to handle the personal information for these limited purposes
- the contract requires any subcontractors to agree to the same obligations, and
- the contract gives the entity effective control of how the personal information is handled by the overseas recipient. Issues to consider include whether the entity retains the right or power to access, change or retrieve the personal information, who else will be able to access the personal information and for what purposes, what type of security measures will be used for the storage and management of the personal information (see also APP 11.1, Chapter 11) and whether the personal information can be retrieved or permanently deleted by the entity when no longer required or at the end of the contract.[10]

8.15 Where the provision of personal information to an overseas contractor is a use, an APP entity may breach the APPs if the information is mishandled while in the overseas contractor's physical possession. This is because the APP entity is considered to still 'hold' the information (as it has effective control of the information), and a number of APPs apply to an entity that 'holds' personal information ('holds' is discussed in Chapter B (Key Concepts)).

Taking reasonable steps to ensure an overseas recipient does not breach the APPs

8.16 The requirement in APP 8.1 to ensure that an overseas recipient does not breach the APPs is qualified by a 'reasonable steps' test. It is generally expected that an APP entity will 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).[11] 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

[10] For further discussion of cloud computing considerations for agencies, see Secure Cloud Strategy, Digital Transformation Agency website <https://www.dta.gov.au>.

[11] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.

information. This should also require the overseas recipient to enter a similar contractual arrangement with any third parties to whom it discloses the personal information (for example, a subcontractor)

- the complaint handling process for privacy complaints, and
- a requirement that the recipient implement a data breach response plan which includes a mechanism for notifying the APP 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).[12]

8.17 However, whether reasonable steps to ensure the overseas recipient does not breach the APPs requires a contract to be entered into, the terms of the contract, and the steps the APP entity takes to monitor compliance with any contract (such as auditing), will depend upon the circumstances that include:

- the sensitivity of the personal information. More rigorous steps may be required 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 entity's relationship with the overseas recipient. More rigorous steps may be required if an entity discloses information to an overseas recipient to which it has not previously disclosed personal information
- the possible adverse consequences for an individual if the information is mishandled by the overseas recipient. More rigorous steps may be required as the risks and adverse consequences increase.
- existing technical and operational safeguards implemented by the overseas recipient which will protect the privacy of the personal information — more rigorous steps may be required where the recipient has limited safeguards in place, and
- the practicability, including time and cost involved. However, an entity is not excused from ensuring that an overseas recipient does not breach the APPs 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.

8.18 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. 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 will generally satisfy the requirement in APP 8.1.

8.19 There are exceptions to the requirement in APP 8.1 and to the accountability provision in s 16C (see paragraphs 8.2020–8.5959 below).

[12] See OAIC, Data Breach Preparation and Response, OAIC website <https://www.oaic.gov.au>.

Exception 1 — Disclosing personal information to an overseas recipient that is subject to a substantially similar law or binding scheme

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

Reasonable belief

8.21 The term 'reasonably believe' is discussed in Chapter B (Key concepts). In summary, an APP entity must have a reasonable basis for its belief, and not merely a genuine or subjective belief. For example, this might be based on independent legal advice. It is the responsibility of an APP entity to be able to justify its reasonable belief.

Law or binding scheme

8.22 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, or
- subject to Binding Corporate Rules (BCRs). BCRs allow multinational corporations, international organisations and groups of companies to make intra-organisational transfers of personal information across borders in compliance with EU Data Protection law.[13] BCRs typically form a stringent, intra-corporate global privacy policy that satisfies EU standards. The Article 29 Working Party issued several guidance documents on BCR content, acceptance criteria and submission process.[14]

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

[13] European Commission website <https://ec.europa.eu/info/law/law-topic/data-protection_en>.

[14] Available at European Commission website <https://ec.europa.eu/info/law/law-topic/data-protection_en>. See in particular documents WP 133 (2007), WP 153 (2008), WP 154 (2008), WP 155 (2008).

- 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, or
- the recipient can opt out of the binding scheme without notice and without returning or destroying the personal information.

Substantially similar to

8.24 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.

8.25 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 personal information disclosed to the recipient
- 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, and
- the law or scheme includes a right to access and seek correction of personal information.

Mechanisms to enforce privacy protections

8.26 An enforcement mechanism should meet two key requirements: it should be accessible to the individual and it should have effective powers to enforce the privacy or data protections in the law or binding scheme. A range of mechanisms may satisfy those requirements, ranging from a regulatory body similar to the Office of the Australian Information Commissioner (the OAIC), to an accredited dispute resolution scheme, an independent tribunal or a court with judicial functions and powers. Factors that may be relevant in deciding whether there is an accessible and effective enforcement mechanism include whether the mechanism:

- is independent of the overseas recipient that is required by the law or binding scheme to comply with the privacy or data protections
- has authority to consider a breach of any of the privacy or data protections in the law or binding scheme
- is accessible to an individual, for example, the existence of the scheme is publicly known, and can be accessed by individuals directly and without payment of any unreasonable charge
- has the power to make a finding that the overseas recipient is in breach of the law or binding scheme and to provide a remedy to the individual
- is required to operate according to principles of procedural fairness.

8.27 The mechanism may be a single mechanism or a combination of mechanisms. It may be established by the law or binding scheme that contains the privacy or data protections, or by another law or binding scheme. Alternatively, the mechanism may take effect through the operation of cross-border enforcement arrangements between the OAIC and an appropriate regulatory authority in the foreign jurisdiction.[15]

Exception 2 — Disclosing personal information to an overseas recipient where the country or a binding scheme is prescribed by regulations

8.28 An APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where the overseas recipient of the relevant personal information is:

- subject to the laws of a country prescribed by regulations, or a participant in a binding scheme prescribed by regulations,[16] and
- if the country or binding scheme is prescribed subject to conditions, those conditions are satisfied.[17]

8.29 Laws and binding schemes are discussed above at paragraphs 8.22–8.23.

8.30 The Governor-General may make regulations under the Privacy Act to prescribe these matters.[18]

Exception 3 — Disclosing personal information to an overseas recipient with the individual's consent after the individual is expressly informed

8.31 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

8.32 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

[15] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.

[16] See the Federal Register of Legislation for up-to-date versions of the regulations made under the Privacy Act.

[17] This exception was introduced by the *Privacy and Other Legislation Amendment Act 2024*. It applies to information disclosed from 11 December 2024 regardless of whether the information was acquired or created before or after that date.

[18] See the Federal Register of Legislation for up-to-date versions of regulations made under the Privacy Act.

explain that if the individual consents to the disclosure and the overseas recipient handles the personal information in breach of the APPs:

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

8.33 The statement should also:

- be made at the time consent is sought, and
- not rely on assumed prior knowledge of the individual.

8.34 The statement could also explain any other practical effects or risks associated with the disclosure that the APP entity is aware of, or would be reasonably expected to be aware of. These may include that:

- the overseas recipient may not be subject to any privacy obligations or to any principles similar to the APPs
- the individual may not be able to seek redress in the overseas jurisdiction, and
- the overseas 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

8.35 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 individual is adequately informed before giving consent (in this case 'expressly informed')
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent.

8.36 An APP entity does not need to obtain consent before every proposed cross-border disclosure.[19] 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.

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

[19] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 84.

Exception 4 — Disclosing personal information to an overseas recipient as required or authorised by law

8.38 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 paragraphs 8.64–8.68 below). The meaning of 'required or authorised by or under an Australian law or a court/tribunal order' is discussed in Chapter B (Key concepts).

8.39 The following are examples of where a law or order may require or authorise disclosure of personal information to an overseas recipient in specific circumstances:

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

8.40 An agency that intends to rely on this exception could 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 that provide privacy protections comparable to the APPs (see discussion of contractual measures in paragraphs 8.16–8.18 above).

Exception 5 — Disclosing personal information to an overseas recipient where a permitted general situation exists

8.41 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 disclosure. 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

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

- it is unreasonable or impracticable to obtain the individual's consent to the disclosure, and
- 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 (s 16A(1), Item 1)

8.43 For example, this permitted general situation 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

8.44 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).

8.45 For example, this permitted general situation 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 person reported as missing

8.46 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) (s 16A(1), Item 3).

Necessary for a diplomatic or consular function or activity

8.47 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). The permitted general situation applies only to agencies, and not to organisations.

8.48 For example, this permitted general situation 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, where assistance is required with repatriation in the case of death or serious illness, or to provide assistance in response to a crisis or emergency overseas.

Necessary for certain Defence Force activities outside Australia

8.49 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).

8.50 For example, this permitted general situation 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.

Exception 6 — Disclosing personal information to an overseas recipient as required or authorised under an international agreement relating to information sharing

8.51 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)). This exception does not apply to organisations.

8.52 The term 'international agreement' is not defined in the Privacy Act. This guideline clarifies that the term includes documents binding at international law (for example, treaties and conventions), as well as other formal written documents not binding at international law (for example, a memorandum of understanding or an official exchange of letters[20]) that provide for information sharing between an agency and an overseas recipient. This exception applies only to such documents where the parties are Australia and one or more foreign states, although the overseas recipient of shared information may be a non-state entity.

8.53 Information sharing may not be the only or the primary subject of the agreement, so long as the agreement makes provision for 'information sharing'. Additionally, the disclosure of personal information to the overseas recipient must be 'required or authorised' by or under the agreement.

8.54 To meet those requirements, the agreement should make specific arrangements for disclosure of information to an overseas recipient, including identifying the agency and the overseas recipient, the categories of personal information that may be disclosed to the recipient under the agreement and the circumstances in which or the purposes for which the information will be disclosed. This exception is unlikely to apply to an agreement that contains only a general commitment by the parties to facilitate, or remove obstacles to, the disclosure or exchange of information (the terms 'required' and 'authorised' are discussed in more detail in Chapter B (Key concepts)).

8.55 The agreement could also include provisions dealing with the responsibility of the parties to ensure adequate protection of the personal information that is disclosed according to standards comparable to those in the APPs, and the procedure to be followed to ensure that obligations or undertakings imposed by the agreement are met. The discussion of contractual measures in paragraphs 8.16–8.18 above lists other matters that could be considered for inclusion the agreement.

[20] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 84.

Exception 7 — Disclosing personal information to an overseas recipient for an enforcement related activity

8.56 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))

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

8.58 'Enforcement body' is defined in s 6(1) as a list of specific bodies and is discussed in Chapter B (Key concepts). 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 Prudential Regulation Authority, Australian Securities and Investments Commission and AUSTRAC.

8.59 '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 (APP 6).

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

8.60 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)).

8.61 This accountability provision 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 the overseas recipient in relation to the personal information (for more information about when the APPs will apply see Chapter A (Introductory matters)), and
- an act or practice by the overseas recipient would breach the APPs (other than APP 1) if they had applied (s 16C(1)).

8.62 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,[21] or
- the overseas recipient inadvertently breaches the APPs in relation to the information.

8.63 However, an APP entity will not be accountable where, for example, it discloses personal information to an overseas recipient under an exception in APP 8.2 (see paragraphs 8.20–8.59 above), or where personal information is disclosed to an overseas recipient with an 'Australian link'. A recipient that has an 'Australian link' will be covered by the Privacy Act. 'Australian link' is defined in s 5B(2) and discussed in more detail in Chapter B (Key concepts).

Overseas acts or practices required by a foreign law

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

8.65 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.

8.66 For example, the USA PATRIOT Act may require the overseas recipient to disclose personal information to the Government of the United States of America.[22] In these circumstances, the APP entity would not be responsible under the accountability provision for the disclosure required by that Act.

8.67 An APP entity could 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, particularly if the entity usually discloses personal information to overseas recipients (see APP 5.2(i), Chapter 5), or in its APP Privacy Policy (see Chapter 1 (APP 1)).

8.68 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.

[21] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 84.

[22] See Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT ACT) of 2001 (USA).

Chapter 9:

Australian Privacy Principle 9 —

Adoption, use or disclosure of government related identifiers

Version 1.1, July 2019

OAIC

Contents

Key points **3**

What does APP 9 say? **3**

'Government related identifier' **3**

'Identifiers' 3

'Government related identifiers' 4

When are agencies covered by APP 9? **4**

Adopting government related identifiers **5**

'Adoption' 5

Adopting a government related identifier as required or authorised by or under an Australian law or a court/tribunal order 5

Adopting a government related identifier as prescribed by regulations 6

Using and disclosing government related identifiers **6**

Using or disclosing a government related identifier where reasonably necessary to verify the identity of the individual 6

Using or disclosing a government related identifier where reasonably necessary to fulfil obligations to an agency or a State or Territory authority 7

Using or disclosing a government related identifier as required or authorised by or under an Australian law or a court/tribunal order 7

Using or disclosing a government related identifier where a permitted general situation exists 8

Using or disclosing a government related identifier to an enforcement body for enforcement related activities 8

Using or disclosing a government related identifier as prescribed by regulations 9

Key points

- APP 9 restricts the adoption, use and disclosure of government related identifiers by organisations. APP 9 may also apply to some agencies in the circumstances set out in s 7A.
- An identifier is a number, letter or symbol, or a combination of any or all of those things, that is used to identify the individual or to verify the identity of the individual.
- A government related identifier is an identifier that has been assigned by an agency, a State or Territory authority, an agent of an agency or authority, or a contracted service provider for a Commonwealth or State contract.
- Where an identifier, including a government related identifier, is personal information, it must be handled in accordance with the APPs.
- An organisation must not adopt a government related identifier of an individual as its own identifier of the individual, unless an exception applies.
- An organisation must not use or disclose a government related identifier of an individual, unless an exception applies.

