Australian Government

Office of the Australian Information Commissioner

Guidelines for developing codes

Issued under Part IIIB of the Privacy Act 1988

6 April 2023

OAIC

ISBN 978-1-877079-21-4

First issued under Part IIIB of the *Privacy Act 1988* on 27 September 2013.

These guidelines cover the development, registration and ongoing administration of Australian Privacy Principles (APP) codes and the Credit Reporting (CR) code.

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 publication: March 2023.

Creative Commons

Office of the Australian Information Commissioner

GPO Box 5288

Sydney NSW 2001

Phone: 1300 363 992www.oaic.gov.au

Acknowledgement of Country

The OAIC acknowledges Traditional Custodians of Country across Australia and recognises their continuing connection to lands, waters and communities. We pay our respect to Aboriginal and Torres Strait Islander cultures and to Elders past and present.

Contents

Key terms

The following terms used in these Guidelines are defined in s 6(1) of the *Privacy Act 1988* (Privacy Act):

- agency
- APP code developer
- APP entity
- credit provider
- credit reporting body
- credit reporting complaint
- CR code developer
- entity
- personal information.

The following terms used in these Guidelines are also defined in the Privacy Act (other than in s 6(1)):

- 'APP code' has the meaning given in s 26C of the Privacy Act.
- 'Australian Privacy Principles' is defined in s 14 of the Privacy Act as the principles set out in Schedule 1 to the Act.[1]
- 'Codes Register' has the meaning given by s 26U of the Privacy Act.
- 'CR code' has the meaning given by s 26N of the Privacy Act.
- 'Organisation' has the meaning given by ss 6C and 6E of the Privacy Act.
- 'Original registered code' has the meaning given by ss 26J(6) and 26T(5) of the Privacy Act.
- 'Registered APP code' has the meaning given by s 26B of the Privacy Act.
- 'Registered CR code' has the meaning given by s 26M of the Privacy Act.

The following terms used in the Guidelines are not defined in the Privacy Act:

- 'Code' means either an APP code or the CR code.
- 'Code administrator' (or 'code administration committee') is a body established to oversee the operation (including monitoring and reporting), of a code.

[1] The APPs set out standards, rights and obligations in relation to the handling and maintenance of personal information by APP entities, including dealing with privacy policies and the collection, storage, use, disclosure, quality and security of personal information, and access and correction rights of individuals in relation to their personal information.

- ‘Code developer’ (or ‘code development committee’) is a body that has responsibility for developing and seeking approval for the registration of a code.
- ‘Minister’ means the Commonwealth Attorney-General.
- ‘Privacy complaint’ means a complaint about the handling of personal information. This includes credit reporting complaints relating to the CR code.

Part 1: Introduction

The Privacy Act and codes

1.1 The *Privacy Act 1988* (Privacy Act)[2] contains 13 Australian Privacy Principles (APPs), which regulate the handling of personal information. The APPs apply to 'APP entities', which includes most Australian and Norfolk Island government agencies and many private sector and not for profit organisations. Part IIIA of the Privacy Act regulates the handling of consumer credit-related information and applies to credit reporting bodies (CRBs), credit providers and other entities in relation to their handling of consumer credit-related information.

1.2 Section 26V of the Privacy Act provides the Australian Information Commissioner (the Information Commissioner)[3] with the power to make written guidelines relating to codes.[4] In deciding whether to register a code, the Information Commissioner will consider whether the code meets the requirements set out in Part IIIB of the Privacy Act and in these guidelines.

1.3 Under Part IIIB of the Privacy Act, the Information Commissioner can approve and register enforceable codes of practice which are developed by entities on their own initiative or on request from the Information Commissioner, or developed by the Information Commissioner.

1.4 An APP code developer can develop a written code of practice for the handling of personal information, called an APP code. An APP code must set out how one or more of the APPs are to be applied or complied with, and the APP entities that are bound by the code.

1.5 The Privacy Act also requires the development of a code of practice about credit reporting, called the CR code. The CR code sets out how the Privacy Act's credit reporting provisions are to be applied or complied with by CRBs, credit providers and other entities bound by Part IIIA. There must always be a registered CR code.

1.6 Codes do not replace the relevant provisions of the Privacy Act, but operate in addition to the requirements of the Privacy Act. A code cannot lessen the privacy rights of an individual provided for in the Privacy Act. Registered codes are disallowable legislative instruments.

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

1.8 As a breach of any provision of a registered code is an interference with the privacy of an individual, a code should limit itself to provisions which outline the specific obligations of entities' bound by the code. For example, for APP codes this would cover obligations about how one or more APPs are to be applied or complied with, or to particularise requirements of

[2] In this guide, unless otherwise indicated, any references to sections of an Act are to sections of the Privacy Act.

[3] The Australian Information Commissioner is the head of the Office of the Australian Information Commissioner. More information is available at: www.oaic.gov.au.

[4] Under subsection 28(1)(c)(ii)–(iv), the Information Commissioner also has guidance related functions for promoting an understanding and acceptance of a registered APP code and the registered CR code.

[5] Privacy Act, ss 26A (APP codes) and 26L (CR code).

personal information handling than required by one or more of the APPs, so long as the additional requirements are not contrary to the APPs. It would also cover other matters that an APP code must address, which includes specifying the APP entities that are bound by the code, or a way of determining the APP entities that are bound by the code, and the period during which the code is in force (s 26C(2)). Other administrative and governance issues should be dealt with separately (see Part 3 on Code governance).

Who should use these guidelines?

1.9 These guidelines should be used by entities that are:

- considering developing a code
- developing a code on their own initiative or following a request from the Information Commissioner
- developing an application to vary or amend a code
- a code administrator (persons or bodies responsible for overseeing the ongoing administration of a code)

Purpose of these guidelines

1.10 These guidelines:

- will assist an APP entity to decide whether it is appropriate for them to develop an APP code
- clarify when the Information Commissioner will request an entity to develop a code, or when the Information Commissioner will develop a code on their own initiative
- outline matters that need to be addressed in the development and registration of a code
- outline matters the Information Commissioner may consider in deciding whether to register or vary a code
- outline matters related to reviewing, varying and removing registered codes.

Why develop an APP code?

1.11 The fundamental purpose of an APP code is to provide detailed information about the application of, or compliance with, the APPs.[6] At a minimum, an APP code must set out how one or more of the APPs are to be applied or complied with. An APP code should not merely replicate the requirements of the APPs. An APP code may also impose additional requirements to those in the APPs and/or cover certain exemptions. As such, reasons for developing an APP code may include:

[6] Explanatory Memorandum, Privacy Legislation Amendment (Enhancing Privacy Protection) Bill 2012, p 200.

- providing greater clarity of how particular APPs are applied or complied with in a specific industry context or in relation to new and emerging technologies which entities bound by the code utilise
- incorporating higher standards for privacy protection than the Privacy Act requires, including covering certain exempt acts or practices or providing for additional obligations to those in the APPs or Part IIIB, so long as those additional requirements are not contrary to, or inconsistent with the APPs or Part IIIB[7]
- assisting in promoting cultural change in an industry sector in relation to personal information handling

1.12 In deciding whether to develop an APP code, an entity should also consider:

- whether existing legislation, regulation or a code covers the same or similar topics that may negate the need to develop an APP code or may be suitable for adoption without the need to develop a separate APP code
- whether entities that will be bound by the APP code have sufficient resources to implement the code's requirements and whether there are sufficient resources available to develop and administer the APP code

1.13 Entities planning to develop an APP code are encouraged to first gain a detailed understanding of the Privacy Act and the APPs. Information to assist entities is available on the Office of the Australian Information Commissioner (OAIC) website.

1.14 A code developer should have in place properly resourced administrative mechanisms to develop the code. This may include forming a code development committee or some other administrative mechanism to manage the development of a code. Where possible, this mechanism should include relevant stakeholder groups and be transparent in its operations.

Resource requirements

1.15 Developing and implementing a code requires resources. A code developer must determine how these resources are obtained and managed at the time of the code's development. The following list outlines where resources may need to be allocated:

- investigating the need for a code
- establishing an administrative mechanism responsible for developing the code
- scoping and drafting the code
- seeking legal or professional advice
- involving stakeholders (including consumers) in effective consultations on the draft code and applications to vary the code

[7] For example, this would allow entities and industries which operate in overseas jurisdictions, where higher privacy standards apply, to match those higher standards in their Australian operations. See Privacy Act, s26C(3)(a).

