Australian Government

Office of the Australian Information Commissioner

EXPLANATORY STATEMENT

Privacy (Australian Government Agencies — Governance) APP Code 2017

Issued by the authority of the Australian Information Commissioner (Commissioner) under the *Privacy Act 1988* (Privacy Act).

The Privacy (Australian Government Agencies — Governance) APP Code 2017 (**the Australian Government Agencies Privacy Code**) has been developed by the Commissioner and included on the Codes Register. It is a registered APP code for the purposes of the Privacy Act.

Purpose

The Australian Government Agencies Privacy Code sets out how agencies are to apply and comply with one of the Australian Privacy Principles (APPs), specifies the APP entities (agencies) that are bound by the Code, and sets out the period during which the Code is in force.

The Australian Government Agencies Privacy Code only applies to APP entities that are agencies. For the purposes of this code, 'agency' has the same meaning as provided in section 6(1) of the Privacy Act, but does not include a Minister.

The Commissioner is satisfied that the making of the Australian Government Agencies Privacy Code is in the public interest in accordance with section 26G(2) of the Privacy Act, and has set out the relevant policy objectives of the Code in section 6. In summary, the Code requires agencies to move towards a best practice approach to privacy governance, by ensuring consistent implementation of the key practices, procedures and systems required under APP 1.2.

The effective implementation of APP 1.2 will enhance agencies' existing privacy capability, build greater transparency in information handling practices, and foster a culture of respect for privacy and the value of personal information. The Code therefore symbolises the commitment of Australian Government agencies to the protection of privacy, and will help build public trust and confidence in information handling practices and any new uses of data proposed by agencies.

Background

An APP code may be developed by APP code developers (either on their own initiative or following a request from the Commissioner) or by the Commissioner. In the case of the Australian Government Agencies Privacy Code, the Commissioner has developed this APP code in accordance with section 26G of the Privacy Act.

APP codes do not replace the APPs, but operate in addition to the requirements of the APPs. An APP code must set out how one or more of the APPs are to be applied or complied with. An APP code may also deal with other relevant matters, and may impose additional requirements to those imposed by the APPs, so long as the additional requirements are not contrary to, or inconsistent with, the APPs.

An APP entity that is bound by a registered APP code must not do an act, or engage in a practice, that breaches the registered APP code. A breach of a registered APP code will be an interference with privacy by the entity under section 13 of the Privacy Act and subject to investigation by the Commissioner under Part 5 of the Privacy Act.

Any APP code that is registered will be a disallowable legislative instrument.

Statement of compatibility with human rights

Subsection 9(1) of the *Human Rights (Parliamentary Scrutiny) Act 2011* requires the rule-maker in relation to a legislative instrument to which section 42 (disallowance) of the *Legislation Act 2003* applies to cause a statement of compatibility to be prepared in respect of that legislative instrument. The statement of compatibility set out below has been prepared to meet that requirement.

Consultation

The Commissioner has consulted on the development of the Australian Government Agencies Privacy Code in accordance with subsection 26G(3) of the Privacy Act (and section 17 of the *Legislation Act 2003*).

The Commissioner made a draft of the Australian Government Agencies Privacy Code publicly available on the Office of the Australian Information Commissioner's website from 30 June 2017 to 11 August 2017 and invited the public to make submissions, thereby satisfying the requirement that a draft be made publicly available for a period of at least 28 days. In addition, in May 2017 the Commissioner contacted the Secretaries of all Australian Government departments by email to notify them of his intention to develop the Code. The Commissioner also requested that departments notify their portfolio agencies of his intention to develop the Code, and invite them to participate in the consultation process.

The Commissioner has given consideration to the submissions received during the consultation period before registering this APP code. In response to the matters raised in the submissions received, the Commissioner has made a number of amendments to the Code, including:

- revising the name of the Code, to better reflect the nature of the entities subject to the Code (section 1)
- excluding Ministers from the operation of the Code (section 5)
- clarifying that an agency can appoint more than one Privacy Officer, depending on the size and nature of an agency (section 10)
- clarifying that an agency may appoint a Privacy Officer from another agency (section 10)
- providing a more general statement about when a project will be 'a high privacy risk' project for the purposes of conducting a privacy impact assessment (PIA) (section 12)
- removing the requirement to publish PIAs, and instead including a requirement to publish the PIA register (or a version of the register) (section 15), and
- clarifying the requirements in relation to the provision of privacy education or training (section 16).