What does APP 9 say?

9.1 An organisation must not adopt, use or disclose a government related identifier unless an exception applies. APP 9 may apply to an agency in the circumstances set out in s 7A (see paragraphs 9.10–9.11 below).

9.2 The objective of APP 9 is to restrict general use of government related identifiers by organisations so that they do not become universal identifiers. That could jeopardise privacy by enabling personal information from different sources to be matched and linked in ways that an individual may not agree with or expect.

9.3 An individual cannot consent to the adoption, use or disclosure of their government related identifier.

9.4 APP 9 restricts how an organisation is permitted to handle government related identifiers, irrespective of whether a particular identifier is the personal information of an individual. An identifier will be personal information if the individual is identifiable or reasonably identifiable from the identifier, including from other information held by, or available to, the entity that holds the identifier. If it is personal information, the identifier must be handled by the entity in accordance with other APPs. 'Personal information' is discussed in more detail in Chapter B (Key concepts), including examples of when an individual may be 'reasonably identifiable'.

'Government related identifier'

'Identifiers'

9.5 An 'identifier' of an individual is defined in s 6(1) as a number, letter or symbol, or a combination of any or all of those things, that is used to identify the individual or to verify the identity of the individual.

9.6 The following are explicitly excluded from the definition of identifier:

- an individual's name
- an individual's Australian Business Number (ABN)
- anything else prescribed by the regulations made under the Privacy Act.[1] This provides flexibility to exclude any specified type of identifier from the definition, and therefore the operation of APP 9, as required.

'Government related identifiers'

9.7 A 'government related identifier' of an individual is defined in s 6(1) as an identifier that has been assigned by:

- an agency
- a State or Territory authority
- an agent of an agency, or a State or Territory authority, acting in its capacity as agent, or
- a contracted service provider for a Commonwealth contract, or a State contract, acting in its capacity as contracted service provider for that contract

9.8 The following are given as examples of government related identifiers:

- Medicare numbers
- Centrelink Reference numbers
- driver licence numbers issued by State and Territory authorities
- Australian passport numbers

9.9 Some government related identifiers are regulated by other laws that restrict the way that entities can collect, use or disclose the particular identifier and related personal information. Examples include tax file numbers and individual healthcare identifiers.[2]

When are agencies covered by APP 9?

9.10 An agency must comply with the adoption, use and disclosure requirements of APP 9 when dealing with government related identifiers in the circumstances set out in s 7A.

9.11 These circumstances include where:

- the agency is listed in Part I of Schedule 2 to the Freedom of Information Act 1982 (the FOI Act) and is prescribed in regulations,[3] or
- the act or practice relates to the commercial activity of an agency that is specified in Part II of Schedule 2 to the FOI Act[4]

---

[1] See the Federal Register of Legislation <https://www.legislation.gov.au> for up-to-date versions of the regulations made under the Privacy Act.

[2] For more information about the legislative regimes, visit the OAIC's Tax File Numbers page and Healthcare Identifiers page <https://www.oaic.gov.au>.

[3] See the Federal Register of Legislation <https://www.legislation.gov.au> for up to date versions of the regulations made under the Freedom of Information Act 1982.

[4] See s 7A and OAIC, FOI Guidelines, Part 2, OAIC website <https://www.oaic.gov.au>.

Adopting government related identifiers

9.12 An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless an exception applies (APP 9.1).

'Adoption'

9.13 The term 'adopt' is not defined in the Privacy Act and so it is appropriate to refer to its ordinary meaning. An organisation adopts a government related identifier if it collects a particular government related identifier of an individual and organises the personal information that it holds about that individual with reference to that identifier.

9.14 The following are examples of when an organisation will be considered to have adopted a government related identifier of an individual:

- A health service provider uses an individual's Medicare number as the basis for the provider's own identification system.
- An accountant uses an individual's tax file number as the basis of the accountant's own identification system.

9.15 Adoption is to be distinguished from merely collecting, using or disclosing a government related identifier. APP 9 does not specifically address the collection of government related identifiers. However, as noted in paragraph 9.4, if an organisation collects a government related identifier that is considered to be personal information, the organisation must comply with other APPs, including APP 3 (collection of solicited personal information) and APP 4 (dealing with unsolicited personal information). These APPs are discussed in Chapters 3 and 4 respectively.

9.16 APP 3 provides that an organisation must only collect personal information that is reasonably necessary for one or more of the organisation's functions or activities. If an organisation collects an identifier that it cannot lawfully use or disclose under APP 9.2 (see paragraphs 9.22–9.46), then the collection is not reasonably necessary for one of the organisation's functions or activities. This means that the collection would not be permitted under APP 3.2.

Adopting a government related identifier as required or authorised by or under an Australian law or a court/tribunal order

9.17 An organisation may adopt a government related identifier of an individual as its own identifier of the individual if the adoption is required or authorised by or under an Australian law or a court/tribunal order (APP 9.1(a)). The meaning of 'required or authorised by or under an Australian law or a court/tribunal order' is discussed in Chapter B (Key concepts).

9.18 The Australian law or court/tribunal order should specify a particular government related identifier, the organisations or classes of organisations permitted to adopt it, and the particular circumstances in which they may do so.

9.19 For example, healthcare providers are authorised by law to adopt the individual healthcare identifiers of their patients as their own identifier.[5] That is, they may organise the personal information of their patients by reference to the patients' individual healthcare identifiers.

Adopting a government related identifier as prescribed by regulations

9.20 An organisation may adopt a government related identifier of an individual as its own identifier of the individual if:

- the identifier is prescribed by regulations
- the organisation, or a class of organisations that includes the organisation, is prescribed by regulations, and
- the adoption occurs in the circumstances prescribed by the regulations (APP 9.1(b))

9.21 Regulations may be made under the Privacy Act to prescribe these matters.[6]

Using and disclosing government related identifiers

9.22 An organisation must not use or disclose a government related identifier of an individual, unless an exception applies (APP 9.2). The terms 'use' and 'disclosure' are discussed in Chapter B (Key concepts).

9.23 The circumstances in which an organisation may use or disclose government related identifiers under APP 9.2 are narrower in scope than the circumstances in which an organisation may use or disclose other personal information under APP 6. APP 6 does not apply to the disclosure of government related identifiers (APP 6.7(b)) (see Chapter 6 (APP 6)).

Using or disclosing a government related identifier where reasonably necessary to verify the identity of the individual

9.24 An organisation may use or disclose the government related identifier of an individual if the use or disclosure 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)).

9.25 This exception allows an organisation to use a government related identifier both to establish the identity of an individual and to verify that an individual is who or what they claim to be, for example, to verify their name or age.

9.26 Government related identifiers are usually contained in high-integrity documents, and are therefore likely to be highly reliable for verifying an individual's identity. An example is that driver licences and passports are used in some circumstances to verify the identity of individuals.

---

[5] See the Healthcare Identifiers Act 2010, s 25. 'Healthcare provider' is defined in s 5 of the Healthcare Identifiers Act 2010 <https://www.legislation.gov.au>.

[6] See the Federal Register of Legislation <https://www.legislation.gov.au> for up-to-date versions of regulations made under the Privacy Act.

9.27 The use and disclosure of the government related identifier to verify the identity of the individual must be reasonably necessary for the purposes of the organisation's functions or activities. Whether the use or disclosure is 'reasonably necessary' is an objective test. This is discussed in more detail in Chapter B (Key concepts). The functions and activities of the organisation are limited to those in which it may lawfully engage. See Chapter 3 (APP 3) for a discussion of identifying the functions and activities of an organisation.

9.28 There are a number of factors that an organisation should consider in deciding whether the use or disclosure is reasonably necessary to verify the identity of an individual. For example, it may not be reasonably necessary where:

- the organisation can carry out the function or activity without verifying the individual's identity
- there are other practicable means of verifying the individual's identity available to the organisation. For example, an organisation may be able to verify an individual's identity by using or disclosing other types of personal information, rather than the government related identifier (noting that the use and disclosure of other personal information must comply with the relevant APPs).

Using or disclosing a government related identifier where reasonably necessary to fulfil obligations to an agency or a State or Territory authority

9.29 An organisation may use or disclose a government related identifier of an individual if the use or disclosure is reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority (APP 9.2(b)).

9.30 This exception is most likely to be relevant to a contracted service provider, and will allow them to use or disclose a government related identifier if this is reasonably necessary to perform a Commonwealth or State or Territory contract.[7] Whether the use or disclosure is 'reasonably necessary' is an objective test. This is discussed in more detail in Chapter B (Key concepts).

Using or disclosing a government related identifier as required or authorised by or under an Australian law or a court/tribunal order

9.31 An organisation may use or disclose a government related identifier of an individual if the use or disclosure is required or authorised by or under an Australian law or a court/tribunal order (APP 9.2(c)).

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

9.33 The Australian law or court/tribunal order should specify a particular government related identifier, the organisations or classes of organisations permitted to use or disclose it, and the particular circumstances in which they may do so.

[7] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 84.

9.34 For example, the Healthcare Identifiers Act 2010 permits the use or disclosure of healthcare identifiers for limited purposes by healthcare providers and other entities specified in that Act.

Using or disclosing a government related identifier where a permitted general situation exists

9.35 An organisation may use or disclose a government related identifier of an individual if a 'permitted general situation' (other than the situations referred to in Items 3, 4 or 5 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the identifier (APP 9.2(d)).

9.36 Section 16A lists two permitted general situations that apply to the use or disclosure of government related identifiers. The two situations are set out below, and are discussed in Chapter C (Permitted general situations) (including the meaning of relevant terms).

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

9.37 An organisation may use or disclose a government related identifier of an individual if:

- the organisation reasonably believes the use or 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).

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

9.38 An organisation may use or disclose a government related identifier of an individual if:

- the organisation has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the organisation's functions or activities has been, is being or may be engaged in, and
- the organisation reasonably believes that the use or disclosure is necessary in order for the organisation to take appropriate action in relation to the matter (s 16A(1), Item 2).

9.39 For example, this permitted general situation might apply where the organisation uses or discloses a government related identifier, such as a customer's Centrelink number, as part of an investigation into suspected fraud by a client in relation to the organisation's functions or activities.

Using or disclosing a government related identifier to an enforcement body for enforcement related activities

9.40 An organisation may use or disclose a government related identifier of an individual if the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body (APP 9.2(e)).

9.41 An organisation that collects or holds a government related identifier will be able to rely on this exception to cooperate with relevant enforcement bodies in certain circumstances.

9.42 '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,[8] the Integrity Commissioner,[9] the Immigration Department,[10] Australian Prudential Regulation Authority, Australian Securities and Investments Commission and AUSTRAC.

9.43 'Enforcement related activities' is defined in s 6(1) and discussed in Chapter B (Key concepts). 'Reasonably believes', 'reasonably necessary' and 'enforcement body' are also discussed in Chapter B (Key concepts). For further discussion of a similar exception in APP 6.2(e), see Chapter 6.

9.44 For example, this exception might apply where the Australian Federal Police are investigating fraud committed by an individual against the organisation. The organisation may reasonably believe that disclosure of a copy of a driver licence to the AFP is reasonably necessary for the AFP's investigation, where the AFP needed to obtain information provided by that individual to the organisation.

Using or disclosing a government related identifier as prescribed by regulations

9.45 An organisation may use or disclose a government related identifier of an individual if:

- the identifier is prescribed by regulations
- the organisation, or a class of organisations that includes the organisation, is prescribed by regulations, and
- the adoption occurs in the circumstances prescribed by the regulations (APP 9.2(f))

9.46 Regulations may be made under the Privacy Act to prescribe these matters.[11]

[8] In July 2016, the former Australian Crime Commission and CrimTrac were merged to form the Australian Criminal Intelligence Commission.

[9] 'Integrity Commissioner' is defined in s 6(1) as having the same meaning as in the Law Enforcement Integrity Commissioner Act 2006.

[10] 'Immigration Department' is defined in s 6(1) as the Department administered by the Minister administering the Migration Act 1958. This is now the Department of Home Affairs.

[11] See the Federal Register of Legislation <https://www.legislation.gov.au> for up-to-date versions of regulations made under the Privacy Act.

Chapter 10:

Australian Privacy Principle 10 —

Quality of personal information

Version 1.1, July 2019

OAIC

Contents

Key points 3
What does APP 10 say? 3
When an APP entity must take reasonable steps to ensure the quality of personal information 3
Taking reasonable steps 3
Examples of reasonable steps 4
What are the quality considerations? 5
Accurate 5
Up-to-date 6
Complete 6
Relevant 6
Interaction with other APPs 6
APP 3 (collection of solicited personal information) 7
APP 11 (security of personal information) 7
APP 12 (access to personal information) and APP 13 (correction of personal information) 7

Key points

- An APP entity must take reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete.
- An APP entity must take reasonable steps to ensure that the personal information it uses and discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

What does APP 10 say?

10.1 An APP entity must take reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete (APP 10.1).

10.2 An APP entity must also take reasonable steps to ensure that the personal information it uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant (APP 10.2). It is implicit that this requirement only applies to personal information 'held' by an entity (see Chapter 6 (APP 6)). 'Holds' is discussed in Chapter B (Key concepts).

10.3 Handling poor quality personal information can have significant privacy impacts for individuals. The requirements in APP 10 ensure that an APP entity takes reasonable steps to only handle high quality personal information, which builds community trust and confidence in an entity's information handling practices.