- establishing and financing a code administrator to oversee the operation of the code, including responding to enquiries from entities bound by the code, reporting on the operation of the code and if applicable, initiating regular reviews of the code
- developing applications to vary the code for approval by the Information Commissioner, where applicable
- maintaining information about the code on a website, including a list of the entities bound by the code, where relevant.

Getting help – what the Office of the Australian Information Commissioner can do

1.16 In the first instance, a code developer should consult these guidelines, the Privacy Act and related publications.

1.17 A code developer should notify the Information Commissioner of their intention to develop a code. This will enable discussion about whether there is a need for a code, and whether the matters that the code developer proposes to address in a code are appropriate in the circumstances.

1.18 A code developer should also keep the OAIC informed throughout the code development process.

1.19 A code developer should engage with OAIC staff to obtain general (non-legal) advice and guidance during the development of a code. This includes guidance as to the content and drafting of a code. However, any advice would not fetter the discretion of the Information Commissioner in deciding whether to register the code.

1.20 The code developer should consider advice or guidance provided by the OAIC before submitting a code to the Information Commissioner for approval.

1.21 If requested, the OAIC will consider publishing information about the proposed code to assist stakeholder consultation.

Part 2: Developing codes

Getting Code requirements under the Privacy Act

2.1 The Privacy Act sets out minimum requirements of what must be included in an APP code and the CR code. It also sets out other matters that may be included in an APP code and the CR code.

2.2 An APP or CR code does not replace the relevant provisions of the Privacy Act, but operates in addition to the requirements of the Privacy Act.

2.3 As a breach of any provision of a registered code is an interference with the privacy of an individual, a code should limit itself to provisions which outline the specific privacy-related obligations of entities' bound by the code and any mandatory requirements under the Privacy

Act. To the extent that a code developer wishes to deal with matters that are unrelated to information privacy when developing a code, these matters would not form part of the code to be registered by the Information Commissioner.[8]

APP codes

2.4 An APP code developer may develop an APP code either on their own initiative or following a request from the Information Commissioner.[9]

2.5 Section 26C outlines what an APP code must do and what other matters it may deal with. An APP code must:

- be in writing
- be about information privacy
- set out how one or more of the APPs are to be applied or complied with
- specify the APP entities that are bound by the code, or a way of determining the APP entities that are bound by the code. An APP code is binding upon subscribers to the code, so it is essential that the code enables the subscribers to the code to be identified. It will be a matter for the Commissioner to determine, when considering registration of the code, whether a way used to determine entities bound by the code is sufficiently clear and specific. [10]
- set out the period during which the code is in force (which must not start before the day the code is registered on the Codes Register)

2.6 Generally, an APP code will commence operation on registration. However, a code may also include a specific commencement date,[11] or a specific timeframe for commencement after registration (for example, the code may specify that it will commence 6 months from the date of registration on the Codes Register) to provide time for implementation activities. For example, to undertake training for entities bound by the code, or for the development of resources or procedures under the code, to ensure entities are able to comply with the code's requirements once it comes into force.[12]

2.7 Similarly, a code will continue to be in force until it is removed from the register. However, a code developer may specify a period for which the code will be in force. For example, the code will be in force for 5 years from the day of registration.

---

[8] Explanatory Memorandum, Privacy Legislation Amendment (Enhancing Privacy Protection) Bill 2012, p 200.

[9] See ss 26E(1) and 26E(2) of the Privacy Act.

[10] See s 26C(2)(b) of the Privacy Act and the Explanatory Memorandum, Privacy Legislation Amendment (Enhancing Privacy Protection) Bill 2012, p 200.

[11] See s 26C(2)(b) of the Privacy Act and the Explanatory Memorandum, Privacy Legislation Amendment (Enhancing Privacy Protection) Bill 2012, p 200

[12] See s 26C(2)(c) of the Privacy Act and the Explanatory Memorandum, Privacy Legislation Amendment (Enhancing Privacy Protection) Bill 2012, p 201.

The CR code

2.8 The Information Commissioner may request an appropriate entity to develop the CR code.[13]

2.9 The CR code must:

- be in writing
- be about credit reporting
- set out how the provisions of Part IIIA are to be applied or complied with
- make provision for, or in relation to, matters required or permitted by Part IIIA to be provided for by the registered CR code
- bind all CRBs
- specify credit providers and other entities bound by the code, or specific parts of the code, or specify a way of determining those entities

2.10 The CR code does not need to deal with all the provisions of Part IIIA. However, there are provisions in Part IIIA which specify matters that must be contained in the CR code, or matters which the CR code is permitted to address. The Explanatory Memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 also specifies matters which the CR code is expected to deal with.[14] Amendments to the Privacy Act may also necessitate updates to the CR code.

Other matters that may be included in a code

APP codes

2.11 Section 26C(3) states that an APP code may:

- impose additional requirements to those imposed by one or more of the APPs, so long as the additional requirements are not contrary to, or inconsistent with, any of the APPs. An APP code cannot derogate from the obligations imposed by the APPs. Entities bound by an APP code must always comply with the APPs as well as the obligations imposed by a code to which they are bound
- cover exempt acts or practices (discussed below)
- deal with the internal handling of privacy complaints by all the entities bound by the code and provide for reporting to the Information Commissioner about those complaints (see Part 4)
- deal with any other relevant matters. These must be relevant to privacy in general and the APPs in particular

[13] See s 26P(1) of the Privacy Act.

[14] Explanatory Memorandum, Privacy Legislation Amendment (Enhancing Privacy Protection) Bill 2012, p 208.

2.12 Section 26C(4) states that an APP code may also be expressed to apply to any one or more of the following:

- all personal information or a specified type of personal information
- a specified activity, or a specified class of activities, of an APP entity
- a specified industry or profession, or a specified class of industries or professions
- APP entities that use technology of a specified kind[15]

2.13 The purpose of the code will generally dictate the types of personal information, activities, industry or technology that the code covers.

The CR code

2.14 Section 26N(3) states that the CR code may:

- impose additional requirements to those imposed by Part IIIA, so long as the additional requirements are not contrary to, or inconsistent with, that Part
- deal with the internal handling of privacy complaints by all the entities bound by the code and provide for the reporting to the Information Commissioner about these privacy complaints (see Part 4)
- deal with any other relevant matters (which must be relevant to credit reporting and, specifically, Part IIIA)

2.15 Section 26N(4) states that the CR code may be expressed to apply differently in relation to:

- classes of entities that are subject to Part IIIA
- specified classes of credit information, credit reporting information or credit eligibility information
- specified classes of activities of entities that are subject to Part IIIA

2.16 The ability for the CR code to apply differently in relation to those matters will allow sufficient flexibility for the CR code to provide detailed guidance about how the provisions of Part IIIA may be applied or complied with.

APP codes covering exempt acts or practices

2.17 An APP code developer may include obligations in an APP code that deal with certain acts or practices that would otherwise be exempt under the Privacy Act.[16] For example, exempt acts or

[15] For example, a code developer may wish to prepare a code that deals with one or more types of biometrics technologies which would be specified in the code.

[16] This provision covers exempts acts or practices within the meaning of s 7B(1), (2) or (3), see also s 26C(3)(b) of the Privacy Act.

practices that may be the subject of an APP code include the handling of employee records by organisations.

2.18 If a registered APP code covers exempt acts or practices, the Privacy Act will apply to those acts or practices as if they were not exempt.[17]

Consultation on codes

2.19 Under the Privacy Act, a code developer is required to undertake a public consultation before making an application to register a code.[18] Specifically, a code developer must:

- make a draft of the code publicly available, for example on the code developer's website or some other suitable website
- invite the public to make submissions to the developer about the draft within a specified period (which must run for at least 28 days) to ensure that members of the public have sufficient time to consider the draft of the code
- give consideration to any submissions made within the specified period

2.20 The 28 day consultation period is the minimum period that must be offered, but a code developer may consider a longer period, depending on:

- the expected level of interest in the code
- the number of expected stakeholders
- the complexity of the code
- the expected impact of the provisions in the code on the practices or procedures of stakeholders[19]

2.21 A code developer should, where practicable, notify all entities proposed to be bound by the code. A code developer should also bring the draft code to the attention of stakeholders to ensure that they are aware of the public consultation period and that they are aware why the code is being developed and what it intends to achieve. Relevant stakeholders may include:

- individuals and entities that may be impacted by the code
- relevant community and industry associations
- relevant regulators and other government agencies to assess any other legal issues associated with codes. For example, a code developer should consult the Australian Competition and Consumer Commission (ACCC) if it is possible that a code might impact anti-competitive conduct.