Commencement

An APP code cannot come into force before it is included on the Codes Register (paragraph 26C(2)(c) of the Privacy Act) and subsection 12(2) (retrospective application of legislative instruments) of the *Legislation Act 2003* does not apply to a registered APP code.

This Australian Government Agencies Privacy Code comes into force on 1 July 2018 and will remain in force until it is repealed.

Explanation of sections

In section 5 there is a recognition that a number of terms used in the APP code are defined in the Privacy Act. Agency has the meaning given in section 6(1) of the Privacy Act, but for the purposes of the Code, does not include a Minister. Further definitions are set out in that section.

The objectives of the Australian Government Agencies Privacy Code are set out in section 6, and 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.

Section 7 is in compliance with paragraph 26C(2)(b) of the Privacy Act and specifies that the APP code is binding on all agencies as defined in section 5 of the Code. The note to that section is to recognise that there are a number of acts and practices that an agency may undertake that are excluded from the scope of operation of the Privacy Act. The Australian Government Agencies Privacy Code is not intended to impact on any of those exclusions.

The Australian Government Agencies Privacy Code does not apply to entities that are not agencies. The nature of the obligations set out in the Australian Government Agencies Privacy Code also means that it is not part of an agency's privacy obligations to contractually impose the obligations under this code on a contracted service provider under section 95B of the Privacy Act.

Section 8 is in compliance with paragraph 26C(2)(a) of the Privacy Act and sets out how APP 1.2 is to be applied or complied with. For the purposes of paragraph 26C(2)(a) of the Privacy Act, agencies must apply Parts 2 to 4 of this Australian Government Agencies Privacy Code as part of meeting their obligations under APP 1.2. In addition to complying with Parts 2 to 4 of the Code, agencies may need to take other steps to ensure compliance with APP 1.2.

The note to section 8 is in recognition that the obligation to comply with an APP code is reflected in APP 1.2. Under subsection 40(2) of the Privacy Act the Commissioner, on his or her own initiative, may investigate an act or practice if the act or practice may be a breach of APP 1 and the Commissioner thinks it is desirable that the act or practice be investigated.

Section 9 imposes an obligation on an agency to have and maintain a privacy management plan. A privacy management plan is a key tool to assist an agency to meet its ongoing compliance obligations under APP 1.2. The Commissioner has published guidance material about privacy management plans on the OAIC website.

Section 10 sets out an obligation on an agency to have, and continue to have, a designated Privacy Officer or Officers. Section 10 also sets out the role of a Privacy Officer. Section 10 subsection 5 sets out a list of Privacy Officer functions that an agency must ensure performance of under the Code.

These functions may be performed by the Privacy Officer, or by another person. A Privacy Officer also acts as the primary point of contact for the OAIC.

Section 11 sets out an obligation on an agency to have, and continue to have, a designated Privacy Champion. An agency's Privacy Champion must be a senior official within that agency. Section 11 also sets out a list of Privacy Champion functions that an agency must ensure performance of under the Code. These functions may be performed by the Privacy Champion, or by another person.

Under section 12, an obligation is placed on agencies to consider whether a project is a high privacy risk project. 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. If a project is a high privacy risk project, the agency is under an obligation to conduct a PIA.

Consistent with the definition in section 33D of the Privacy Act, a PIA is a written assessment of an activity or function (or project) that identifies the impact that a project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact. PIAs are an important component in the protection of privacy, and should be part of the overall risk management and planning processes of APP entities.

Under section 13 an agency may publish a PIA, or may choose to publish a summary version or an edited copy of the PIA, on the agency's website.