When an APP entity must take reasonable steps to ensure the quality of personal information

10.4 An APP entity must take reasonable steps to ensure the quality of personal information at two distinct points in the information handling cycle. The first is at the time the information is collected. The second is at the time the information is used or disclosed.

10.5 Regular reviews, at other times, of the quality of personal information held by the APP entity may also assist in ensuring it is accurate, up-to-date, complete and relevant at the time it is used or disclosed.

Taking reasonable steps

10.6 The reasonable steps that an APP entity should take will depend upon circumstances that include:

- the sensitivity of the personal information. More rigorous steps may be required if the information collected, used or disclosed 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 APP entity holding the personal information. Relevant considerations include an entity's size, resources and its business model. For example, the reasonable steps expected of an entity that operates through franchises or dealerships, or gives

database and network access to contractors, may differ from the reasonable steps required of a centralised entity.

- the possible adverse consequences for an individual if the quality of personal information is not ensured. More rigorous steps may be required as the risk of adversity increases.
- the practicability, including time and cost involved. However an entity is not excused from taking particular steps 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.

10.7 In some circumstances it will be reasonable for an APP entity to take no steps to ensure the quality of personal information. For example, where an entity collects personal information from a source known to be reliable (such as the individual concerned) it may be reasonable to take no steps to ensure the quality of personal information. It is the responsibility of the entity to be able to justify that this is reasonable.

Examples of reasonable steps

10.8 The following are given as examples of reasonable steps that an APP entity could consider:

- implementing internal practices, procedures and systems to audit, monitor, identify and correct poor quality personal information (including training staff in these practices, procedures and systems). For example, if the entity commonly uses or discloses personal information in time-critical situations such that it may not be possible to take steps to ensure quality at the time of the use or disclosure, the entity might take steps to ensure the quality of personal information at regular intervals
- implementing protocols that ensure personal information is collected and recorded in a consistent format. For example, to help assess whether personal information is up-to-date, an entity might, where practicable, note on a record when the personal information was collected and the point in time to which it relates, and if it is an opinion, that fact
- ensuring updated or new personal information is promptly added to relevant existing records
- providing individuals with a simple means to review and update their personal information on an on-going basis, for example through an online portal
- reminding individuals to update their personal information each time the entity engages with the individual
- contacting the individual to verify the quality of personal information when it is used or disclosed, particularly if there has been a lengthy period since collection
- checking that a third party, from whom personal information is collected, has implemented appropriate practices, procedures and systems to ensure the quality of personal information. Depending on the circumstances, this could include:
    - making an enforceable contractual arrangement to ensure that the third party implements appropriate measures to ensure the quality of personal information the entity collects from the third party

  - undertaking due diligence in relation to the third party's quality practices prior to the collection
- if personal information is to be used or disclosed for a new purpose that is not the primary purpose of collection, assessing the quality of the personal information having regard to that new purpose before the use or disclosure.

What are the quality considerations?

10.9 The three terms listed in APPs 10.1 and 10.2, 'accurate', 'up-to-date', 'complete', and the additional term in APP 10.2, 'relevant', are not defined in the Privacy Act. These terms are also listed in APP 13.1, which deals with the correction of personal information held by an APP entity.[1]

10.10 The following analysis of each term draws on the ordinary dictionary meaning of the terms, as well as case law concerning the meaning of those terms in the Privacy Act, Freedom of Information Act 1982 (FOI Act) and other legislation.[2] As the analysis indicates, there is overlap in the meaning of the terms.

10.11 In applying the terms to the use and disclosure of personal information, it is necessary to have regard to 'the purpose of the use or disclosure' (APP 10.2). This is also a necessary consideration when applying these terms to the collection of personal information (see paragraph 10.21 below). That is, personal information may be of poor quality having regard to one purpose for which it is collected, used or disclosed, but not another. 'Purpose' is discussed in Chapter B (Key concepts).

Accurate

10.12 Personal information is inaccurate if it contains an error or defect. Personal information is also inaccurate if it is misleading.[3] An example is incorrect factual information about a person's name, date of birth, residential address or current or former employment.

10.13 An opinion about an individual given by a third party is not inaccurate by reason only that the individual disagrees with that opinion or advice.[4] For APP 10 purposes, the opinion may be 'accurate' if it is presented as an opinion and not objective fact, it accurately records the view held by the third party, and is an informed assessment that takes into account competing facts and views. Other matters to consider under APP 10, are whether the opinion is 'up-to-date', 'complete', 'not misleading' or 'relevant'.

10.14 In relation to a similar issue, s 55M of the FOI Act provides that the Information Commissioner (in conducting an Information Commissioner review) cannot alter a record of opinion unless satisfied that it was based on a mistake of fact, or the author of the opinion

[1] Similar terms are used also in Part V of the Freedom of Information Act 1982 concerning a person's right to apply to an agency to amend or annotate personal information.

[2] See OAIC, FOI Guidelines, Part 7 — Amendment and Annotation of Personal Records, OAIC website <https://www.oaic.gov.au>; and 'S' and Veda Advantage Information Services and Solutions Limited [2012] AICmr 33 (20 December 2012).

[3] See Australian Government June 2010, Companion Guide: Australian Privacy Principles, Parliament of Australia website <https://www.aph.gov.au>, p 14.

[4] The definition of 'personal information' includes 'information or an opinion' (s 6(1)).

was biased, unqualified to form the opinion or acted improperly in conducting the factual inquiries that led to the formation of the opinion.

Up-to-date

10.15 Personal information is out-of-date if it contains facts, opinions or other information that is no longer current. An example is a statement that an individual lacks a particular qualification or accreditation that the individual has subsequently obtained.

10.16 Personal information about a past event may have been accurate at the time it was recorded, but has been overtaken by a later development. Whether that personal information is out-of-date will depend on the purpose for which it is collected, used or disclosed. If current personal information is required for the particular purpose, the personal information will, to that extent, be out-of-date. Personal information held by an APP entity that is no longer needed for any purpose, may need to be destroyed or de-identified under APP 11.2 (Chapter 11 (APP 11)).

Complete

10.17 Personal information is incomplete if it presents a partial or misleading picture, rather than a true or full picture. An example is a tenancy database which records that a tenant owes a debt, which in fact has since been repaid. The personal information will be incomplete under APP 10 if the tenancy database is used or disclosed for the purpose of providing members with personal information about defaults on tenant agreements.[5] Similarly, a statement that a person has only two rather than three children will be incomplete under APP 10 if that personal information is used for the purpose of, and is relevant to, assessing a person's eligibility for a benefit or service.

10.18 Where an APP entity is required to collect additional personal information to ensure that the information is complete, having regard to the purpose for which the information is collected, used or disclosed, the collection of that information will be reasonably necessary for the entity's functions or activities (see Chapter 3 (APP 3)).

Relevant

10.19 Personal information is irrelevant if it does not have a bearing upon or connection to the purpose for which the personal information is used or disclosed. An example is an APP entity that holds personal information about a client collected for the purpose of providing financial advice. If the entity later discloses personal information to purchase shares on the client's behalf, it should only disclose parts of the personal information relevant to that secondary purpose.

Interaction with other APPs

10.20 The requirements in APP 10 to take reasonable steps to ensure the quality of personal information are complemented by other requirements in APP 3 (collection of solicited

[5] For further discussion of reasonable steps in these circumstances, see Tenants' Union of Queensland Inc, Tenants' Union of NSW Co-op Ltd and complainants C, D, E, F and G v TICA Default Tenancy Control Pty Ltd [2004] PrivCmrACD 2 (16 April 2004).

personal information), APP 11 (security of personal information), APP 12 (access to personal information) and APP 13 (correction of personal information).

APP 3 (collection of solicited personal information)

10.21 APP 10.1 does not specifically require an APP entity to take reasonable steps to ensure that the personal information it collects is relevant to the purpose of collection. However, this requirement is implied in APP 3. Under APP 3, an APP entity must only collect personal information which is reasonably necessary for 'one or more of the entity's functions or activities'. Agencies may, in addition, collect personal information that is directly related to one or more of the agency's functions or activities. For sensitive information, an entity will also need the individual's consent, unless an exception applies (see Chapter 3 (APP 3)).

APP 11 (security of personal information)

10.22 Where an APP entity amends personal information or adds new personal information to a record to comply with APP 10, it should consider whether it needs to take action under APP 11 to destroy or de-identify other personal information that it holds (for example a copy of that information). APP 11 requires an APP entity to take reasonable steps to destroy or de-identify personal information that it no longer needs, unless it is contained in a Commonwealth record or the entity is required by or under an Australian law, or a court/tribunal order, to retain it (see Chapter 11 (APP 11)).

APP 12 (access to personal information) and APP 13 (correction of personal information)

10.23 APPs 12 and 13 can support an APP entity in meeting its obligation under APP 10 to ensure the quality of personal information that it collects, uses and discloses. Providing an individual with access to their personal information under APP 12 will allow the individual to identify whether any personal information is inaccurate, out-of-date, incomplete or irrelevant. Similarly, taking reasonable steps to correct incorrect personal information at the request of an individual under APP 13 can also enhance the quality of that information.

10.24 APP 13 also requires an APP entity to take reasonable steps to correct personal information where an APP entity is satisfied, independently of any request, that personal information it holds, is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to a purpose for which the information is held (see Chapter 13 (APP 13)).

10.25 In addition to responding to requests for access and correction under APPs 12 and 13, an APP entity should proactively provide individuals with a simple means to access and update their personal information on an on-going basis (see paragraph 10.8 above).

Chapter 11:

Australian Privacy Principle 11 —

Security of personal information

Version 1.3, October 2025

OAIC

Contents

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

Key points

- An APP entity must take such steps as are reasonable in the circumstances to protect the 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 such steps as are reasonable in the circumstances 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 or under an Australian law or a court/tribunal order to retain the personal information.
- Reasonable steps include technical and organisational measures.
- 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 in the circumstances 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 or under an Australian law or a court/tribunal order to retain the personal information (APP 11.2).

11.4 The reasonable steps an APP entity must take, for the purposes of ensuring the security of personal information and destroying or de-identifying personal information that is no longer needed, include technical and organisational measures (APP 11.3).[3]

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

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

[3] APP 11.3 was introduced by the *Privacy and Other Legislation Amendment Act 2024*. APP 11.3 applies to personal information held from 11 December 2024, regardless of whether the information was acquired or created before or after this date. APP 11.3 does not limit APP 11.1, APP 11.2 or any other provision in the Privacy Act.

‘Holds’

11.5 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)).

11.6 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.

11.7 The term ‘holds’ is discussed in more detail in Chapter B (Key concepts).

Taking reasonable steps to ensure the security of personal information

11.8 The ‘reasonable steps’ that an APP entity must take to ensure the security of personal information will depend upon circumstances, including:

- 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 risks and adverse consequences increase
- 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, and
- 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)).

11.9 In all cases, reasonable steps should include taking steps and implementing strategies in relation to the following:

- governance, culture and training
- internal policies, procedures and systems
- ICT security
- access security

- third party providers (including cloud computing)
- data breaches
- physical security
- destruction and de-identification, and
- standards.

11.10 The reasonable steps an APP entity must take for the purposes of ensuring the security of personal information include both technical and organisational measures (APP 11.3).

11.11 Technical and organisational measures work together within a broader organisational framework to protect personal information and mitigate information security and cyber security risks.

11.12 Technical measures include protecting personal information by implementing technological controls and physical measures relating to software and hardware. Examples of technical measures may include (but are not limited to) securing access to premises, encrypting data, anti-virus software and strong passwords. [4]

11.13 Organisational measures involve implementing policies, processes and procedures to protect the security of information. Examples of organisational measures may include (but are not limited to) staff training on privacy and security obligations, developing standard operating procedures and policies for securing personal information.[5]

11.14 Some steps may encompass a combination of technical and organisational aspects, as technical and organisational measures complement each other and overlap. For example, physical security measures such as security systems, alarms or keycards are technical measures as they involve restricting physical access to personal information. These physical security measures can also be organisational measures where there are policies, procedures and practices for managing how staff access and use physical spaces and information assets.

11.15 As part of taking reasonable steps to protect personal information (also known as 'personal information security') an APP entity should implement technical and organisational measures, using a layered approach to avoid a single point of failure.

11.16 An APP entity should also 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.

11.17 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.[6]

---

[4] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth), paragraph 101.

[5] Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth), paragraph 102.

[6] 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.

What are the security considerations?

11.18 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

11.19 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).

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

Interference

11.21 '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

11.22 '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.

11.23 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.

11.24 However, it does not apply to intentional destruction or de-identification of that personal information that is done in accordance with the APPs.

Unauthorised access

11.25 '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 entity[7] or independent contractor, as well as unauthorised access by an external third party (such as hacking and other malicious

[7] 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'.

activity). This can also involve the unauthorised copying of personal information and extracting that information.

Unauthorised modification

11.26 '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

11.27 '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 Act.[8]

11.28 This includes an unauthorised disclosure by an employee of the APP entity.[9] The term 'disclosure' is discussed in more detail in Chapter B (Key concepts).

Destroying or de-identifying personal information

11.29 An APP entity must take such steps as are reasonable steps in the circumstances 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).

11.30 Destroying or de-identifying personal information no longer needed is an important concept that can help reduce privacy and security risks. For example, retaining too many categories of personal information can increase the harm to an individual in the event of a data breach or unauthorised access. Retaining a high volume of personal information can also amplify the reputational and financial risks to the APP entity.