[17] Privacy Act, s 26D.

[18] Privacy Act, s 26F(2) (APP codes) and s 26Q(2) (CR code).

[19] Privacy Act, ss 26F(2)(b) and s 26Q(2)(b).

2.22 The appropriate way to bring the code to the attention of relevant stakeholders will depend on the circumstances but will usually include:

- placing the code or information about the code online
- public notices in relevant media outlets or industry publications
- direct engagement with relevant government agencies, industry groups and consumer representatives
- requesting the OAIC to include a link on its website to the consultation

2.23 When formulating a consultation, a code developer should ensure that:

- participation in the consultation is accessible to all interested stakeholders
- full and proper consideration is given to the comments raised by the affected parties and stakeholders consulted
- comments are considered promptly and, where appropriate, relevant stakeholders are included in any redrafting exercise as part of an ongoing consultation process

2.24 A code developer must not infer agreement to, or acceptance of, a code from silence or a lack of response from the entities that will be bound by the code. A code developer must ensure that entities likely to be affected by the code are consulted and demonstrate a sufficient level of support for the code.

2.25 Section 17 of the *Legislation Act 2003* requires that, prior to an instrument being made, the rule-maker must be satisfied that appropriate consultation was undertaken. In determining whether any consultation that was undertaken is appropriate, the rule-maker may have regard to the extent to which the consultation ensured that persons likely to be affected by the proposed instrument had an adequate opportunity to comment on its proposed content.[20]

2.26 Accordingly, the Information Commissioner, as the rule-maker, must be satisfied that appropriate consultation has been undertaken before deciding to register a code on the Codes Register.[21]

2.27 The Information Commissioner will have particular regard to whether persons likely to be affected by the code and entities bound by a code have had an adequate opportunity to comment on its proposed content as well as the views of stakeholders provided during the consultation. A code developer should make a reasonable effort to work with stakeholders to resolve issues before an application for the registration of a code is submitted to the Information Commissioner.

2.28 In deciding whether a code developer has made a reasonable effort to work with stakeholders to resolve issues the Information Commissioner will take into account the context of the code, including the number of entities proposed to be bound by the code and the extent of their

[20] Legislation Act, s 17(2)(b).

[21] See s 6 of the Legislation Act for the definition of 'rule-maker'.

obligations under the code. Failure to make reasonable efforts to resolve issues with stakeholders could adversely affect the Information Commissioner's decision to register a code.

2.29 A code developer must submit a statement of consultation with the application for registration of the code, which should contain the following details:

- the period that the draft code was available for public consultation
- the entities likely to be affected by the code
- the methods that were employed by the code developer to consult with entities and the public
- a list of entities and individuals who made submissions to the draft of the code
- details of the changes made to the code following public consultation
- a summary of any issues raised by the consultation that remain unresolved (if any)
- the reasons why any other feedback was not incorporated into the final document

2.30 Registration requirements for codes are discussed in more detail in Part 5.

Code content and drafting style

2.31 As registered codes are binding legislative instruments, it is important that entities bound by the code, the Information Commissioner, other stakeholders and the public are able to easily understand and interpret the code.

2.32 Code developers should comply with the drafting and publishing standards for legislative instruments prepared by the Office of the Parliamentary Counsel (OPC). Compliance with these standards will help ensure new instruments are legally effective, clear and intelligible. Legislative instruments are published on the Federal Register of Legislation (FRL) so attention to formatting issues is also important to ensure that registered documents meet government accessibility requirements.[22]

2.33 Obligations should be set out in the code in a logical order. For example, obligations for an APP code could be grouped under headings for each relevant APP and in the order in which the APPs appear in the Privacy Act. Drafting an APP code in this way will:

- ensure that obligations in the code follow the lifecycle of personal information handling
- explain how entities bound to a code can apply or comply with the APPs
- outline what an individual can expect when determining if an entity bound by the code has acted in a way which may breach an APP

[22] The OPC has published resources to assist with drafting legislative instruments including the Instruments Handbook and drafting templates available at www.opc.gov.au.

2.34 Codes should be written to a professional standard using plain English language that is clear, concise and easy for individuals to understand.[23]

2.35 Language used in the code should be consistent with the Privacy Act to make it easier for individuals to understand the code and for the Information Commissioner to apply in relation to a privacy complaint.[24] For example, a code developer should adopt the definition of terms and language contained in the Privacy Act where it is consistent with the proposed code content.

2.36 Technical or industry specific language or jargon should be avoided as it may limit individuals from fully understanding the code. Where it is necessary for a code to use technical or industry specific language, for example when it is intended to guide industry on a practice issue, the Information Commissioner expects the code to include definitions that clearly explain such terms.

Explanatory statements and statements of compatibility with human rights

2.37 To assist with the Information Commissioner's consideration of an application of a code or variation of a code, the application must include an explanation or summary of how the proposed changes are intended to operate and a statement on the applicant's understanding of the impact the proposed changes may have on human rights.

2.38 The Information Commissioner's preference is for the information required in para 2.37 to be provided in the form of a draft explanatory statement and statement of compatibility with human rights prepared by the code developer in accordance with the OPC's *Instruments Handbook*.

Code developer representativeness

2.39 In deciding whether to register an APP code, the Information Commissioner will consider whether the APP code developer has demonstrated that they represent the APP entities that will be bound by the code. An APP code developer may demonstrate this through conducting an appropriate consultation with entities that will be bound by the code, and addressing feedback received during this consultation (paragraphs 2.19-2.30).

[23] For information about plain English, see the OPC *Plain English Manual*.

[24] Using the words and language of the Privacy Act will also reinforce that a code cannot reduce the privacy protections provided for by that Act.

Request by the Information Commissioner to develop a code

Circumstances where the Information Commissioner may request the development of a code

2.40 The Information Commissioner may request the development of a code.[25]

2.41 The Information Commissioner will only request the development of an APP code where the Information Commissioner is satisfied it is in the public interest. The following is a non-exhaustive list of circumstances where the Information Commissioner may make such a request:

- a code will be the most effective way of resolving an identified privacy issue within a sector or industry. For example, if a particular industry has a history of privacy breaches or has been the subject of a large number of privacy complaints to the Information Commissioner in a short period of time
- a code will clarify an uncertainty regarding the application of the APPs to a particular sector, industry or group of entities. For example, where a new or emerging technology may impact personal information handling practices
- a new code is required as the Information Commissioner has formed the view that a registered APP code is ineffective, out of date or irrelevant but the entities bound by the code have generally expressed a desire to continue to be bound by a code

2.42 The Information Commissioner may consult with APP entities, or their representative organisations, of the intention to request the development of a code.

2.43 Unlike the development of an APP code by the Information Commissioner, a public interest test does not need to be met for the Information Commissioner to request development of the CR code by a code developer. The CR code is a necessary part of the credit reporting regulatory scheme and there must always be a CR code in place.

Request requirements

2.44 Under the Privacy Act, a request from the Information Commissioner to develop a code must:

- be in writing
- specify the period in which a code developer must comply with the request.[26] The period must run for at least 120 days from the date the request is made to allow for an effective consultation to take place (consultation requirements are discussed in paragraphs 2.19-2.30). If necessary, the Information Commissioner may extend the period for whatever

[25] Privacy Act, ss 26E(2) (APP codes) and 26P(1) (CR code).

[26] Privacy Act, ss 26E(3)(a) (APP codes) and 26P(2)(a) (CR code).

period of time that the Information Commissioner considers appropriate in the circumstances.[27]

- inform a code developer that a code is a binding instrument which contains enforceable obligations on code members once registered[28]
- be publicly available as soon as practicable after a request to a code developer is made.[29] A copy of the request will be published on the OAIC website

2.45 The Information Commissioner may, in the request, specify one or several matters that a code must deal with, and set out the entities or class of entities that should be bound by the code.[30] While it is not mandatory for the Information Commissioner to specify these matters in the request, the Information Commissioner will generally provide guidance on these matters.

2.46 The Information Commissioner's request cannot require the requested APP code to deal with exempt acts or practices.[31] However, an APP code developer can, on their own initiative, deal with exempt acts or practices, and can include such provisions in the APP code if they wish. If this occurs, the Information Commissioner can consider those provisions along with the rest of the code provisions when an APP code developer applies for registration of the code.

Identifying the appropriate code developer

2.47 The Information Commissioner's request to develop a code will specify a code developer, and will not take the form of a public request for someone to develop a code.