Section 14 provides that where two or more agencies participate in the same project, they may conduct a joint PIA, but each agency must retain a copy of the PIA.

Section 15 imposes an obligation on an agency to maintain a register of the PIAs that it conducts. Agencies must publish this register, or a version of this register, on its website. Agencies should include all PIA titles and any other relevant information on the published register, unless doing so would divulge information that it would not be appropriate to share publicly, for example, for reasons of national security.

Section 16 of the Code codifies what many agencies are already doing as best practice. Section 16 imposes an obligation on agencies to include appropriate privacy education or training in any staff induction programs they provide.

An agency must also 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. The level and amount of privacy education or training that will be appropriate may differ between and within agencies, depending on the degree to which an agency's staff members deal with personal information in the course of their employment.

Section 17 imposes an obligation on an agency to review and update its privacy practices, procedures and systems regularly. The minimum scope of that review is also set out, and includes the agency's privacy policy and any privacy notices.

An agency must also regularly monitor compliance with its privacy practices, procedures and systems. The Commissioner expects agencies to consider (and where appropriate, to respond to) the outcomes of those compliance reviews in accordance with the APPs and its privacy management plan.

STATEMENT OF COMPATIBILITY FOR A DISALLOWABLE LEGISLATIVE INSTRUMENT THAT RAISES HUMAN RIGHTS ISSUES

Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011.*

Privacy (Australian Government Agencies — Governance) APP Code 2017

Issued by the authority of the Australian Information Commissioner (Commissioner) under the *Privacy Act 1988*.

This Disallowable Legislative Instrument is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview of the Privacy (Australian Government Agencies — Governance) APP Code 2017

The *Privacy (Australian Government Agencies — Governance) APP Code 2017* (the **Australian Government Agencies Privacy Code**) has been developed by the Commissioner and included on the Codes Register. It is a registered APP code for the purposes of the Privacy Act.

APP codes do not replace the Australian Privacy Principles (APPs), but operate in addition to the requirements of the APPs. An APP code must set out how one or more of the APPs are to be applied or complied with. An APP code may also deal with other relevant matters, and may impose additional requirements to those imposed by the APPs, so long as the additional requirements are not contrary to, or inconsistent with, the APPs.

An APP entity that is bound by a registered APP code must not do an act, or engage in a practice, that breaches the registered APP code. A breach of a registered APP code will be an interference with privacy by the entity under section 13 of the Privacy Act and subject to investigation by the Commissioner under Part 5 of the Privacy Act.

The Australian Government Agencies Privacy Code sets out how agencies (as defined in section 5 of the Code) are to apply and comply with one of the APPs, specifies the APP entities that are bound by the Code and sets out the period during which the Code is in force. The Australian Government Agencies Privacy Code only applies to APP entities that are agencies and therefore does not apply to private sector organisations.

The policy objectives of the Australian Government Agencies Privacy Code are set out in section 6. The objectives of the Australian Government Agencies Privacy 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.

Under the Australian Government Agencies Privacy Code, additional requirements are imposed on agencies, including obligations to conduct privacy impact assessments, have a privacy management plan, appoint a Privacy Officer and a Privacy Champion, and to provide privacy education or training at regular intervals, among other obligations.

Human rights implications

The Australian Government Agencies Privacy Code engages the following right:

- the right to privacy in Article 17 of the *International Covenant on Civil and Political Rights*.

The right to privacy is positively affected by the development and registration of the Australian Government Agencies Privacy Code.

The Australian Government Agencies Privacy Code positively affects the right to privacy through:

(a) the enhancement of privacy capability and accountability of agencies by imposing additional requirements and setting out specific requirements that agencies must undertake in complying with APP 1.2;

(b) the promotion of good privacy governance within agencies to create and embed a culture that respects privacy and treats personal information as a valuable asset; and

(c) contributing to community trust and confidence in the personal information handling practices of agencies.

Conclusion

The Disallowable Legislative Instrument is compatible with human rights because it promotes the protection of human rights through the enhancement of the right to privacy by providing another component of the privacy framework for agencies as they apply the Privacy Act in their acts and practices.