11.31 It is expected that an APP entity actively considers the privacy and security risks of any personal information it retains, and actively seeks to mitigate these risks by taking reasonable steps to destroy or de-identify personal information that is no longer needed.

11.32 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).

---

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

[9] 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)).

11.33 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 court/tribunal order requires it to be retained (APP 11.2). In practice, this means that different rules apply to agencies and organisations.

11.34 The reasonable steps an APP entity must take for the purposes of destroying or de-identifying personal information that is no longer needed include both technical and organisational measures (APP 11.3).

Personal information held by an agency

11.35 The term 'Commonwealth record' in s 6(1) has the same meaning as in s 3 of the Archives Act 1983 (Cth) (the Archives Act) and is discussed in more detail in Chapter B (Key concepts).[10] 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.

11.36 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.

11.37 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

11.38 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 11.5–11.7 above and Chapter B (Key concepts).

11.39 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.

11.40 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).

---

[10] Archives Act 1983 (Cth) 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.

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

11.41 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)).

11.42 '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

11.43 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 risks and adverse consequences increase.
- 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, and
- 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.

11.44 The reasonable steps an APP entity must take for the purposes of destroying or de-identifying personal information that is no longer needed include both technical and organisational measures (APP 11.3).

11.45 Technical measures include physical and technological methods to destroy or de-identify personal information. Examples of technical measures may include (but are not limited to) shredding, disintegrating and pulping, sanitisation of hardware and de-identification techniques.

11.46 Organisational measures involve implementing policies, processes and procedures to ensure personal information that is no longer needed is destroyed or de-identified. Examples of organisational measures may include (but are not limited to) staff training,

policies and procedures to determine if personal information needs to be retained, destroyed or de-identified, and verifying and documenting when and what personal information is destroyed or de-identified.

11.47 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.[11]

11.48 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 11.51 and 11.55–11.577 below).

Destroying personal information — irretrievable destruction

11.49 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.

11.50 For example, for personal information held:

- 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.[12] 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 11.5411.58 below), or should put the information beyond use (see paragraphs 11.51–53 below), or
- 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

11.51 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 11.54–11.58 below) and if so, take reasonable steps to de-identify the personal information.

---

[11] See OAIC website <https://www.oaic.gov.au>.

[12] 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.

11.52 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.

11.53 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.

De-identifying personal information

11.54 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).

11.55 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.[13]

11.56 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.

11.57 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 11.49–11.55 above).

11.58 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.

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

Chapter 12:

Australian Privacy Principle 12 —

Access to personal information

Version 1.1, July 2019

OAIC

Contents

Key points 3
What does APP 12 say? 3
'Holds' 4
Access to 'personal information' 4
Verifying an individual's identity 5
Giving access under APP 12 — general processing requirements 5
Giving access under APP 12 — further processing requirements for agencies 6
Refusing to give access under APP 12 — agencies 7
Authority to refuse access under the FOI Act 7
Required or authorised to refuse access under another Act 8
Refusing to give access under APP 12 — organisations 9
Giving access would pose a serious threat to the life, health or safety of any individual or to public health or public safety 9
Giving access would have an unreasonable impact on the privacy of other individuals 10
The request for access is frivolous or vexatious 10
The information requested relates to an existing or anticipated legal proceeding 11
Giving access would prejudice negotiations between the organisation and the individual 11
Giving access would be unlawful 11
Denying access is required or authorised by law or a court/tribunal order 12
Giving access would likely prejudice the taking of appropriate action in relation to suspected unlawful activity or serious misconduct 12
Giving access would be likely to prejudice an enforcement related activity conducted by, or on behalf of, an enforcement body 13
Giving access would reveal evaluative information in connection with a commercially sensitive decision-making process 13
APP 12 minimum access requirements 14
Difference with access requirements applying to agencies under FOI Act 14
Timeframe for responding to a request for access under APP 12 — agencies 14
Timeframe for responding to a request for access under APP 12 — organisations 15
How access is to be given under APP 12 15
Giving access by other means 15
Giving access through an intermediary 16
Access charges under APP 12 — agencies 16
Access charges under APP 12 — organisations 16
Giving written notice where access is refused, or not given in the manner requested under APP 12 17

Key points

- APP 12 requires an APP entity that holds personal information about an individual to give the individual access to that information on request.
- APP 12 also sets out other requirements in relation to giving access, including how access is to be given and when access can be refused. There are separate grounds on which agencies and organisations may refuse to give access.
- APP 12 operates alongside and does not replace other informal or legal procedures by which an individual can be provided with access to information, including, for agencies, the Freedom of Information Act 1982 (FOI Act) that provides a right of access to information held by agencies.

What does APP 12 say?

12.1 An APP entity that holds personal information about an individual must, on request, give that individual access to the information (APP 12.1). The grounds on which access may be refused differ for agencies and organisations.

12.2 APP 12 also sets out minimum access requirements, including the time period for responding to an access request, how access is to be given, and that a written notice, including the reasons for the refusal, must be given to the individual if access is refused.

12.3 APP 12 operates alongside and does not replace other informal or legal procedures by which an individual can be given access to information. In particular, APP 12 does not prevent an APP entity from giving access to personal information under an informal administrative arrangement,[1] provided the minimum access requirements stipulated in APP 12 have been met.

12.4 For agencies, APP 12 operates alongside the right of access in the FOI Act. The FOI Act provides individuals with a right of access to documents held by most Australian Government agencies,[2] including documents containing personal information.[3]

12.5 Some paragraphs in this Chapter are only relevant to agencies or to organisations:

- paragraphs only for agencies: 12.22–12.24; 12.25–12.32; 12.66; 12.76
- paragraphs only organisations: 12.33–12.62; 12.67; 12.77–12.81

[1] For information about administrative access schemes, see OAIC, Administrative Access, OAIC website <https://www.oaic.gov.au>.

[2] The FOI Act is expressed to apply separately to Ministers' offices in respect of 'an official document of a Minister' (s 48). APP 12 also applies to Ministers' offices: see the discussion of 'APP entity' in Chapter B (Key concepts), and the Privacy Act s 7(1)(d),(e).

[3] The Australian Information Commissioner has issued Guidelines (the FOI Guidelines) under s 93A of the FOI Act to which regard must be had for the purposes of performing a function, or exercising a power, under that Act. The FOI Guidelines are available at OAIC website <https://www.oaic.gov.au>.

‘Holds’

12.6 APP 12 only applies to personal information that an APP entity ‘holds’. An APP entity ‘holds’ personal information ‘if the entity has possession or control of a record that contains the personal information’ (s 6(1)).

12.7 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. In these circumstances, the entity must comply with APP 12 by giving the individual access (unless an exception applies). It cannot simply refer the individual to the third party that has physical possession. However, the individual has a separate right to request access from the third party, if the third party is an APP entity.

12.8 An agency that has placed a record of personal information in the care of the National Archives of Australia, or in the custody of the Australian War Memorial, is considered to be the agency that holds the record for the purposes of the Privacy Act (s 10(4)).

12.9 Upon receiving a request for access, an APP entity should search the records that it possesses or controls to assess whether the requested personal information is contained in those records. For example, an entity may search hard copy records and electronic databases and make enquiries of staff or contractors with relevant knowledge. A discussion with the individual may assist the entity to locate the information.

12.10 The term ‘holds’ is discussed in more detail in Chapter B (Key concepts).

Access to ‘personal information’

12.11 APP 12 requires an APP entity to provide access to ‘personal information’. It does not provide a right of access to other kinds of information. ‘Personal information’ is defined in s 6(1) as ‘information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not, and
- whether the information or opinion is recorded in a material form or not’

12.12 Personal information of one individual may also be personal information of another individual. For example:

- information in a marriage certificate may be personal information of both parties to the marriage
- an opinion may be personal information of both the subject and the giver of the opinion

12.13 APP 12 requires an APP entity to provide access to all of an individual’s personal information it holds, even if that information is also the personal information of another individual, unless a ground to refuse access applies. The grounds are discussed below, and include the ground that giving access would have an unreasonable impact on the privacy of another individual. ‘Personal information’ is discussed in more detail in Chapter B (Key concepts).

12.14 As to other requested information that is not personal information:

- If the APP entity is an organisation, it could consider whether the person has a right of access to that information under other legislation. If not, the organisation may make a

discretionary decision either to grant access to that other information or to refuse access.

- If the entity is an agency, it could consider whether access to that information can be granted under the FOI Act, or on an administrative basis. Before refusing access to that other information, the agency should advise the individual to consider making the request under the FOI Act.

Verifying an individual's identity

12.15 An APP entity must be satisfied that a request for personal information under APP 12 is made by the individual concerned, or by another person who is authorised to make a request on their behalf, for example, as a legal guardian or authorised agent. If an entity gives access to the personal information of another person, this could constitute a disclosure, which may not comply with APP 6 (see Chapter 6).

12.16 It would generally be impracticable for an APP entity to deal with an anonymous request for personal information. However, it may be practicable to deal with a pseudonymous request, for example, where the individual has previously transacted under that pseudonym, can establish their identity as that individual and the request for access relates to information about that pseudonymous identity (see Chapter 2 (APP 2)).

12.17 The steps appropriate to verify an individual's identity will depend on the circumstances. In particular, whether the individual is already known to or readily identifiable by the APP entity, the sensitivity of the personal information and the possible adverse consequences for the individual of unauthorised disclosure. The minimum amount of personal information needed to establish an individual's identity should be sought. Where possible, the personal information should be sighted rather than copied or collected for inclusion in a record. For example, in a face-to-face dealing with an individual, an entity may be able to record that an identity document was sighted without copying the document. In a telephone contact it may be adequate to request information that can be checked against records held by the entity. An entity that collects personal information to verify an individual's identity should consider the requirement in APP 11.2, to take reasonable steps to destroy or de-identify personal information no longer needed for any purpose for which it may be used or disclosed (unless an exception applies) (see Chapter 11 (APP 11)).

Giving access under APP 12 — general processing requirements

12.18 APP 12 requires that personal information be given to an individual 'on request'. APP 12 does not stipulate formal requirements for making a request, or require that a request be made in writing, or require the individual to state that it is an APP 12 request.[4]

12.19 It is open to an APP entity to provide access to personal information on an informal basis, provided the minimum access requirements in APP 12 are met. The access requirements in APP 12 relate to response times (see paragraphs 12.66–12.67 below), how access is to be given (see paragraphs 12.68–12.75 below), access charges (see paragraphs 12.76–12.81 below), and providing a written notice, including the reasons for the refusal, if access is

[4] This differs from the formal requirements relating to requests for access to documents under Part III of the FOI Act. See Part III of the FOI Act and Part 3 of the FOI Guidelines, OAIC website <https://www.oaic.gov.au>.

refused (see paragraphs 12.82–12.87 below). These are only the minimum requirements. An entity should endeavour to provide access in a manner that is as prompt, uncomplicated and inexpensive as possible.

12.20 An APP entity is required by APP 1.4(d) to state in an APP Privacy Policy 'how an individual may access personal information about the individual' (see Chapter 1 (APP 1)). An APP entity is also required by APP 5.2(g) to take reasonable steps to notify an individual, or ensure they are aware, of the fact that the entity's APP Privacy Policy contains information about how the individual may access their personal information held by the entity.

12.21 If an APP entity wishes an individual to follow a particular procedure in requesting access to their personal information, the entity could publish that procedure and draw attention to it, for example, by providing a link in the entity's APP Privacy Policy and on the entity's website homepage to the access procedure, to an online request form, or to an online portal that enables an individual to access their personal information. However, an entity cannot require an individual to follow a particular procedure, use a designated form or explain the reason for making the request. Any recommended procedure should be regularly reviewed to ensure that it is flexible and facilitates rather than hinders access.

Giving access under APP 12 — further processing requirements for agencies

12.22 Agencies should ensure that APP 12 access procedures are integrated with FOI Act procedures. The FOI Act sets out comprehensive rules about requesting and providing access to documents held by most Australian Government agencies, including documents containing personal information, and resolving access disputes. An important FOI requirement is that an agency has a duty to take reasonable steps to assist an individual to make an access request that complies with the FOI Act access requirements (FOI Act, s 15(3)). That means an agency could refer to the FOI Act in the agency's APP Privacy Policy and, in appropriate circumstances, draw the FOI Act to an individual's attention. Agencies should also consider providing this information through an 'Access to information' link on the agency's website homepage.[5]

12.23 Agencies are not required to advise individuals to request personal information under the FOI Act rather than under an administrative arrangement or by relying on APP 12. As explained in the FOI Guidelines,[6] agencies should consider establishing administrative access arrangements that operate alongside the FOI Act and that provide easier and less formal means for individuals to obtain access to government information, including personal information. Providing access to personal information under an administrative arrangement will fulfil an agency's obligation under APP 12 to provide access upon request, provided the arrangement meets the minimum access requirements in APP 12.

12.24 In some circumstances it may be preferable for an agency to suggest that an individual make an access request under the FOI Act:

- An FOI access request can relate to any document in the possession of an agency (FOI Act, s 15(1)) and is not limited to personal information held in an agency record (APP 12.1).

[5] See OAIC, Guidance for Agency Websites: 'Access to Information' Web Page, OAIC website <https://www.oaic.gov.au>.

[6] See OAIC, FOI Guidelines, Part 3, OAIC website <https://www.oaic.gov.au>. See also OAIC, Administrative Access, OAIC website <https://www.oaic.gov.au>.