2.48 An APP code developer and CR code developer could be an entity, a group of entities, or an association or body representing one or more entities. For example, the Information Commissioner may conclude that the expertise required to develop a code is spread across several entities and therefore will request that they jointly develop the code.

2.49 A CR code developer can be an entity or group of entities subject to Part IIIA, or a body or association that represents entities that are subject to Part IIIA.[32]

2.50 It is a matter for the Information Commissioner to determine how to identify the appropriate code developer to which the request should be made. The factors which will be taken into account by the Information Commissioner in identifying an appropriate code developer include whether the entity, group of entities, or association or body:

- has the capacity to develop a code including whether they have the resources and expertise, and

[27] Privacy Act, ss 26E(4)(b) (APP codes) and 26P(3)(b) (CR code).

[28] Privacy Act, ss 26E(3)(b) (APP codes) and 26P(2)(b) (CR code).

[29] Privacy Act, ss 26E(7) (APP codes) and 26P(5) (CR code).

[30] Privacy Act, ss 26E(5) (APP codes) and 26P(4) (CR code).

[31] Privacy Act, s 26E(6).

[32] Privacy Act, s 6(1).

- is generally representative of the entities in the sector or industry to which the code will apply

Development of codes by the Information Commissioner

2.51 The Information Commissioner has the option of developing a code:[33]

- where a code developer has failed to comply with a request to develop a code, or
- where a code developer has developed a code as requested by the Information Commissioner and the Information Commissioner has decided not to register the code

2.52 Before the Information Commissioner develops an APP code, the Information Commissioner must be satisfied that it is in the public interest to do so.[34] In considering the public interest, the Information Commissioner may consider the interests of stakeholders relevant to the industry or activity to which the code will apply, the interests of segments of the public (for example people with a disability or children), as well as the public interest at large.

2.53 Any APP code developed by the Information Commissioner will not cover exempt acts or practices.[35]

2.54 In developing a code, the Information Commissioner will undertake consultation on the code.[36] The Information Commissioner will make a draft of the code publicly available on the OAIC's website and invite public submissions on the draft code. The period in which submissions may be made will be at least 28 days. Matters the Information Commissioner might take into account in considering whether a longer consultation period is necessary include the:

- expected level of interest in the code
- number of expected stakeholders
- complexity of the code
- expected impact of the provisions in the code on the practices or procedures of stakeholders

2.55 The Information Commissioner will only be required to undertake this consultation period when the code has been developed by the Information Commissioner.[37] The Information Commissioner will not be required to conduct this period of consultation where a code developer has developed a code either on their own initiative or following a request from the Information Commissioner and where appropriate consultation has been undertaken by the code developer.[38]

---

[33] Privacy Act, ss 26G (APP codes) and 26R (CR code).

[34] Privacy Act, s 26G(2).

[35] See s 26G(2) of the Privacy Act. This is despite s 26C(3)(b) which states than an APP code may cover an act or practice that is exempt.

[36] Privacy Act, ss 26G(3) (APP codes) and 26R(2) (CR code).

[37] Privacy Act, ss 26G(3) (APP codes) and 26R(2) (CR code).

[38] Privacy Act, s 26E(1) and s 26E(2).

2.56 However, in deciding whether to register the code, the Information Commissioner may also consult any person they consider appropriate.[39]

Where a code developer has failed to comply with a request to develop a code

2.57 The circumstances in which the Information Commissioner may determine that a code developer has not complied with a request to develop an APP code or the CR code may include where:

- the code developer refuses or declines to develop the code as requested
- the code developer does not develop the code within the time period specified in the request (noting that this period must run for at least 120 days from the date the request is made)
- the code produced by the developer does not set out the effect of ss 26A (APP codes) and 26L (CR code) which says that an entity bound by the code must not do an act, or engage in a practice, that breaches a registered code that binds the entity. The purpose of including this reference is to ensure that the code developer is aware that an APP code is a binding legislative instrument
- the Information Commissioner has specified one or more matters that the code must deal with, and the code does not adequately deal with those matters
- the Information Commissioner forms a view that the APP entities or classes of entities that should be bound by the APP code as specified in the request are not sufficiently bound by the code.

2.58 Before determining that a developer has not complied with a request to develop a code, the Information Commissioner will:

- notify the developer of any lack of compliance with the request
- provide the developer a reasonable opportunity and period of time in which to respond to, or remedy, any deficiency
- consider any reasonable requests for an extension of time to develop the code where appropriate in the circumstances.

2.59 The Information Commissioner may determine that a code developer has not complied with a request to develop the code before the developer makes a formal application for registration of the code. However, the Information Commissioner will generally not make this determination until the minimum time period of 120 days has expired from the date the request was made, unless there is clear information available within that period that the developer is unlikely to develop the code.

2.60 While a statement of reasons is not required under the Act, where the Information Commissioner decides that a request has not been complied with, the Commissioner will set

[39] Privacy Act, ss 26H(2)(a) (APP codes) and 26S(2)(a) (CR code).

out the reasons for the decision in writing, and give appropriate notice to the developer of the Commissioner's intention to make such a decision.

Where the Information Commissioner has decided not to register a code

2.61 The Information Commissioner may also develop an APP code or the CR code where there has been compliance with a request to develop a code but the Commissioner has decided not to register the code that was developed as requested. More information about the matters the Information Commissioner will consider in deciding whether to register a code is in Part 5.

Part 3: Code governance

3.1 The Privacy Act does not state how a code should be administered. However, there are a number of matters regarding the code's governance arrangements to consider when deciding whether to develop an APP code. The Information Commissioner will consider, among other things, the governance arrangements of an APP code upon receiving an application for code registration (see the Appendix A).

3.2 As such, code developers should consider the importance of establishing a mechanism to ensure a code is operating effectively, including that entities bound by the code are meeting the privacy standards set by that code. Given that codes effect a co-regulatory approach to privacy regulation, the establishment of a code administrator is considered to be a practical and important method for code developers to demonstrate that the relevant industry sector has a commitment to maintain the effectiveness of the code over time.

3.3 Governance arrangements should include the appropriate funding of a code administrator and the APP code should include a nomination of the body which will fulfil the role of code administrator. However, the obligations and governance arrangements of a code administrator should generally remain outside of the APP code.

3.4 The Information Commissioner may review the operation of a registered APP Code or the registered CR Code.[40]

APP codes

3.5 An APP code administrator will generally oversee:

- the maintenance of an accessible record of code members (paragraph 3.14)
- regular monitoring and reporting on compliance with the code (paragraphs 3.18-3.27)
- commencement of regular independent reviews of the code to ensure it operates effectively and remains relevant (paragraphs 6.1–6.6)
- code variations (paragraphs 6.7–6.13)

[40] Privacy Act, s 26W.

The CR code

3.6 Part IIIA of the Privacy Act sets out compliance monitoring and reporting obligations in relation to the entities bound by the CR code. Under s 20N(3) of the Privacy Act, CRBs must enter into contractual arrangements with credit providers that require compliance with particular obligations contained in that Part, and to monitor and report on compliance with those agreements.[41]

Entities bound by codes

APP codes

3.7 Under the Privacy Act, an APP code must clearly state the APP entities that are bound by the code, or establish a way of identifying the APP entities bound by the code.[42] APP entities bound by an APP code may be subject to privacy complaints for not complying with the code.

3.8 An organisation which is not covered by the Privacy Act but wants to be bound by an APP code will need to 'opt-in' to being covered by the Act. Section 6EA of the Privacy Act allows a small business operator not otherwise covered by the Act to choose to be treated as an organisation, and therefore an APP entity, for the purposes of the Act.

The CR code

3.9 Under Part IIIA of the Privacy Act, the CR code binds all CRBs.[43]

3.10 The CR code also binds all credit providers as well as any other entities subject to Part IIIA of the Privacy Act. However, where parts of the CR code only apply in relation to certain classes of entities subject to Part IIIA, the CR code should specify the entities within that class, or a way of determining which entities are in that class.[44]

Identifying entities bound by APP codes

3.11 APP codes can identify the entities that are bound by that code, for example, by listing the entities in the code itself. However, there may be situations in which it is more effective for a code to describe a way in which entities bound by the code can be identified. For example, an industry association that develops an APP code for all members of that association may be able to describe all association members as being bound by the code. This method may be more practical if the code covers a large number of entities and the code membership will change frequently.

---

[41] Obligations regarding quality and security of credit reporting information for CRBs and credit providers are contained in ss 20N and 20Q respectively.

[42] Privacy Act, s 26C(2)(b).

[43] Privacy Act, s 26N(2)(c).

