Australian Government

Office of the Australian Information Commissioner

Privacy (Australian Government Agencies — Governance) APP Code 2017

Made under the *Privacy Act 1988*

I, Timothy Pilgrim, Australian Information Commissioner, have developed the following APP code and included it on the Codes Register.

Dated 26 October 2017

Timothy Pilgrim

Australian Information Commissioner

Part 1—Introduction

1 Name

(1) This APP code may be cited as the *Privacy (Australian Government Agencies — Governance) APP Code 2017.*

(2) This APP code may also be cited as the *Australian Government Agencies Privacy Code*.

2 Commencement

This APP code comes into force on 1 July 2018.

3 Authority

This APP code has been developed under section 26G of the *Privacy Act 1988.*

4 Preamble

APP 1 is the foundation principle that assists agencies to achieve compliance with the APPs. Compliance with APP 1 is essential to ensure good privacy management and governance practices, which can build community trust and confidence in those practices.

APP 1 implicitly promotes a 'privacy by design' approach to ensure that privacy compliance is included in the design of information systems and practices from their inception. It does this by requiring agencies to take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs and any binding registered APP code.

5 Definitions

Note: A number of expressions used in this APP code are defined in the Act, and have the same meaning in this APP code, including the following:

(a) APP code;

(b) Commissioner;

(c) personal information;

(d) privacy impact assessment; and

(e) sensitive information.

In this APP code:

Act means the *Privacy Act 1988*.

Agency has the meaning given in section 6(1) of the Act, but for the purposes of this APP code, does not include a Minister.

APP means an Australian Privacy Principle as set out in the Act.

handling personal information means dealing with personal information in any way, including managing, collecting, holding, using or disclosing personal information.

OAIC means the Office of the Australian Information Commissioner.

PIA means privacy impact assessment.

Privacy Champion has the meaning given by section 11.

privacy management plan has the meaning given by section 9.

Privacy Officer has the meaning given by section 10.

6 Objectives

The objectives of this APP code are to:

(a) set out specific requirements that agencies must comply with as part of their compliance with APP 1.2;

(b) enhance the privacy capability and accountability of agencies;

(c) promote good privacy governance within agencies to create and embed a culture that respects privacy and treats personal information as a valuable asset; and

(d) build community trust and confidence in the personal information handling practices of agencies.

7 Agencies bound by this APP code

This APP code is binding on all agencies as defined in section 5 of this APP code.

Note: This APP code does not affect the operation of Part II, Division 3 of the Act which sets out the acts and practices which come within the scope of the Act and those acts and practices that do not come within the scope of the Act. As an example, section 7 of the Act sets out the extent to which a reference in the Act to an 'act or practice' is an act or practice of an agency for the purposes of the Act.

8 Application of this APP code to APP 1.2

For the purposes of paragraph 26C(2)(a) of the Act, Parts 2 to 4 of this APP code set out how APP 1.2 is to be complied with by agencies.

Note 1: Under subsection 40(2) of the Act the Commissioner, on his or her own initiative, may investigate an act or practice if the act of practice may be a breach of APP 1 and the Commissioner thinks it is desirable that the act or practice be investigated.

Note 2: In addition to complying with this APP code, an agency may need to take additional steps in order to satisfy its obligations under APP 1.2.

Part 2—Privacy management and governance

9 Privacy management plan

(1) An agency must have a privacy management plan.

(2) A privacy management plan is a document that:

(a) identifies specific, measurable privacy goals and targets; and

(b) sets out how an agency will meet its compliance obligations under APP 1.2.

(3) An agency must measure and document its performance against its privacy management plan at least annually.

10 Privacy Officer

(1) An agency must, at all times, have a designated Privacy Officer. An agency may have more than one Privacy Officer.

(2) An agency may designate an officer as a Privacy Officer by reference to a position or role, including by reference to a position or role in another agency.

(3) An agency must keep the OAIC notified in writing of the contact details for the Privacy Officer, or if an agency has more than one Privacy Officer, for one of those Privacy Officers.

(4) Privacy Officers are the primary point of contact for advice on privacy matters in an agency.

(5) An agency must ensure that the following Privacy Officer functions are carried out:

(a) handling of internal and external privacy enquiries, privacy complaints, and requests for access to and correction of personal information made under the Act;

(b) maintaining a record of the agency's personal information holdings;

(c) assisting with the preparation of PIAs conducted under section 12;

(d) maintaining the agency's register of PIAs as required by section 15; and

(e) measuring and documenting the agency's performance against the privacy management plan at least annually as required by section 9.

11 Privacy Champion

(1) An agency must, at all times, have a designated Privacy Champion.

(2) An agency may designate an officer as a Privacy Champion by reference to a position or role within the agency.

(3) The Privacy Champion must be a senior official within the agency.

(4) An agency must ensure that the following Privacy Champion functions are carried out:

(a) promoting a culture of privacy within the agency that values and protects personal information;

(b) providing leadership within the agency on broader strategic privacy issues;

(c) reviewing and/or approving the agency's privacy management plan, and documented reviews of the agency's progress against the privacy management plan; and

(d) providing regular reports to the agency's executive, including about any privacy issues arising from the agency's handling of personal information.

(5) An agency's designated Privacy Officer may also be its designated Privacy Champion.

PART 3—PIAs

12 Conduct of PIA

(1) An agency must conduct a PIA for all high privacy risk projects.

(2) For the purposes of this section, a project may be a high privacy risk project if the agency reasonably considers that the project involves any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals.

Note: 'Privacy impact assessment' is defined in section 33D of the Act. This section of the Act also requires an agency to conduct a PIA if directed to do so by the Commissioner.

13 Publication of PIA

An agency may publish a PIA conducted under section 12, or a summary version or an edited copy of the PIA, on the agency's website.

14 Joint PIA

If two or more agencies participate in the same project, they may conduct a joint PIA. Each agency must retain a copy of the PIA.

15 Register of PIAs

(1) An agency must maintain a register of the PIAs it conducts. An agency must publish the register, or a version of the register, on its website.

(2) An agency may provide a copy of the register, and any PIAs that are listed on the register, to the Commissioner on request from the Commissioner.

PART 4—Internal privacy capability

16 Privacy education and training

(1) An agency must include appropriate privacy education or training in any staff induction program it provides. The privacy education must address the privacy obligations of agency staff, and agency policies and procedures relating to privacy.

(2) An agency must take reasonable steps to provide appropriate privacy education or training annually to all staff who have access to personal information in the course of performing their duties as a staff member.

17 Regular review of internal privacy processes

(1) An agency must regularly review and update its privacy practices, procedures and systems, to ensure their currency and adequacy for the purposes of compliance with the APPs. The scope of the review must include any:

(a) privacy policy prepared for the purposes of APP 1; and

(b) privacy notice prepared for the purposes of APP 5.

(2) An agency must monitor compliance with its privacy practices, procedures and systems regularly.