- The FOI Act contains a consultation process for dealing with requests for documents that contain personal or business information about a person other than the requester (FOI Act, ss 27, 27A).
- An applicant who applies for access under the FOI Act can complain to the Information Commissioner about an action taken by an agency under that Act (FOI Act, s 70) (complaint mechanisms under the Privacy Act are discussed in paragraph 12.30 and 12.87 below).
- An applicant who is refused access under the FOI Act has a right to apply for internal review or Information Commissioner review of the access refusal decision (FOI Act, ss 54, 54L).

Refusing to give access under APP 12 — agencies

12.25 An agency is not required by APP 12 to give access to personal information if the agency is required or authorised to refuse access to that information by or under:

- the FOI Act (APP 12.2(b)(i))
- any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents (APP 12.2(b)(ii))

12.26 The meaning of 'required or authorised' is discussed in Chapter B (Key concepts). In summary, an agency is 'required' to refuse access by an Act that prohibits the disclosure of the personal information; and an agency is 'authorised' to refuse access by an Act that authorises or confers discretion on the agency to refuse a request for access to the personal information.

Authority to refuse access under the FOI Act

12.27 The FOI Act lists several grounds on which an agency can refuse a request under the Act for access to documents. An agency may rely on any of those grounds to refuse access under APP 12. It is nevertheless open to an agency not to rely on any such ground and to provide access upon request, unless disclosure is prohibited, for example, by a secrecy provision.[7]

12.28 The grounds on which an access request can be declined under the FOI Act include:[8]

- a document is an exempt document under Part IV, Division 2 of the FOI Act, for example, the document is a Cabinet document, is subject to legal professional privilege, contains material obtained in confidence, or a secrecy provision applies
- a document is a conditionally exempt document under Part IV, Division 3 of the FOI Act, for example, the document contains deliberative matter, or disclosure of the document would involve the unreasonable disclosure of personal information about another

[7] The same discretionary principle applies under the FOI Act. Section 3A of the FOI Act provides that it does not limit any power of an agency to publish or grant access to information under other legislative or administrative schemes.

[8] The Australian Information Commissioner has issued guidelines (the FOI Guidelines) under s 93A of the FOI Act to which regard must be had for the purposes of performing a function, or exercising a power, under that Act. See OAIC, FOI Guidelines, OAIC website <https://www.oaic.gov.au>.

person and it would be contrary to the public interest to release the document at that time

- the individual is not entitled to obtain access to a document of the kind requested, for example, the document is available for purchase from an agency (FOI Act, ss 12, 13)
- providing access in the terms requested by a person would substantially and unreasonably divert an agency's resources from its other operations (s 24AA)
- processing a person's request would require an agency to disclose the existence or non-existence of a document, where that would otherwise be exempt information (s 25)

12.29 The FOI Act specifies consultation processes that may apply to requests made under that Act, for example, where a 'practical refusal reason' may apply (FOI Act, s 24) to the request, or where a requested document contains a third party's personal or business information (FOI Act, ss 27, 27A). An agency is not required to undertake any of those consultation processes before refusing access on any of those grounds under APP 12. This is required only if the person decides to make a request under the FOI Act.

12.30 A decision to refuse access under APP 12.2(b)(i) (on one of the FOI grounds listed above) is a decision made under the Privacy Act, not the FOI Act. As required by APP 12.9, the agency must provide the individual with a written notice that sets out the reasons for the refusal and the complaint mechanisms available to the individual (see paragraph 12.87 below). The individual may have a right to complain to the Information Commissioner under the Privacy Act. After investigation, the Commissioner may make a determination that the agency has failed to comply with APP 12 and require, for example, that the agency give access (Privacy Act, s 52). However, the individual will not have a right to seek internal review or Information Commissioner review under the FOI Act.

Required or authorised to refuse access under another Act

12.31 APP 12.2(b)(ii) provides that an agency is not required to give access to personal information if it is required or authorised to refuse to give access by another Act that provides for access by persons to documents. An example is a statutory secrecy provision that requires or authorises that access be refused in certain circumstances.

12.32 A further example is that the National Archives of Australia (NAA) is authorised to refuse access to certain 'exempt records' under the Archives Act 1983 (the Archives Act). The Archives Act provides that the NAA must make available for public access Commonwealth records in the open access period that are in the care of the NAA and that are not exempt records (s 31 of the Archives Act). The categories of exempt records include information whose disclosure would constitute a breach of confidence, would involve the unreasonable disclosure of information relating to the personal affairs of any person, or would unreasonably affect a person adversely in relation to his or her business, financial or professional affairs (s 33 of the Archives Act).[9]

[9] For further information about the National Archives of Australia's obligation to make available Commonwealth records for public access, see National Archives of Australia website <www.naa.gov.au>.

Refusing to give access under APP 12 — organisations

12.33 APP 12.3 lists ten grounds on which an organisation can refuse to give access to personal information. It is nevertheless open to an organisation not to rely on any such ground and to provide access upon request, unless disclosure is prohibited. Before relying on any of these grounds an organisation should consider whether redacting some information would enable access to be provided (for example, redacting personal information about another person).

12.34 The grounds, which are considered separately below, are:

- the organisation reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety (APP 12.3(a))
- giving access would have an unreasonable impact on the privacy of other individuals (APP 12.3(b))
- the request for access is frivolous or vexatious (APP 12.3(c))
- the information relates to existing or anticipated legal proceedings between the organisation and the individual, and would not be accessible by the process of discovery in those proceedings (APP 12.3(d))
- giving access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations (APP 12.3(e))
- giving access would be unlawful (APP 12.3(f))
- denying access is required or authorised by or under an Australian law or a court/tribunal order (APP 12.3(g))
- the organisation has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the organisation'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 (APP 12.3(h))
- giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body (APP 12.3(i))
- giving access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process (APP 12.3(j))

Giving access would pose a serious threat to the life, health or safety of any individual or to public health or public safety

12.35 The phrase, 'serious threats to the life, health or safety of any individual, or to public health or public safety' is discussed in Chapter C (Permitted general situations).

12.36 An example of where this ground might apply is a healthcare provider having reasonable grounds to believe that giving an individual access to their personal information may cause that person significant distress or lead to self-harm or harm to another person.

Giving access would have an unreasonable impact on the privacy of other individuals

12.37 This ground may apply where the record of personal information that an individual has requested contains personal information of another individual. As noted above (paragraph 12.12), a record of an individual's opinions or views (for example, a referee comment) may be personal information of that individual.[10]

12.38 Before relying on this ground an organisation must be satisfied that giving access would have 'an unreasonable impact' on the privacy of another. Factors that may be relevant in deciding that issue include:

- the nature of the personal information about the other individual. For example, if the personal information is of a sensitive or confidential nature it may be unreasonable to provide it to others.
- the reasonable expectation of the other individual about how that personal information will be handled (this should be assessed objectively and on the basis that the other individual may not have special knowledge of the industry or activity involved). For example, if both individuals were present when the personal information was collected, there may be a reasonable expectation that each individual could later access the personal information.
- the source of the personal information. For example, if the individual requesting access provided the personal information about the other individual, access may not have an unreasonable impact on that person.
- whether the personal information of another individual could be redacted from the record provided to the individual requesting access.
- whether access could be provided through an intermediary (see paragraphs 12.72–12.75 below).
- whether the other individual consents to access being given to the individual requesting access.

12.39 In applying this ground, an organisation may consult the other individual about whether giving access would have an unreasonable impact on their privacy. The view expressed by that individual may be relevant but not determinative. However, before consulting another individual, an organisation should consider whether doing so poses a privacy risk for the individual seeking access.

The request for access is frivolous or vexatious

12.40 A request should not be refused on this ground unless there is a clear and convincing basis for deciding that a request is frivolous or vexatious. It is not a sufficient basis, for example, that a request would cause inconvenience or irritation to an organisation.

12.41 The following are given as examples of requests that may be treated as frivolous or vexatious:

[10] For further discussion of where giving access would have an unreasonable impact on the privacy of other individuals, see Smallbone v New South Wales Bar Association [2011] FCA 1145 (6 October 2011).

- Repeated requests for access to personal information that has already been provided to the requester.
- A request that contains offensive or abusive language, or that does not appear to be a genuine request for personal information.
- A repeat request for personal information that an organisation has earlier explained to an individual it does not hold, has been destroyed, or cannot be located after a reasonable search.
- A request made for the apparent purpose of harassing or intimidating the staff of an organisation, or interfering unreasonably with its operations.

The information requested relates to an existing or anticipated legal proceeding

12.42 This ground applies where legal proceedings between the individual and the organisation are underway or anticipated, and the information would not be accessible by the process of discovery in those proceedings. A legal proceeding is anticipated if there is a real prospect of proceedings being commenced, as distinct from a mere possibility.

Giving access would prejudice negotiations between the organisation and the individual

12.43 This ground applies where giving access would prejudice negotiations between the organisation and the individual by revealing the intentions of the organisation in relation to the negotiations. The negotiations may be current or reasonably anticipated.

12.44 Examples of where this ground might apply is an organisation negotiating:

- a claim brought by an individual for compensation (for example, for negligence or wrongful dismissal), and releasing the personal information requested by the individual may reveal the organisation's strategy to settle or defend the claim
- a sponsorship arrangement with an individual, and releasing the personal information requested by the individual may reveal the organisation's strategy in relation to negotiating the arrangement

12.45 This exception applies only to personal information that would prejudice negotiations, and not to all information relevant to the negotiations. Access should be provided to other personal information that is requested, unless another exception applies.

Giving access would be unlawful

12.46 'Unlawful activity' is not defined in the Privacy Act. The core meaning is activity that is criminal, illegal or prohibited or proscribed by law, and can include unlawful discrimination or harassment, but does not include breach of a contract. Examples of unlawful activity include criminal offences, unlawful discrimination, and trespass.

12.47 Examples of where this ground might apply are where giving access would be a breach of legal professional privilege, a breach of confidence or a breach of copyright.

Denying access is required or authorised by law or a court/tribunal order

12.48 The meaning of 'required or authorised by or under an Australian law or a court/tribunal order' is discussed in Chapter B (Key concepts). This ground applies where an Australian law or court or tribunal order forbids the disclosure of information; or a law or order authorises or confers discretion on an organisation to refuse a request from an individual for access to their personal information. (There is overlap between this ground and the preceding ground 'giving access would be unlawful'.)

12.49 An example of where this ground might apply is a court order providing that an organisation is not required to provide personal information to an individual who is in the care of or is undergoing treatment by the organisation.

Giving access would likely prejudice the taking of appropriate action in relation to suspected unlawful activity or serious misconduct

12.50 There are a number of separate elements to this ground.

12.51 First, an organisation must have reason to suspect that unlawful activity or misconduct of a serious nature has been, is being or may be engaged in. The term 'unlawful activity' is not defined in the Privacy Act. The core meaning is activity that is criminal, illegal or prohibited or proscribed by law, and can include unlawful discrimination or harassment, but does not include breach of a contract. Examples of unlawful activity include criminal offences, unlawful discrimination, and trespass.

12.52 Misconduct is defined in s 6(1) to include 'fraud, negligence, default, breach of trust, breach of duty, breach of discipline or any other misconduct in the course of duty'. An added requirement of this ground is that the misconduct is 'serious' in nature. This excludes minor breaches or transgressions.

12.53 The organisation must have 'reason to suspect' the unlawful activity or serious misconduct has been, is being or may be engaged in. This is a different and lesser standard to 'reasonably believes', which is used in some other APPs (see Chapter B (Key concepts)). There should nevertheless be a reasonable basis for the suspicion. It is the responsibility of the organisation to be able to justify its reasonable basis for the suspicion.

12.54 The suspected unlawful activity or serious misconduct must relate to the organisation's functions or activities. As discussed in Chapter 3 (APP 3), an organisation's functions or activities include current, proposed and support functions and activities.

12.55 Lastly, giving access must be likely to prejudice the organisation in taking appropriate action in relation to the suspected unlawful activity or serious misconduct. The proposed action may include investigation of the activity or misconduct, or reporting it to the police or another relevant person or authority. There should again be a reasonable basis for this expectation of prejudice. For example, in some instances giving an individual access would not prejudice the taking of appropriate action, but would allow the individual to provide further information relevant to the suspected unlawful activity.

12.56 An example of where this ground might apply is where giving access to the requested personal information would reveal that, covertly but lawfully, an organisation is

investigating suspected misconduct of a client and disclosure would prejudice the covert investigation.

Giving access would be likely to prejudice an enforcement related activity conducted by, or on behalf of, an enforcement body

12.57 '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, the Australian Crime Commission, Customs, the Integrity Commissioner,[11] the Immigration Department,[12] the Australian Prudential Regulation Authority, the Australian Securities and Investments Commission and AUSTRAC.

12.58 'Enforcement related activity' is also defined in s 6(1). It includes the prevention, detection, investigation and prosecution or punishment of criminal offences and intelligence gathering activities.

12.59 The terms 'enforcement related activity' and 'enforcement body' are discussed in Chapter B (Key concepts).

12.60 An example of where this ground might apply is an enforcement body asking an organisation not to give an individual access to certain personal information, as doing so would be likely to reveal the existence of a criminal investigation or interfere with preparation for court proceedings.