[44] It is acknowledged that there would be significant difficulties in formulating and maintaining a list of entities bound by the CR code given the significant breadth of coverage of that code across a wide variety of different industry sectors and therefore it would not be practical to maintain a list of current entities bound by the CR code.

3.12 If an APP code only describes the way in which entities that are bound by the code can be identified, a code administrator should, unless it is impractical, maintain an easily accessible and up to date online record of current entities bound by the code.

3.13 Where an online record of entities bound by the APP code is maintained:

- the application to register an APP code should include a statement as to how the online record will be maintained
- the online record should be accessible and link directly to the code
- the online record should include the names of all subsidiary companies that will be bound by the code. Names should include the entity's legal name and any trading names

3.14 Regardless of the approach adopted in identifying entities bound by an APP code, an APP code administrator must be able to liaise with entities bound by the code for activities, such as notification of variations to the code and consulting on reviews of the code. Having a list of entities bound by the code will assist a code administrator to fulfil these functions.

3.15 Failure to clearly identify entities bound by an APP code, either through listing the entities that will be bound or by clearly describing the way in which entities bound by the code can be identified, may constitute a reason not to register an APP code, or to remove a registered APP code.

Monitoring compliance with a code

APP codes

3.16 Under APP 1.2, all APP entities must have practices or procedures in place to deal with complaints or enquiries from individuals about the entity's compliance with the APPs and any APP code they are bound by. An APP code developer should include, as part of the ongoing code governance, mechanisms for a code administrator to monitor the code's effectiveness in achieving compliance from entities bound by the code.

3.17 To assist a code administrator to monitor the compliance of entities bound by an APP code, the APP code should require bound entities to provide an annual report to the code administrator. These annual reports should outline how the entity is complying with the code including the number, nature and outcomes of any complaints about the code made to the entity. More specifically, such a report could include:

- the number of complaints in relation to the code received in the financial year
- statistical information about the nature of the complaints (e.g. the number of complaints related to specific code provisions or APPs)
- the average time taken to resolve the complaints

- statistical information about the outcomes of complaints (e.g. conciliate, withdrawal, referrals to an EDR scheme)[45]
- statistical information about the remedies awarded in finalising the complaint (e.g. compensation, apology, staff training)

3.18 These reporting requirements should be undertaken in a way that minimises the burden, for both the code administrator and the entities bound by a code. It is anticipated that reporting should be achieved through simple collection, aggregation and reporting methods. However, the methodology used to complete these reporting requirements will be determined by the code developer when drafting the code.

3.19 To further assist in monitoring compliance, code developers may also include a standardised internal complaint handling system to be adopted by entities bound by the code (see Part 4). Also, where relevant, consideration could be given to including a risk based system for auditing[46] for serious or repeated interferences with privacy[47] or systemic issues[48] related to compliance with the code.

The CR code

3.20 CRBs have functions and duties in the credit reporting system requiring them to effectively monitor compliance with the provisions of Part IIIA. For example, CRBs are required to enter into contractual arrangements with credit providers that require compliance with particular obligations contained in that Part, and to conduct audits to monitor compliance with those agreements.[49]

3.21 The CR code should include an obligation on CRBs to provide the Information Commissioner, on request, with access to the results of the compliance monitoring activities, including the results of any audits undertaken by or on behalf of the CRB.

[45] Where a complaint cannot be resolved by internal complaint handling procedures of an entity bound by the code, and instead is referred to an EDR scheme, such a referral may be listed as an 'outcome'. However, entities bound by the code are not expected to report on matters taken to an EDR scheme where an outcome was reached through the original internal complaint handling process.

[46] A risk based audit system will allow an APP code administrator to tailor the frequency and extent of any audits to the entities that present the greatest risk of non-compliance. Information obtained through these audits may then be provided to the Information Commissioner in summary form in the annual report.

[47] Serious or repeated interferences with privacy can attract a civil penalty under s13G of the Privacy Act. More information in relation to serious or repeated interferences with privacy is available on the OAIC website.

[48] Systemic issues relate to problems inherent in the code or in the way the code operates where a change to the code or to the structure, organisation or policies in relation to the operation of the code could alleviate the systemic problem.

[49] Privacy Act, ss 20N and 20Q.

Reporting on compliance with a code

APP codes

3.22 An APP code administrator should provide an annual report to the Information Commissioner covering the 12 month period to 30 June. The annual report should be submitted by 31 August, and made available online. The report should include:

- accurate, up to date and sufficient information about how a code administrator has monitored compliance with the code. This should include information received in reports from bound entities and from audits or investigations, if these methods of monitoring are utilised by a code administrator. Information may be provided in summary form.
- aggregated information about systemic issues, or serious or repeated interferences with privacy that occurred during the reporting period
- where information regarding a code's effectiveness in achieving compliance has significantly changed from the last report, a description of the change and any proposed process or practice to address the change

3.23 If reports are not provided to the Information Commissioner or they indicate a lack of compliance with a registered APP code, this may inform a decision by the Information Commissioner to review, vary or remove the registered APP code.

The CR code

3.24 To ensure effective transparency and accountability, the CR code should require CRBs to produce and publish online annual reports that contain aggregated statistical information relating to compliance, complaints and the effectiveness of the credit reporting system by 31 August each year. These reports should contain an overview of CRBs' compliance monitoring activities and aggregated information about any systemic issues, or serious and repeated interferences with privacy that occurred during the reporting period. The CR code should outline what information is required in the reports.

3.25 If reports are not produced and published or they indicate a lack of compliance with the registered CR code, this may inform a decision by the Information Commissioner to review or vary the registered CR code.

Part 4: Standardised internal privacy complaint handling

Privacy complaint handling under the Privacy Act

Privacy complaint handling by APP entities

4.1 APP entities are required to take reasonable steps to implement practices, procedures and systems to deal with privacy-related inquiries or privacy complaints from individuals, including in relation to a registered code that the entity is bound by (APP 1.2). The Information

Commissioner generally expects that an individual's privacy complaint will follow a three-stage process:

1. The individual first makes a privacy complaint to the APP entity.
2. If the individual is not satisfied with the outcome, the individual may make a privacy complaint to a recognised external dispute resolution (EDR) scheme[50] of which the APP entity is a member.
3. If the APP entity is not a member of a recognised EDR scheme, or the individual is not satisfied with the outcome of the EDR process, the individual may make a privacy complaint to the Information Commissioner under s 36 of the Privacy Act.

4.2 The Information Commissioner can decline to investigate a privacy complaint on a number of grounds, including:

- where the individual did not first make a privacy complaint to the APP entity
- if the Information Commissioner considers that the privacy complaint is already being dealt with by a recognised EDR scheme
- if the complaint would be more effectively or appropriately dealt with by a recognised EDR scheme of which the APP entity is a member[51]

Privacy complaint handling by CRBs and credit providers

4.3 The Privacy Act contains more prescriptive requirements for CRBs' and credit providers' privacy complaint handling processes. Like APP entities, CRBs and credit providers are required to implement practices, procedures and systems to deal with privacy-related enquiries or complaints from individuals.[52] In addition, Division 5 of Part IIIA of the Privacy Act sets out how CRBs and credit providers must deal with privacy complaints about credit-related information. Section 23B provides that a complaint must be acknowledged within 7 days and a decision made about the complaint within 30 days.

4.4 Credit providers must also be members of a recognised EDR scheme to be able to disclose information to CRBs.[53] Examples include the Australian Financial Complaints Authority, the Telecommunications Industry Ombudsmen and industry-based ombudsmen schemes e.g. Energy & Water Ombudsman NSW (EWON).

4.5 The general privacy complaint-handling scheme for credit-related complaints is modified for CRBs and credit providers where the privacy complaint relates to an individual's request for access to or correction of their credit-related information. If an individual requests access to or correction of their credit-related information and the request is refused, the Privacy Act does not require the individual to then make a privacy complaint to the credit reporting body or

[50] The Privacy Act gives the Information Commissioner the discretion to recognise EDR schemes to handle privacy-related complaints and to decide not to investigate an act or practice if a complaint about the act or practice is being dealt with by a recognised EDR scheme or would be more effectively or appropriately dealt with by a recognised EDR scheme. For more information see Parts IV and V of the Privacy Act.

[51] Privacy Act, s 41(1)(dd).

[52] Privacy Act, ss 20B(2) and 21B(2).

