Chapter A:
Introductory matters

Version 1.2, July 2019

OAIC

Contents

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>