Giving access would reveal evaluative information in connection with a commercially sensitive decision-making process

12.61 This ground applies if giving access would reveal 'evaluative information' generated within an organisation in connection with a commercially sensitive decision-making process. An example of evaluative information is a score card weighting system and score card result. The ground applies only to the evaluative information, and not to personal information on which a decision was based.[13]

12.62 APP 12.10 provides that if an organisation refuses to give access to personal information under this ground, its written notice explaining the reasons for refusal may include an explanation for the commercially sensitive decision. This may include explaining the reasons for the decision and giving a copy of the personal information that informed the decision. For discussion of the requirement to give a written notice refusing access, see paragraphs 12.82–12.87 below.

---

[11] 'Integrity Commissioner' is defined in s 6(1) as having the same meaning as in the Law Enforcement Integrity Commissioner Act 2006.

[12] 'Immigration Department' is defined in s 6(1) as the Department administered by the Minister administering the Migration Act 1958.

[13] See also C v Insurance Company [2006] PrivCmrA 3 (1 February 2006).

APP 12 minimum access requirements

12.63 APP 12 sets out minimum access requirements that must be met when an APP entity receives a request from an individual for access to their personal information. The access requirements relate to the response time, how access is to be given, access charges and giving a written notice, including the reasons for refusal, if access is refused.

12.64 An individual may complain under s 36 to the Information Commissioner about the failure of an APP entity to comply with any of the APP 12 minimum access requirements. The Commissioner will not investigate a complaint if the person has not first raised the matter with the entity complained about, unless it was not appropriate to require that as a first step (s 40(1A)). When investigating a complaint, the OAIC will initially attempt to conciliate the complaint (s 40A), before considering the exercise of other complaint resolution powers (s 52).

Difference with access requirements applying to agencies under FOI Act

12.65 The APP 12 minimum access requirements and the Privacy Act complaint and review mechanisms differ in important respects from those applying to agencies in relation to requests for information received under the FOI Act.[14] For example, the FOI Act requires an agency to acknowledge receipt of an FOI request within 14 days, and to make a decision on the request within 30 calendar days. The processing period can be extended with the agreement of the applicant, to enable an agency to consult a third party, or with the approval of the Information Commissioner for complex and voluminous requests.[15] If an agency fails to make a decision within the statutory processing period (including an authorised extension) the agency is deemed to have made a decision refusing access. The applicant may then apply for internal review or Information Commissioner review, although the OAIC can extend the time for an agency to make a decision on the request. The FOI Act also contains special requirements on charges, the form of access and statements of reasons.

Timeframe for responding to a request for access under APP 12 — agencies

12.66 APP 12.4(a)(i) provides that an agency must 'respond' to a request for access within 30 calendar days. The 30 day time period commences on the day after the day the agency receives the request. The agency must respond by giving access to the personal information that is requested, or by notifying its refusal to give access. If this is impracticable (for example, there is a justifiable need to clarify the scope of an individual's request, or to locate and assemble the requested information, or to consult a third party), the agency is expected to contact the individual to explain the delay and provide an expected timeframe for finalising the request. These are matters the Information Commissioner may examine if a complaint is made about an agency's failure to comply with the timeframe in APP 12.4(a).

[14] The circumstances in which an individual may apply to the Administrative Appeals Tribunal for review of a decision of the Information Commissioner are set out in s 96.

[15] See OAIC, Extension of Time for Processing Requests, OAIC website <https://www.oaic.gov.au>.

Timeframe for responding to a request for access under APP 12 — organisations

12.67 APP 12.4(a)(ii) provides that an organisation must respond 'within a reasonable period after the request is made'. As with agencies, an organisation must respond by giving access to the personal information that is requested, or by notifying its refusal to give access. Factors that may be relevant in deciding what is a reasonable period include the scope and clarity of a request, whether the information can be readily located and assembled, and whether consultation with the individual or other parties is required. However, as a general guide, a reasonable period should not exceed 30 calendar days.

How access is to be given under APP 12

12.68 An APP entity must give access to personal information in the manner requested by the individual, if it is reasonable and practicable to do so (APP 12.4(b)). The manner of access may, for example, be by email, by phone, in person, hard copy, or an electronic record.

12.69 Factors relevant in assessing whether it is reasonable and practicable to give access in the manner requested by an individual include:

- the volume of information requested. For example, it may be impracticable to provide a large amount of personal information by telephone.
- the nature of the information requested. For example, it may be impracticable to give access to digitised information in hard copy and it may be unreasonable to give access to information of a highly sensitive nature by telephone if the APP entity cannot sufficiently verify the individual's identity over the telephone.
- any special needs of the individual requesting the information. For example, it may be reasonable to give information in a form that can be accessed via assistive technology where this meets the special needs of the individual.

Giving access by other means

12.70 APP 12.5 applies where an APP entity refuses to give access to personal information under APP 12 on a permitted ground, or refuses to give access in the manner requested by the individual. The entity must take reasonable steps to give access in a way that meets the needs of the entity and the individual. This should be done within 30 calendar days where practicable.

12.71 The APP entity is expected to consult the individual to try to satisfy their request.[16] The following are given as examples of alternative manners of access that may meet the needs of the entity and the individual, and in particular result in more rather than less personal information being provided to an individual:

- deleting any personal information for which there is a ground for refusing access and giving the redacted version to the individual
- giving a summary of the requested personal information to the individual
- giving access to the requested personal information in an alternative format

[16] Explanatory memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 87.

- facilitating the inspection of a hard copy of the requested personal information and permitting the individual to take notes
- facilitating access to the requested personal information through a mutually agreed intermediary (see paragraphs 12.72–12.75 below)

Giving access through an intermediary

12.72 APP 12.6 provides that, without limiting APP 12.5, 'access may be given through the use of a mutually agreed intermediary'.

12.73 The role of an intermediary is to enable an individual to be given access to their personal information and to have the content of that information explained, where direct access would otherwise be refused. An example is an organisation refusing direct access under APP 12.3(a) on the reasonable belief that access may lead the individual to self-harm, but deciding that access through an intermediary may not pose a similar threat. The role of the intermediary in conveying or explaining the information to the individual will need to be tailored to the nature of the information and any instructions given by the APP entity to the intermediary.

12.74 The intermediary must be acceptable to both the APP entity and the individual. In seeking an individual's agreement to use an intermediary, an entity should clearly explain the process and the type of access that will be provided through this process. Depending on the nature of the personal information to which access is sought, the intermediary may need particular skills or knowledge. For example, an intermediary may need to be a qualified health service provider if used to give access to health information.

12.75 If an individual does not agree to the use of an intermediary, or agreement cannot be reached on whom to use as the intermediary, the APP entity must still take reasonable steps to give access through another manner that meets the needs of the entity and the individual.

Access charges under APP 12 — agencies

12.76 An agency cannot impose upon an individual any charge for providing access to personal information under APP 12 (APP 12.7). This includes:

- a charge for the making of the request to access personal information
- a charge for giving access to requested personal information, such as charges for copying costs, postage costs and costs associated with using an intermediary

Access charges under APP 12 — organisations

12.77 An organisation cannot impose upon an individual a charge for the making of the request to access personal information.

12.78 An organisation may, however, impose a charge for giving access to requested personal information, provided the charge is not excessive (APP 12.8). Items that may be charged for include:

- staff costs in searching for, locating and retrieving the requested personal information, and deciding which personal information to provide to the individual
- staff costs in reproducing and sending the personal information

- costs of postage or materials involved in giving access
- costs associated with using an intermediary (see paragraphs 12.72–12.75 above)

12.79 Whether a charge is excessive will depend on the nature of the organisation, including the organisation's size, resources and functions, and the nature of the personal information held. The following charges may be considered excessive:

- a charge that exceeds the actual cost incurred by the organisation in giving access
- a charge associated with obtaining legal or other advice in deciding how to respond to an individual's request
- a charge for consulting with the individual about how access is to be given
- a charge that reflects shortcomings in the organisation's information management systems. An individual should not be disadvantaged because of the deficient record management practices of an organisation

12.80 An organisation should also consider waiving, reducing or sharing any charge that may be imposed, so that the charge is not excessive. In determining the amount to charge, an organisation should consider:

- the organisation's relationship with the individual
- any known financial hardship factors claimed by the individual
- any known adverse consequences on the individual if they do not get access to the personal information

12.81 A charge by an organisation for giving access must not be used to discourage an individual from requesting access to personal information. To the extent practicable, an organisation should advise an individual in advance if a charge may be imposed, and the likely amount of the charge. The individual should be invited to discuss options for altering the request to minimise any charge. This may include options for giving access in another manner that meets the needs of the entity and the individual (see APP 12.5 and paragraphs 12.70–12.71 above). Any charge that is imposed should be clearly communicated and explained before access is given.

Giving written notice where access is refused, or not given in the manner requested under APP 12

12.82 APP 12.9 provides that if an APP entity refuses to give access, or to give access in the manner requested by the individual, the entity must give the individual a written notice setting out:

- the reasons for the refusal, except to the extent that it would be unreasonable to do so, having regard to the grounds for refusal
- the complaint mechanisms available to the individual, and
- any other matters prescribed by regulations made under the Privacy Act

12.83 The reasons for refusal should explain, where applicable:

- that the entity does not hold the requested personal information
- the ground of refusal. For example, if the entity is required or authorised by an Australian law to refuse access, notice should include the name of that law and, if practicable, could include the provision relied upon.

- that access cannot be given in the manner requested by the individual, and the reason why
- that the steps necessary to give access in a way that meets the needs of the entity and the individual under APP 12.5 are not reasonable in the circumstances

12.84 The notice could, in addition, set out any steps that may be taken by the individual that would mean that access would not be refused, for example, by re-framing or narrowing the scope of the individual's request.

12.85 APP 12.10 additionally provides that, where an organisation relies on the commercially sensitive decision ground in APP 12.3(j), the written notice may provide an explanation for the commercially sensitive decision (see paragraphs 12.61–12.62 above).

12.86 An APP entity is not required to explain the ground of refusal to the extent that it would be unreasonable to do so. This course should be adopted only in justifiable circumstances. Examples for organisations include that an explanation may prejudice action by an organisation to respond to unlawful activity (APP 12.3(h)); may prejudice enforcement action by an enforcement body (APP 12.3(i)). An example for agencies is that this would reveal the existence of a document whose existence an agency would be entitled to neither confirm nor deny under s 25 of the FOI Act.

12.87 The description of the complaint mechanisms available to an individual should explain the internal and external complaint options, and the steps that should be followed. In particular, the individual should be advised that:

- a complaint should first be made in writing to the APP entity (s 40(1A))
- the entity should be given a reasonable time (usually 30 days) to respond
- a complaint may then be taken to a recognised external dispute resolution scheme of which the entity is a member (if any), and
- lastly, a complaint may be made to the Information Commissioner (s 36)

Chapter 13:

Australian Privacy Principle 13 —

Correction of personal information

Version 1.1, July 2019

OAIC

Contents

Key points 3
What does APP 13 say? 3
Interaction of APP 13 and other correction procedures 4
Interaction of APP 13 and other APPs 4
'Holds' 5
Taking reasonable steps to correct personal information 5
Correcting at the APP entity's initiative 5
Correcting at the individual's request 6
Agencies — comparison of APP 13 and FOI Act procedures 7
Grounds for correcting personal information 8
Accurate 9
Up-to-date 9
Complete 10
Relevant 10
Not misleading 10
Being satisfied and taking reasonable steps 10
Being satisfied 10
Reasonable steps to correct 11
APP 13 minimum procedural requirements 12
Taking reasonable steps to notify another APP entity 12
Giving written notice where correction is refused 13
Taking reasonable steps to associate a statement 14
Timeframe for responding to a request for correction under APP 13 15
Access charges under APP 13 15

Key points

- APP 13 requires an APP entity to take reasonable steps to correct 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.
- This requirement applies where:
  - the APP entity is satisfied the personal information is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to a purpose for which it is held, or
  - the individual requests the entity to correct the personal information
- Special considerations apply to Commonwealth records, which can only be destroyed or altered in accordance with the Archives Act 1983 (Archives Act).
- APP 13 also sets out other minimum procedural requirements in relation to correcting personal information, including when an APP entity must:
  - take reasonable steps to notify other APP entities of a correction
  - give notice to the individual which includes reasons and available complaint mechanisms if correction is refused
  - take reasonable steps to associate a statement with personal information it refuses to correct
  - respond to a request for correction or to associate a statement, and
  - not charge an individual for making a request, correcting personal information or associating a statement
- APP 13 operates alongside and does not replace other informal or legal procedures by which an individual can seek correction of their personal information, including informal arrangements and, for agencies, the Freedom of Information Act 1982 (FOI Act).

What does APP 13 say?

13.1 APP 13.1 provides that an APP entity must take reasonable steps to correct personal information it holds, to ensure it is accurate, up-to-date, complete, relevant and not misleading, having regard to the purpose for which it is held. The shorthand expression used in this chapter is that an APP entity is required to correct 'incorrect personal information'.

13.2 The requirement to take reasonable steps applies in two circumstances:

- where an APP entity is satisfied, independently of any request, that personal information it holds is incorrect, or
- where an individual requests an APP entity to correct their personal information

13.3 Special considerations apply to Commonwealth records. A Commonwealth record can, as a general rule, only be destroyed or altered in accordance with the Archives Act (see paragraph 13.48).