[53] Privacy Act, s 21D.

credit provider. Rather, the individual may make a privacy complaint directly to a recognised EDR scheme of which the credit reporting body or credit provider is a member, or to the Information Commissioner.[54]

How the Information Commissioner investigates privacy complaints

4.6 Code developers, code administrators and entities bound by a registered code who require more information about the handling of privacy complaints should consult OAIC guidance such as the *Privacy regulatory action policy*, and *Guide to privacy regulatory action* as well as privacy determinations made by the Information Commissioner.

Developing procedures for standardised internal handling of privacy complaints

4.7 A code developer may choose to include in a code, standardised provisions for the internal handling of privacy complaints by entities bound by the code and reporting to the Information Commissioner on those complaints.[55] A decision to include standardised internal complaint handling procedures will benefit the entities bound by the code, the code administrator, and individuals seeking to make complaints to those entities bound by the code. These procedures will ensure a consistent approach to the internal handling of privacy complaints by all entities bound by the code, and facilitate a code administrator reporting to the OAIC on compliance with the code.

4.8 To keep privacy complaint procedures simple and easy to read, it is advisable that, where appropriate, standardised internal privacy complaint handling procedures cover all Privacy Act related privacy complaints relating to entities bound by the code, rather than just complaints concerning breaches of the code.

4.9 A code may also include standardised procedures relating to complaint referral to external dispute resolution schemes to ensure a consistent approach to managing and reporting these complaints by all entities bound by the code. For example, the code may require entities bound by the code to be members of an external dispute resolution scheme[56] and specify that if an individual is not satisfied with how their complaint is handled by an entity, the individual can complain to a designated external dispute resolution scheme.

4.10 A registered code which contains standardised procedures for the internal handling of privacy complaints does not affect an individual's right to complain to a recognised external dispute resolution scheme that the entity is a member of, or to the Information Commissioner under Part V of the Privacy Act.

---

[54] Privacy Act, s 40(1B).

[55] Privacy Act, ss 26C(3)(c)–(d) (APP codes) and 26N(3)(b)–(c) (CR code).

[56] Note it is mandatory for credit providers to be members of an external dispute resolution scheme to participate in the credit reporting system (s 21D(2)(a)(i)).

Standardised internal handling of privacy complaints

4.11 For codes that contain standardised procedures related to the internal handling of privacy complaints, code developers should ensure these procedures are consistent with the following requirements:

- internal privacy complaint handling processes should be clearly outlined, including how privacy complaints are made to an entity and how they will be dealt with by that entity. This may include the process for lodging privacy complaints, timeframes for investigating and responding to privacy complaints, the criteria used for assessing privacy complaints and how privacy complaints may be resolved
- clarification that the internal complaint handling process does not remove the right of individuals to make a privacy complaint to a recognised EDR scheme that the entity is a member of, or to the Information Commissioner under Part V of the Privacy Act
- provide for privacy complaints to be handled by staff with appropriate training
- ensure that an adequate explanation of the privacy complaint process is provided to the individual
- allow privacy complaints to be handled with as little formality and technicality, and as quickly as a proper consideration of the privacy complaint permits
- ensure that the privacy and confidentiality of information collected in the course of investigating and managing privacy complaints is maintained. For example, by outlining how entities would handle and secure that information and the circumstances under which it may be provided to third parties and handled internally
- ensure that the investigation and resolution of privacy complaints is conducted with procedural fairness. For example, privacy complaint decisions are made on the basis of specific criteria and relevant information before the entity
- ensure appropriate tracking of privacy complaints so that privacy complaints are dealt with in a timely way, and can be easily reported on

4.12 If a standardised privacy complaint process is adopted, it should be accessible to all individuals by:

- making the procedures simple for individuals to follow and use, and providing information about those procedures in a variety of accessible formats
- allowing individuals to make contact with the entity handling the privacy complaint through a variety of communication channels
- providing individuals with assistance to make a written privacy complaint on paper or via email where applicable
- providing appropriate facilities and assistance for disadvantaged individuals or those with additional needs, such as free access to interpreters

4.13 If a code contains standardised internal privacy complaint handling procedures, whether the procedures are consistent with the above criteria will be a relevant consideration in the Information Commissioner's decision to register a code.

Reporting of privacy complaints

APP codes

4.14 After the end of each financial year, the Information Commissioner must give the Minister a report on the operations of the OAIC during that year (the OAIC's Annual Report), which includes information about the operation of registered APP codes that contain standardised procedures for making and dealing with privacy complaints.[57] This information includes details about the number of privacy complaints made under these codes, their nature and outcome. The Information Commissioner seeks to report on all APP codes in the Annual Report not just those with standardised internal complaint handling procedures.

4.15 The most efficient way in which the Information Commissioner is able to provide the necessary information in the Annual Report is from reports provided by APP code administrators to the Information Commissioner. The provision, by APP code administrators, of annual reports about the operation of codes is already discussed at paragraphs 3.22-3.23.

The CR code

4.16 The Information Commissioner reports on the CR code in the OAIC's Annual Report. The CR Code should require CRBs to include information about the number, nature and outcome of complaints in the annual reports they are required to produce. This information will assist the Information Commissioner in reporting on the CR code. The provision, by CRBs, of annual reports about the operation of codes is discussed at paragraphs 3.24-3.25.

Part 5: Applying for registration of a code

Application for registration of a code

5.1 A code is binding and comes into force once it is registered on the Codes Register kept by the Information Commissioner. Alternatively, an instrument or a provision of an instrument may commence at a later date specified in the code. A code developer must apply to the Information Commissioner for the registration of a code.[58] When the Information Commissioner receives an application for registration of a code, the code and any supporting documents, will be published on the OAIC website while the Information Commissioner considers the application.

5.2 The registration of a code is at the discretion of the Information Commissioner.[59] Each code will be assessed by the Information Commissioner on its merits.

---

[57] *Australian Information Commissioner Act 2010*, ss 30 and 32(1)(b).

[58] Privacy Act, ss 26F(1) (APP codes) and 26Q(1) (CR code).

[59] Privacy Act, ss 26H(1) (APP codes) and 26S(1) (CR code).

5.3 A code developer is required to undertake a public consultation before making an application to register a code (see paragraphs 2.19-2.30). In deciding whether to register the code, the Information Commissioner may also consult any person they consider appropriate.[60]

5.4 A code developer may, with the Information Commissioner's consent, vary a code at any time before the Information Commissioner registers the code.[61] This allows a code developer to make variations that respond to concerns or comments made by the Information Commissioner or others. Even if variations are made to the code at the suggestion of, or in response to comments from, the Information Commissioner, this does not affect the Information Commissioner's discretion to register the code. That is, the Information Commissioner may still decide not to register a code.

The form and manner of the application

5.5 An application for the registration of a code must be made in the form and manner specified by the Information Commissioner and must be accompanied by the information specified by the Information Commissioner.[62]

5.6 An application to register a code must be made in writing. There is no formal application form to complete; however, the application would normally consist of a letter addressed to the Information Commissioner which sets out:

- the name of the code developer or entity that is applying for registration of the code
- a request by the code developer for the Information Commissioner to consider the code for registration
- the type of code which is the subject of the application (APP code or the CR code)
- the preferred title of the code
- the name of the entity that will be a code administrator (where applicable)

5.7 The application must also include the following documentation:

- a copy of the code
- submissions received during consultation
- a statement of consultation (see paragraph 2.29)
- the draft explanatory statement and the statement of compatibility with human rights (see paragraph 2.37)
- if all of the requirements in these guidelines are not met, a statement explaining why those requirements have not been met or why they are not relevant

[60] Privacy Act, ss 26H(2)(a) (APP codes) and 26S(2)(a) (CR code).

[61] Privacy Act, ss 26F(4) (APP codes) and 26Q(4) (CR code).

[62] Privacy Act, ss 26F(3) (APP codes) and 26Q(3) (CR code).

- any other material that may be relevant to the Information Commissioner's decision to register the code

Matters the Information Commissioner will consider in deciding whether to register a code

5.8 In deciding whether to register a code, the Information Commissioner will consider whether the code meets the requirements set out in Part IIIB of the Privacy Act. The Information Commissioner will also consider whether the code meets the requirements set out in these guidelines.

5.9 In deciding whether to register a code, the Information Commissioner may consult any person the Information Commissioner considers appropriate.[63] The Information Commissioner will name all parties consulted with under ss 26H(2)(a) and 26S(2)(a) in a letter accompanying the decision to register a code.

5.10 In deciding whether to consult prior to registering a code, the Information Commissioner will consider the extent to which entities that will be bound by the code and members of the public have been given an opportunity to comment. If considered appropriate, the Information Commissioner may consult industry groups that represent those that will be bound by the code, advocacy associations that represent the interests of the community, and others that have an interest or who may be affected by the registration of the code.

See Appendix A for a list of matters the Information Commissioner may consider when deciding whether to register a code. Timeframes

5.11 The Information Commissioner will acknowledge receipt of the application in writing. Timeframes for assessing a code application will vary depending on a number of factors, including:

- the length and complexity of the code, the application, and the draft explanatory statement and the statement of compatibility with human rights
- the comprehensiveness of the consultation process undertaken by a code developer – if the Information Commissioner is not satisfied that an adequate consultation has been undertaken, the Information Commissioner may request that additional consultation occur, or conduct their own consultation
- whether all documentation has been provided to the OAIC at the time the code is submitted for registration

[63] Privacy Act, ss 26H(2)(a) (APP codes) and 26S(2)(a) (CR code).

Notification

5.12 The Information Commissioner will notify the code developer of a decision to register the code in writing. The decision will include the date when registration is to take effect. Upon registration of a code, the Information Commissioner will publish a letter outlining the reasons for approving the code.

5.13 The Information Commissioner will also notify the code developer of a decision not to register a code. The Information Commissioner's notice will include reasons for that decision.[64]

The Codes Register

5.14 The Privacy Act requires the Information Commissioner to keep a register, known as the Codes Register, which includes all APP codes and the CR code the Information Commissioner has decided to register.[65] Where the Information Commissioner approves a variation to an APP code or CR code, the Codes Register will include the relevant code as varied.[66] However, the Codes Register will not include any code that the Information Commissioner has removed from the Register.[67] Variations and the removal of codes are discussed in Part 6.

5.15 The Codes Register will always include one, and only one, CR code.[68]

5.16 The Codes Register, including the full content of any registered APP codes and the registered CR code will be made publicly available on the OAIC's website: www.oaic.gov.au.[69]

Registration of codes – what this means

5.17 An APP code and the CR code come into force once they are registered by the Information Commissioner on the Codes Register, or at a later date specified in the code. Once in force, the codes are legally binding for identified entities.[70]

5.18 The Privacy Act states that registered codes are legislative instruments. Legislative instruments must be registered on the Federal Register of Legislation (FRL).[71] The Information Commissioner is responsible for registering the code on the FRL.

---

[64] Privacy Act, ss 26H(3) (APP codes) and 26S(3) (CR code).

[65] Privacy Act, s 26U(1).

[66] Privacy Act, ss 26J(6)(b) (APP codes) and 26T(5)(b) (CR code).

[67] Privacy Act, s 26U(2).

[68] Privacy Act, s 26S(4).

[69] Privacy Act, s 26U(3).

[70] Privacy Act, ss 26B(1) (APP codes) and 26M(1) (CR code). See also ss 26C(5) (APP codes) and 26N(5) (CR code) which are declaratory provisions which state that APP codes and the CR code are not legislative instruments. This is because codes are not enforceable until they are registered on the Codes Register. Once the code is registered on the Codes Register by the Information Commissioner it will be a legislative instrument.

[71] The registration of legislative instruments on FRL is governed by the Legislation Act.

5.19 This means that there is a double registration process for codes – first on the Codes Register and then registration as a legislative instrument on the FRL. However, ss 26B(3) (APP codes) and 26M(3) (CR code) state that:

- the code comes into force on the day it is registered on the Codes Register or
- on a later date specified in the code registered on the Codes Register, even if this is before the date it is registered on the FRL.

Review by the Administrative Appeals Tribunal

5.20 A code developer can make an application to the Administrative Appeals Tribunal (AAT) for review of decisions by the Information Commissioner not to register a code (s 96). More information about making an application for review to the AAT is available on the AAT's website: www.aat.gov.au.

Part 6: Reviewing, varying and removing registered codes

Review of registered codes

Regular independent reviews of registered codes required

6.1 Generally, the governance arrangements for both registered APP codes and the CR code should include a regular independent review of the operation of the code. This will ensure the code remains effective and relevant.

6.2 An independent review of a code should:

- occur at regular intervals, at least every 5 years, and have a scope broad enough to capture all potential issues related to the code's effectiveness and relevance[72]
- include a public consultation process with relevant stakeholders (e.g. entities bound by the code, individuals who transact with those entities)
- result in a report made publicly available online which outlines:
- the issues raised by the review
- the findings of the review
- the actions taken, or that will be taken, by a code administrator and/or the entities bound by the code to address issues identified by the review

6.3 Where there is a code administrator in place, they may also decide to initiate an independent review of a registered code before a regular review is due. For example, a code administrator may initiate an independent review if an audit indicates a lack of compliance with the

[72] The Information Commissioner should also be kept informed throughout the process.

registered code or a code administrator becomes aware of systemic issues that would justify a review.

Review of registered codes by the Information Commissioner

6.4 The Information Commissioner may also review the operation of a registered APP code or the registered CR code.[73] A review of a registered code may occur where the Information Commissioner becomes aware, among other matters:

- of a change in industry practices, technology or consumer expectations that may impact the effective operation of the code
- that the code is not otherwise operating effectively
- that there may be a lack of compliance with a registered code

6.5 The Information Commissioner may ask a code administrator, where one exists, to assist the review by conducting an investigation and analysis of specific issues and report on those issues. This approach may be appropriate where a code administrator's expertise would be helpful to the review.

6.6 The outcome of any review of a code may inform a decision by the Information Commissioner to approve a variation of a registered APP code or the registered CR code, or to remove a registered APP code from the Codes Register.

Variations to a registered code

6.7 The Information Commissioner may approve, in writing, a variation of a registered code.[74] A variation may occur:

- when a body or association representing one or more entities bound by the registered code (such as a code administrator) applies for a variation
- when an entity bound by the registered code applies for a variation
- on the Information Commissioner's own initiative

6.8 Where the Information Commissioner decides to vary a registered APP code on the Information Commissioner's own initiative, the variation cannot include provisions that deal with exempt acts or practices.[75] However, where an entity or representative body applies for a variation of an APP code, the variation may deal with exempt acts or practices.

6.9 Before deciding whether to approve a variation to an APP code or the CR code, the Information Commissioner must:

- make a draft of the variation publicly available on the OAIC website

[73] Privacy Act, s 26W.

[74] Privacy Act, ss 26J (APP codes) and 26T (CR code).

[75] Privacy Act, s 26J(3).

- consult any person the Information Commissioner considers appropriate about the variation. For example, the Information Commissioner may consult industry associations that represent those bound by the code, consumer advocacy associations and others that have an interest or who may be affected by the variation
- consider the extent to which members of the public have been given an opportunity to comment on the variation[76]

6.10 In deciding whether to approve a variation, the Information Commissioner will consider the matters specified in these guidelines.[77] The decision will primarily be informed by whether the proposed variation effectively addresses the issues it seeks to resolve.

6.11 See Appendix B for a list of matters the Information Commissioner may consider when deciding whether to vary a registered code. If the Information Commissioner decides to vary a registered code, the Information Commissioner will:

- notify the code developer of the decision, including the date on which the variation will occur
- unless the circumstances require that the variation take place in a shorter timeframe, publish a public notice about the proposed variation of the registered code on the OAIC's website at least 28 business days before the registered code is due to be varied. The OAIC will endeavour to publish the variation as soon as practicable to ensure entities have sufficient time to adapt to any variations
- add the code as varied to the Codes Register and remove the original registered[78]
- lodge the variation of the code with the OPC for registration on the FRL
- publish a notice on the OAIC's website following the date of variation stating that the original registered code has been varied

CR code variation process

6.12 For variations to the CR code, the code developer must give consideration to the need for all stakeholders to have early input at the issues identification stage, and before drafting commences. The code developer should:

- engage with stakeholders to gauge their position on proposed amendments to the CR code before drafting commences (i.e. roundtables or initial conversations)
- enable stakeholders to submit proposals for amendments to the CR code and consider these proposals

[76] Privacy Act, ss 26J(4) (APP codes) and 26T(3) (CR code).

[77] Privacy Act, ss 26J(5) (APP codes) and 26T(4) (CR code).

[78] Privacy Act, ss 26J(6) (APP codes) and 26T(5) (CR code). A variation comes into effect on the day specified in the Information Commissioner's approval. However, as registration is the act that ensures a code is enforceable, the variation cannot take effect before the whole code, as varied, is registered on the Codes Register. The variation itself is not registered. The whole code is replaced with a new version of the code that incorporates the variation.