13.4 APP 13 also sets out other minimum procedural requirements in relation to correcting personal information. An APP entity must:

- upon request by an individual whose personal information has been corrected, take reasonable steps to notify another APP entity of a correction made to personal information that was previously provided to that other entity (APP 13.2)
- give a written notice to an individual when a correction request is refused, including the reasons for the refusal and the complaint mechanisms available to the individual (APP 13.3)
- upon request by an individual whose correction request has been refused, take reasonable steps to associate a statement with the personal information that the individual believes it to be inaccurate, out-of-date, incomplete, irrelevant or misleading (APP 13.4)
- respond in a timely manner to an individual's request to correct personal information or to associate a statement with the personal information (APP 13.5(a))
- not charge an individual for making a request to correct personal information or associate a statement, or for making a correction or associating a statement (APP 13.5(b))

Interaction of APP 13 and other correction procedures

13.5 APP 13 operates alongside and does not replace other informal or legal procedures by which an individual can request that personal information be corrected. In particular, APP 13 does not prevent an APP entity from correcting personal information under an informal administrative arrangement, provided the arrangement satisfies the requirements of APP 13. For example, an entity may allow individuals to correct their personal information by providing updated information through an online portal.

13.6 For agencies, APP 13 operates alongside the right to amend or annotate personal information in Part V of the Freedom of Information Act 1982 (FOI Act). The FOI Act procedures, criteria and review mechanisms differ in important respects from those applying under APP 13 and the Privacy Act. These differences, and when it is more appropriate to use one Act rather than another, are considered below at paragraphs 13.25–13.29.

Interaction of APP 13 and other APPs

13.7 The correction requirements in APP 13 complement and overlap with the requirements in other APPs, including APP 10 (quality of personal information) and APP 11 (security of personal information).

13.8 APP 10 provides that an APP entity must take reasonable steps to ensure the quality of personal information it collects, uses or discloses (see Chapter 10 (APP 10)). If reasonable steps are taken to comply with APP 10, this reduces the likelihood that personal information will need correction under APP 13. Similarly, by taking reasonable steps to correct personal information under APP 13, an entity can better ensure that it complies with APP 10 by ensuring that information is accurate, up-to-date, complete and relevant when it is used or disclosed.

13.9 APP 11.1 provides that an APP entity must take reasonable steps to protect the personal information it holds, including from interference, loss and unauthorised modification. If reasonable steps are taken to comply with APP 11.1, this reduces the likelihood that personal information will need correction under APP 13. APP 11.2 provides that an entity

must take reasonable steps to destroy or de-identify personal information that it no longer needs for any purpose for which it may be used or disclosed. This requirement does not apply where the information is contained in a Commonwealth record or where the entity is required by law or a court/tribunal order to retain the personal information (see Chapter 11 (APP 11)). When taking steps to identify and correct incorrect personal information under APP 13, an entity should consider whether it still needs the personal information for a permitted purpose, or whether reasonable steps must be taken to destroy or de-identify the information under APP 11.2.

'Holds'

13.10 APP 13 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)).

13.11 The term 'holds' extends beyond physical possession of a record to include a record that an entity has the right or power to deal with. For example, an APP entity that has outsourced 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 and must comply with APP 13 (see paragraph 13.47 below). In addition, the individual has a separate right to request correction of the information by the third party, if the third party is an APP entity.

13.12 An agency that has placed a record of personal information in the care of the National Archives of Australia, or in the custody of the Australian War Memorial, is considered to be the agency that holds the record for the purposes of the Privacy Act (s 10(4)).

13.13 Upon receiving a request for correction, an APP entity should search the records that it possesses or controls to assess whether the personal information to be corrected is contained in those records. For example, an entity may search hard copy records and electronic databases and make enquiries of staff or contractors with relevant knowledge. A discussion with the individual may assist the entity to locate the information.

13.14 The term 'holds' is discussed in more detail in Chapter B (Key concepts).

Taking reasonable steps to correct personal information

13.15 APP 13.1 requires an APP entity to take reasonable steps to correct personal information it holds, in two circumstances: on its own initiative, and at the request of the individual to whom the personal information relates.

Correcting at the APP entity's initiative

13.16 An APP entity is required to take reasonable steps to correct personal information it holds if the entity is satisfied, having regard to a purpose for which the personal information is held, that it is inaccurate, out-of-date, incomplete, irrelevant or misleading (that is, the personal information is incorrect). Implicit in that requirement is that an entity should be alert to the possibility that personal information it holds may be incorrect and may require correction.

13.17 Generally, an APP entity may become aware that an item of personal information requires correction if it discovers an inconsistency during normal business practices. Examples include:

- information provided to the entity by the individual or a third party may be inconsistent with other personal information held by the entity. For example, an identity document, letter, medical record or photograph
- a court or tribunal has made a finding about the personal information, in a case involving the entity or in another case that comes to the entity's notice
- the entity may be notified by another entity or person that the personal information is incorrect, or that similar personal information held by the other entity has been corrected
- a practice, procedure or system the entity has implemented in compliance with APP 1.2 (such as an auditing or monitoring program) indicates that personal information the entity holds requires correction.

13.18 After becoming aware that personal information may require correction, the APP entity should satisfy itself that the information is incorrect, before taking reasonable steps to correct it (see paragraphs 13.30–13.41).

Correcting at the individual's request

13.19 An APP entity is required by APP 13.1 to take reasonable steps to correct an individual's personal information to ensure it is not incorrect when the individual 'requests' the entity to do so. Upon receiving a request an entity must decide if it is satisfied that the information is incorrect, and if so, take reasonable steps to correct it (see paragraphs 13.43–13.48 below).

13.20 APP 13 does not stipulate formal requirements that an individual must follow to make a request, or require that a request be made in writing, or require the individual to state that it is an APP 13 request.[1]

13.21 An APP entity is required by APP 1.4(d) to state in an APP Privacy Policy how an individual may seek the correction of their personal information held by the entity. An APP entity is also required by APP 5.2(g) to take reasonable steps to notify an individual, or ensure they are aware, of the fact the entity's APP Privacy Policy contains information about how the individual may seek correction of their personal information held by the entity.

13.22 If an APP entity wishes an individual to follow a particular procedure in requesting correction of their personal information, the entity could publish that procedure and draw attention to it, for example, by providing a link in the APP Privacy Policy and on the entity's website homepage to the correction request procedure, to an online request form, or to an online portal that enables an individual to correct their personal information. However, an entity cannot require an individual to follow a particular procedure, use a designated form or explain the reason for making the request. Any recommended procedure should be regularly reviewed to ensure that it is flexible and facilitates rather than hinders correction of personal information.

[1] This differs from the formal requirements relating to requests for amendment or annotation under the FOI Act (see FOI Act, Part III).

13.23 An APP entity must be satisfied that a request to correct personal information under APP 13 is made by the individual concerned, or by another person who is authorised to make a request on their behalf, for example, a legal guardian or authorised agent. The steps appropriate to verify an individual's identity will depend on the circumstances, and in particular, whether the individual is already known to or readily identifiable by the entity. The discussion in Chapter 12 (APP 12) of steps that can be taken to verify the identity of an individual seeking access to their personal information apply also to APP 13.

13.24 APP 13 stipulates minimum procedural requirements that must be met by an APP entity when dealing with a request to correct personal information. These are discussed later in this chapter, and include taking reasonable steps if requested by the individual to notify other APP entities when a correction is made (see paragraphs 13.49–13.53), providing an individual with a written notice that includes the reasons for refusal if a correction request is refused (paragraphs 13.54–13.58), response times (paragraphs 13.63–13.64) and charging (paragraph 13.65). Provided an entity meets those minimum requirements, it may choose the arrangements (including an informal arrangement) for receiving and acting upon correction requests. An online portal through which individuals can access and correct their personal information is an example of an informal arrangement that may provide a fast and easy means of correction, and that can qualify as an APP 13 'request' procedure.

Agencies — comparison of APP 13 and FOI Act procedures

13.25 For agencies, APP 13 operates alongside the right to amend or annotate personal information in Part V of the FOI Act. There is substantial overlap between the APP 13 and the FOI Act procedures, but also some noteworthy differences.

13.26 The FOI Act provides that a person may apply to an agency[2] to amend or annotate a record of personal information about that person, to which they have lawfully had access under the FOI Act or otherwise (FOI Act, s 48). The application must be in writing, specify as far as practicable how and why the record should be amended or annotated, and provide a return address to which notices can be sent (FOI Act, ss 49, 51A). The grounds on which such an application may be made are that the record of personal information 'is incomplete, incorrect, out of date or misleading' (FOI Act, s 48(a)). The record must also have been used or be available for use by the agency 'for an administrative purpose' (FOI Act, s 48(b)). The agency may act upon an application by altering or adding a note to a record, but as far as practicable must not obliterate the text of the record as it existed prior to the amendment (FOI Act, s 50). An applicant whose application is not accepted may provide a statement specifying their disagreement with the decision, and the agency must annotate the record by attaching that statement (FOI Act, ss 51, 51B). The time period for making a decision on an applicant's application is 30 calendar days. An applicant may apply for internal review or Information Commissioner review of an adverse decision.

13.27 While APP 13 sets out minimum procedural requirements (see paragraph 13.24), these are not as detailed as in the FOI Act. However, in two respects APP 13 goes further than the FOI Act:

- The grounds for correction in APP 13 are that the personal information is 'inaccurate, out-of-date, incomplete, irrelevant or misleading'. The main additional ground in this

[2] The FOI Act is expressed to apply separately to Minister's offices in respect of 'an official document of a Minister' (FOI Act, s 48). APP 13 also applies to Minister's offices: see the discussion of 'APP entity' in Chapter B (Key concepts), and the Privacy Act, s 7(1)(d),(e).

list is that the information is 'irrelevant'. The other wording difference — 'inaccurate' in APP 13, 'incorrect' in the FOI Act — is not substantive.

- If an agency corrects personal information, the agency must, if requested by the individual, take reasonable steps under APP 13 to notify that change to any APP entity to which the personal information was previously disclosed, unless it is unlawful or impracticable to do so (see paragraphs 13.49–13.53). Where an agency amends personal information under the FOI Act, an agency could consider providing similar notification on request from the individual.

13.28 The complaint options available to the individual under the FOI Act and APP 13 also differ. Under the FOI Act, a person may apply for Information Commissioner review of an agency's or Minister's failure to amend or annotate a record in accordance with the person's request. The Commissioner may exercise the agency's or Minister's discretion to amend or annotate a record. Under the Privacy Act, an individual may complain to the Information Commissioner about an APP entity's failure to take reasonable steps to correct personal information to ensure it is not incorrect. After investigation, the Commissioner may find that an agency has failed to take reasonable steps to correct personal information or to comply with the minimum procedural requirements (see paragraphs 13.54–13.65) under APP 13. The Commissioner may make a determination to that effect, and require, for example, the entity to correct personal information or to comply with the minimum procedural requirements (Privacy Act, s 52).

13.29 It is open to an individual to decide whether to make an application under the FOI Act or a request under APP 13. Agencies could ensure, in appropriate cases, that people are made aware of both options and the substantive differences. An agency could refer to the FOI Act in the agency's APP Privacy Policy. More detailed information could be provided by an agency in other ways — such as a separate document that sets out the procedure for requesting correction of personal information (see paragraph 13.21), through an 'Access to information' icon on the agency's website,[3] or on a case-by-case basis as the need arises. An agency could draw attention to the more flexible procedure for which APP 13 provides. As explained in the FOI Guidelines,[4] agencies should consider establishing administrative access arrangements that operate alongside the FOI Act and that provide an easier and less formal means for individuals to make information access requests (including requests to correct personal information). Correcting or annotating personal information under an administrative arrangement is consistent with an agency's obligations under APP 13, provided the agency meets the minimum procedural requirements stipulated in APP 13.

Grounds for correcting personal information

13.30 The five grounds listed in APP 13 — 'accurate', 'up-to-date', 'complete', 'relevant' and 'not misleading' — are not defined in the Privacy Act. The first four terms are listed in APP 10.1, which deals with the quality of personal information that an APP entity can collect, use and disclose. Similar terms are used also in Part V of the FOI Act concerning a person's right to apply to an agency to amend or annotate personal information (see paragraph 13.26 above).

[3] See OAIC, Guidance for Agency Websites: 'Access to Information' Web Page, OAIC website <https://www.oaic.gov.au>.

[4] OAIC, FOI Guidelines, Part 3, OAIC website <https://www.oaic.gov.au>.

13.31 The following analysis of each term draws on the ordinary dictionary meaning of the terms, as well as case law concerning the meaning of those terms in the Privacy Act, FOI Act and other legislation.[5] As the analysis indicates, there is considerable overlap in the meaning of the terms.

13.32 In applying the terms to personal information, it is necessary to have regard to 'the purpose for which it is held'. Personal information may be incorrect having regard to one purpose for which it is held, but not another. For a discussion of relevant considerations where personal information is held for multiple purposes, see paragraph 13.47.

Accurate

13.33 Personal information is inaccurate if it contains an error or defect. An example is incorrect factual information about an individual's name, date of birth, residential address or current or former employment.[6]

13.34 An opinion about an individual given by a third party is not inaccurate by reason only that the individual disagrees with that opinion or advice.[7] For APP 13 purposes, the opinion may be 'accurate' if it is presented as an opinion and not objective fact, it accurately records the view held by the third party, and is an informed assessment that takes into account competing facts and views. Other matters to consider under APP 13, where there is disagreement with the soundness of an opinion, are whether the opinion is 'up-to-date', 'complete', 'not misleading' or 'relevant'. If an individual disagrees with an opinion that is otherwise not incorrect, the individual may associate a statement with the record of the opinion (see paragraphs 13.59–13.62).

13.35 In relation to a similar issue, s 55M of the FOI Act provides that the Information Commissioner (in conducting an IC review) cannot alter a record of opinion unless satisfied that it was based on a mistake of fact, or the author of the opinion was biased, unqualified to form the opinion or acted improperly in conducting the factual inquiries that led to the formation of the opinion.

Up-to-date

13.36 Personal information is out-of-date if it contains facts, opinions or other information that is no longer current. An example is a statement that an individual lacks a particular qualification or accreditation that the individual has subsequently obtained.

13.37 Personal information about a past event may have been accurate at the time it was recorded, but has been overtaken by a later development. Whether that information is out-of-date will depend on the purpose for which it is held. If current information is required for the particular purpose, the information will to that extent be out-of-date. By contrast, if information from a past point in time is required for the particular purpose, the information may not be out-of-date for that purpose. Personal information held by an APP entity that is

[5] OAIC, FOI Guidelines, Part 7 — Amendment and Annotation of Personal Records, OAIC website <https://www.oaic.gov.au>; and 'S' and Veda Advantage Information Services and Solutions Limited [2012] AICmr 33 (20 December 2012).

[6] Personal information is also inaccurate if it is misleading. See Australian Government, Companion Guide: Australian Privacy Principles, June 2010, p 14, Parliament of Australia website <https://www.aph.gov.au>.

[7] The definition of 'personal information' in the Privacy Act includes 'information or an opinion' (s 6(1)).

no longer needed for any purpose may need to be destroyed or de-identified under APP 11.2 (Chapter 11 (APP 11)).

Complete

13.38 Personal information is incomplete if it presents a partial or misleading picture, rather than a true or full picture. An example is a tenancy database which records that a tenant owes a debt, which in fact has since been repaid. The statement will be incomplete under APP 13 if the tenancy database is held for the purpose of assessing the tenancy record or reliability of individuals recorded in the database. Similarly, a statement that an individual has only two rather than three children will be incomplete under APP 13 if that information is held for the purpose of, and is relevant to, assessing a person's eligibility for a benefit or service.

Relevant

13.39 Personal information is irrelevant if it does not have a bearing upon or connection to the purpose for which the information is held.

Not misleading

13.40 Personal information is misleading if it conveys a meaning that is untrue or inaccurate or could lead a user, receiver or reader of the information into error. An example is a statement that is presented as a statement of fact but in truth is a record of the opinion of a third party. In some circumstances an opinion may be misleading if it fails to include information about the limited facts on which the opinion was based or the context or circumstances in which the opinion was first recorded.

13.41 A statement may also be misleading by failing to include other relevant information. An example is a statement that a dismissed employee was reinstated, without explaining that this followed the ruling of a court or tribunal that the dismissal was legally flawed.[8]

Being satisfied and taking reasonable steps

13.42 An APP entity is required to take 'reasonable steps' to correct personal information when 'satisfied' that it is inaccurate, out-of-date, incomplete, irrelevant or misleading for the purpose for which it is held.

Being satisfied

13.43 This requirement will not always involve distinct analysis or decision by an APP entity. For example, if an entity maintains an online portal through which a person can access and correct their personal information, no additional step may be required by the entity. Correction may similarly be a straightforward process in other situations where, for example, an individual presents information to indicate that their personal information is incorrect in an entity's records.

[8] An organisation that is or was an employer of an individual is exempt from the operation of the Privacy Act where its act or practice is related directly to the employment relationship between the organisation and the individual, and an employee record held by the organisation (s 7B(3)).

13.44 Where correction is requested by an individual and an APP entity requires further information or explanation before it can be satisfied that personal information is incorrect, the entity should clearly explain to the individual what additional information or explanation is required and/or why the entity cannot act on the information already provided. The entity could also advise where additional material may be obtained. The individual should be given a reasonable opportunity to comment on the refusal or reluctance of the entity to make a correction without further information or explanation from the individual.

13.45 An APP entity should also be prepared in an appropriate case to search its own records and other readily-accessible sources that it reasonably expects to contain relevant information to find any information in support of, or contrary to the individual's request. For example, an entity could take into account a finding of an Australian court or tribunal relating to the personal information that has a bearing on whether it is or is not incorrect. However, an entity need not conduct a full, formal investigation into the matters about which the individual requests correction. The extent of the investigation required will depend on the circumstances, including the seriousness of any adverse consequences for the individual if the personal information is not corrected as requested.

13.46 Where personal information is held for multiple purposes, an APP entity need only be satisfied that the personal information requires correction having regard to one of the purposes for which it is held, not all purposes (see paragraph 13.46).

Reasonable steps to correct

13.47 A decision as to what constitutes 'reasonable steps' to correct personal information spans a range of options. These include making appropriate additions, deletions or alterations to a record, or declining to correct personal information if it would be unreasonable to take such steps. In some instances it may be appropriate to destroy or de-identify the personal information (there are separate requirements to destroy or de-identify personal information in APPs 4 and 11 — see Chapters 4 and 11 respectively). The reasonable steps that an APP entity should take will depend upon considerations that include:

- the sensitivity of the personal information. More rigorous steps may be required if the incorrect 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 possible adverse consequences for an individual if a correction is not made. More rigorous steps may be required as the risk of adversity increases.
- the practicability, including time and cost involved. However, an entity is not excused from correcting 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.
- the likelihood that the entity will use or disclose the personal information. For example, the likelihood of the entity using or disclosing the personal information may be relevant if it would be difficult or costly to make the correction requested by an individual.
- the purpose for which the personal information is held. As noted at paragraph 13.32, personal information may be held for multiple purposes, and require correction for one purpose but not for another purpose. Reasonable steps in these circumstances may

require the entity to retain the original record of personal information for one purpose and create a record with the corrected personal information for another.

- record-keeping requirements that apply to the personal information under an Australian law or court/ tribunal order. For example, the Health Practitioner Regulation 2010 (NSW), Schedule 2, clause 2.
- whether the personal information is in the physical possession of the entity or a third party. For example, where personal information is in the physical possession of a third party, the entity may still 'hold' it (see discussion of 'holds' at paragraph 13.11) and be required to take reasonable steps to correct it. In these circumstances, it may be a reasonable step for the entity to notify the third party that the information is incorrect and request that it be corrected. It will not generally be sufficient to refer the individual to the third party with physical possession. However, the third party with physical possession may also 'hold' the personal information, and if so, the individual will have a separate right to request the third party to correct it.

13.48 Special considerations apply to Commonwealth records. The term 'Commonwealth record' is defined in s 3 of the Archives Act and is discussed in more detail in Chapter B (Key concepts).[9] The definition is likely to include, in almost all cases, all personal information held by agencies. It may also include personal information held by contracted service providers. A Commonwealth record can, as a general rule, only be destroyed or altered in accordance with s 24 of the Archives Act. Further, s 26 of the Archives Act makes it an offence to alter a Commonwealth record that is over 15 years old.[10] In relation to such records, and more generally, it may be reasonable (and consistent with statutory requirements) to:

- retain a version of a record which contains incorrect personal information (see paragraph 13.47)
- associate a statement to clarify that, having regard to the purpose for which the personal information is held, the personal information is not accurate, up-to-date, complete, relevant or is misleading, and either including the correct personal information in the note or cross referencing where it is held (such as in an attachment to the record)

APP 13 minimum procedural requirements

Taking reasonable steps to notify another APP entity

13.49 APP 13.2 provides that an APP entity must, on request, take reasonable steps to notify another APP entity of a correction made to personal information that was previously provided to that entity, unless it is impracticable or unlawful to do so. Implicit in this requirement is that an entity should take reasonable steps to inform the individual that

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

[10] See Archives Act 1983, s 26.

they can make such a request. This information could be provided, for example, at the time, or as soon as practicable after, a correction is made.

13.50 The reasonable steps for an APP entity will depend upon considerations that include:

- the sensitivity of the personal information. More rigorous steps may be required for 'sensitive information' (defined in s 6(1) and discussed in Chapter B (Key concepts)) or other personal information of a sensitive nature.
- the possible adverse consequences for an individual if notice is not provided to the other entity. More rigorous steps may be required as the risk of adversity increases.
- the nature or importance of the correction. For example, it may not be reasonable to provide notice of a small typographical error that does not materially affect the quality of the personal information.
- the length of time that has elapsed since the personal information was disclosed to the other entity, and the likelihood that it is still being used or disclosed by the other entity
- the materiality of the correction
- the practicability of providing notice to another entity. For example, it may be impracticable to do so if the other entity has ceased carrying on business or has been substantially restructured.
- the practicability, including time and cost of providing a notice to all entities to which the personal information was previously provided. However, an entity is not excused from giving notification 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.

13.51 An APP entity is not required to provide notice of a correction if it would be impracticable or unlawful to do so. Impracticability is addressed in the list at paragraph 13.50. An entity should consider whether it would be practicable to notify some but not all of the other APP entities to which the entity previously disclosed the personal information. In these circumstances, the entity could discuss with the individual whether there are particular entities that they wish to be notified.

13.52 The term 'unlawful' is not defined in the Privacy Act. The core meaning is activity that is criminal, illegal or prohibited or proscribed by law, and can include unlawful discrimination or harassment, but does not include breach of a contract. An example of when it would be unlawful to notify another APP entity is when a statutory secrecy provision prevents an agency from taking this step.

13.53 An APP entity that is notified of a correction should, in turn, consider whether to correct the personal information that it holds. As noted at paragraphs 13.16–13.18, an APP entity is required on its own initiative to take reasonable steps to correct incorrect personal information.

Giving written notice where correction is refused

13.54 APP 13.3 provides that if an APP entity refuses to correct personal information as requested by an individual, the entity must give the individual a written notice setting out:

- the reasons for the refusal, except to the extent that it would be unreasonable to do so
- the complaint mechanisms available to the individual, and

- any other matters prescribed by regulations made under the Privacy Act

13.55 The reasons for refusal should explain, where applicable:

- that the APP entity does not hold the personal information that the individual wishes to correct
- that the entity is satisfied that the personal information it holds is accurate, up-to-date, complete, relevant and not misleading having regard to the purposes for which it is held, or
- that the steps necessary to correct the personal information as requested are not reasonable in the circumstances

13.56 An APP entity is not required to provide its reasons for refusing to correct personal information to the extent that it would be unreasonable to do so. This course should be adopted only in justifiable circumstances. An example would be where providing reasons would prejudice an investigation of unlawful activity, or prejudice enforcement action by an enforcement body.

13.57 The description of the complaint mechanisms available to an individual should explain the internal and external complaint options, and the steps that should be followed. In particular, the individual should be advised that:

- a complaint should first be made in writing to the APP entity (s 40(1A))
- the entity should be given a reasonable time (usually 30 days) to respond
- a complaint may then be taken to a recognised external dispute resolution scheme of which the entity is a member (if any), and
- lastly, that a complaint may be made to the Information Commissioner (s 36)

13.58 Other information can also be included in the notice advising an individual that a request to correct personal information has been refused. The individual should be advised of the right under APP 13.4 to request the APP entity to associate a statement with the personal information (see paragraphs 13.59–13.62). An agency could also advise an individual of the parallel right under the FOI Act to apply for a record to be amended or annotated, and of the right to Information Commissioner review of an adverse decision under that Act (see paragraphs 13.25–13.29).

Taking reasonable steps to associate a statement

13.59 APP 13.4 provides that if an APP entity refuses to correct personal information as requested by an individual, the individual can request the entity to associate a statement that the individual believes the personal information to be inaccurate, out-of-date, incomplete, irrelevant or misleading. Implicit in this requirement is that the entity should notify the individual of the right to request that a statement be associated, for example, in the written notice where correction is refused (see paragraphs 13.54–13.58).

13.60 The APP entity must take reasonable steps to associate the statement in a way that will make it apparent to users of the personal information. For example, a statement may be attached physically to a paper record, or by an electronic link to a digital record of personal information. The statement should be associated with all records containing personal information claimed to be incorrect.

13.61 The content and length of any statement will depend on the circumstances, but it is not intended that the statement be unreasonably lengthy.[11] A longer statement may be appropriate in some instances, such as where there is a large volume of personal information that the APP entity has refused to correct. If it is not practicable to attach an extensive statement to the personal information or otherwise create a link to the statement, a note could be included on, or attached to, the personal information referring to the statement and explaining where it can be found. Where it is not reasonable for the entity to associate an extensive statement to the personal information, reasonable steps would generally include giving the individual an opportunity to revise the statement.

13.62 The reasonable steps for an APP entity will depend upon considerations that include:

- the information management practices of the entity, including whether the personal information is stored in hard copy or electronic form (see paragraph 13.59)
- whether content in a statement may be irrelevant, defamatory, offensive, abusive or breach another individual's privacy — it may be unreasonable to associate a statement containing that content, however the individual should be given the option of revising the statement
- the practicability, including time and cost involved. However, an entity is not excused from associating a statement 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.

Timeframe for responding to a request for correction under APP 13

13.63 APP 13.5 provides that an agency must respond to a request to correct a record or to associate a statement within 30 calendar days. The 30 day time period commences on the day after the day the agency receives the request. An organisation must respond within a reasonable period after the request is made. As a general guide, a reasonable period should not exceed 30 calendar days.

13.64 The APP entity must respond by correcting the personal information as requested by the individual, or by notifying the individual of its refusal to correct it.

Access charges under APP 13

13.65 An APP entity cannot impose any charge upon an individual for correcting personal information under APP 13. This includes:

- a charge for the making of the request to correct personal information
- a charge for making a correction or for associating a statement with the personal information (APP 13.5(b))

[11] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy) Bill 2012, p 88.