- integrate stakeholders' proposals prior to, and during, the drafting process
- consider and where appropriate implement feedback provided by OAIC staff during the variation process

The form and manner of the application to vary a registered code

6.13 An application for a variation of a registered code must be made in the form and manner specified by the Information Commissioner and must be accompanied by the information specified by the Information Commissioner.[79]

6.14 An application to vary a registered code must be made in writing. There is no formal application form to complete; however, the application would normally consist of a letter addressed to the Information Commissioner which sets out the following:

- the title of the registered code
- the name of the code developer applying for the variation
- the details of the proposed variation
- the reasons for the variation
- any potential consequences resulting from the variation, including the impact on entities bound by the registered code
- details of any consultation carried out with entities bound by the registered code along with other relevant stakeholders

6.15 The application must also include:

- a copy of the proposed amendments to the code
- a separate document showing the complete code as varied
- the draft explanatory statement and the statement of compliance with human rights (see paragraph 2.37 above)
- any submissions received on any consultation undertaken on the variation
- if all of the requirements in these guidelines are not met, a statement explaining why those requirements have not been met or why they are not relevant
- any other material that may be relevant to the Information Commissioner's decision to register the code as varied

[79] Privacy Act, ss 26J(2) (APP codes) and 26T(2) (CR code).

Removal of a registered APP code

6.16 The Information Commissioner may remove a registered APP code from the Codes Register.[80] In deciding whether to remove a registered APP code, the Information Commissioner will consider the matters specified in these guidelines.[81]

6.17 As with a variation, the Information Commissioner can remove a registered APP code:

- on the application of a body or association representing one or more entities bound by the code
- on the application of an entity bound by the code
- on the Information Commissioner's own initiative

6.18 In removing a registered APP code, the Information Commissioner will undertake a consultation in the same way as for a variation of a registered code (see 6.9).[82]

6.19 See Appendix C for a list of matters that the Information Commissioner may consider when deciding whether to remove a code from the Codes Register. If a registered APP code is removed from the register, the Information Commissioner will:

- notify the person or entity that applied for the removal (if applicable), as well as a code administrator, of a decision to remove the registered APP code, including the date on which the removal will occur
- unless the circumstances require that the removal take place in a shorter timeframe, publish a public notice about the proposed removal of the registered APP code on the OAIC's website at least 28 business days before the registered code is due to be removed. During this period, a code administrator should inform the entities that are bound by the registered code of the date of the code's removal from the Codes Register and advise that following this date the registered code will no longer be in force
- remove the registered APP code from the Codes Register on the specified date
- ensure that the registered APP code is noted as 'repealed' on FRL
- publish a public notice that the registered APP code has been removed from the Codes Register on the OAIC's website following the date of removal

[80] Privacy Act, s 26K. There are no procedures for removing the registered CR code. There will always be a CR code in force. Any changes to the registered CR code will be made by way of variation to the registered CR code.

[81] Privacy Act, s 26K(4).

[82] Privacy Act, s 26K(3).

The form and manner of the application to remove a registered APP code

6.20 An application for the removal of a registered APP code must be made in the form and manner specified by the Information Commissioner and must be accompanied by such information as is specified by the Information Commissioner.[83]

6.21 An application to remove a registered code must be made in writing. There is no formal application form to complete, however, it is recommended that the application take the form of a letter addressed to the Information Commissioner which sets out the following:

- the title of the relevant registered APP code
- the name of the entity bound by the code, or the body or association representing one or more of the entities bound by the registered APP code applying for the removal
- the reasons for the removal
- any potential consequences resulting from the removal of the registered APP code, including the impact on entities bound by the registered APP code
- details of any consultation carried out with entities bound by the registered APP code along with other relevant stakeholders
- any submissions received during the consultation on removal of the code

[83] Privacy Act, s 26K(2).

Appendix A

Matters the Commissioner may consider in deciding whether to register a code

This is a list of matters the Information Commissioner may consider when deciding whether to register a code. This list is not exhaustive and not all matters will apply in all circumstances.

Preliminary and procedural matters

- whether a code developer has provided all relevant documentation with the application (Part 5)
- whether the code satisfies the requirements in Part IIIB of the Privacy Act (Part 2)
- whether there is existing legislation, regulation or a code that covers the same or similar topics that may negate the need to develop a code or may be suitable for adoption without the need to develop a separate code (Part 1)
- whether a code developer that has developed an APP code on their own initiative has demonstrated that they represent the APP entities that will be bound by the code (Part 2)
- whether there was initial notification of, and updates on, the code's development (Part 1)

Code content

- whether the code meets the drafting style requirements (Part 2)
- whether entities bound by the code are clearly identified, or whether the way used to determine entities bound by the code is sufficiently clear and specific (Part 3)
- whether the code adequately and effectively sets out how one or more APPs are to be applied or complied with
- whether any additional requirements included in the code are not contrary to, or inconsistent with, any of the APPs and are otherwise adequate and appropriate in the circumstances
- whether the code adequately and effectively addresses any matters the Commissioner specified the code must deal with in a request to develop the code
- whether the code's substantive content is otherwise effective and appropriate in the circumstances
- whether there are appropriate governance arrangements in place to administer the code where appropriate (Parts 3 and 6)
- whether there are appropriate reporting mechanisms where appropriate (Part 3)
- if there are standardised internal privacy complaint handling procedures, whether they satisfy the matters set out in Part 4

Consultation requirements

- whether a code developer satisfied the public consultation requirements and considered views of stakeholders obtained during the consultation (Part 2)
- any matters put forward by stakeholders or other submitters during consultation
- any matters raised by any person whom the Information Commissioner consults (paragraphs 5.9–5.10)

Other relevant matters

- the interests of those regulated by the code, and any adverse or beneficial impact on those individuals
- the protection of privacy in a particular sector, and any adverse or beneficial impacts on commercial or other entities proposed to be regulated
- published research in respect of matters addressed by the APP code
- community expectations of privacy, in particular expectations within the regulated community
- whether the code advances the objects of the Privacy Act
- the Commissioner's own observations drawn from the Commissioner's regulation of matters that would be covered by the APP code (i.e. enquiries, complaints or other information elicited during investigations)
- whether the code improves upon complaint handling mechanisms or promotes further access to options for resolution of a privacy dispute by the regulated community
- any other factors the Commissioner considers to be relevant

Appendix B

Matters considered for a code variation

- This is a list of matters the Information Commissioner will consider when deciding whether to vary a registered code. This list is not exhaustive and not all matters apply (e.g. when the variation is on the Information Commissioner's own initiative).whether the applicant has provided all relevant documentation with the application and has met the requirements under the Privacy Act to vary a code (paragraph 6.15)
- whether the proposed variation effectively addresses the issues it seeks to resolve (paragraph 6.10)
- whether adequate consultation has occurred, and the views of the entities bound by the code and others about the proposed variation (paragraph 6.9)

- whether in relation to the CR code (paragraph 6.13)
  - all stakeholder groups, including for example consumer advocacy associations, have had the opportunity to have early input at the issues identification stage and before drafting commences
  - the code developer has engaged sufficiently with stakeholders to gauge their position on proposed amendments to the CR code before drafting commences, for example through mechanisms such as roundtables
  - stakeholder proposals have been considered and where appropriate, implemented
  - feedback provided by OAIC staff during the variation process has been considered and where appropriate, implemented

Appendix C

Matters considered for an APP code removal

This is a list of matters the Information Commissioner will consider when deciding whether to remove an APP code from the register. This list is not exhaustive and not all matters apply (e.g. when the removal is on the Information Commissioner's own initiative).

- whether the applicant has provided all relevant documentation with the application (paragraph 6.23)
- whether the operation of a registered APP code's governance arrangements remain effective including whether a code administrator is monitoring and reporting the registered APP code's effectiveness (paragraphs 3.15-3.18 and 3.21-3.22)
- whether the entities bound by the code are adhering to any standardised internal privacy complaint handling and reporting procedures (Part 4)
- if a review of the code by the Information Commissioner or an independent review initiated by a code administrator (paragraphs 6.1–6.6), or the reported information from a code administrator or entities bound by the registered code indicates the registered APP code is not operating effectively
- whether the registered APP code is out of date or irrelevant, including if no entities remain bound by the code (paragraph 2.41)
- a failure to clearly identify entities bound by the registered APP code (paragraphs 3.8-3.9)
- whether adequate consultation on the removal has occurred and the views of the entities bound by the registered APP code and others about the proposed removal
- whether the registered APP code is effective in protecting privacy and meets its objectives