Australian Government

Office of the Australian Information Commissioner

Guidelines for developing codes

Issued under Part IIIB of the *Privacy Act 1988*

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

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

Date of initial publication: September 2013

Creative Commons

With the exception of the Commonwealth Coat of Arms, and to the extent that copyright subsists in a third party, this report, its logo and front page design are licensed under a Creative Commons Attribution 3.0 Australia licence (http://creativecommons.org/licenses/by/3.0/).

To the extent that copyright subsists in third party quotes and diagrams it remains with the original owner and permission may be required to reuse the material.

Content from these guidelines should be attributed as: Office of the Australian Information Commissioner, *Guidelines for developing codes – issued under Part IIIB of the Privacy Act 1988*.

Enquiries regarding the licence and use of the guidelines are welcome at:

Office of the Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001
Telephone: 02 9284 9800
Email: enquiries@oaic.gov.au
Web: www.oaic.gov.au

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[1]; 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[2]

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.

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.

---

1 Entity includes entities regulated by the credit reporting provisions in Part IIIA of the Privacy Act.

2 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.

Part 1 – Introduction

The Privacy Act and codes

1.1 The *Privacy Act 1988* (Privacy Act)[3] 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 Under Part IIIB of the Privacy Act, the Australian Information Commissioner (the Information Commissioner)[4] can approve and register enforceable codes which are developed by entities on their own initiative or on request from the Information Commissioner, or developed by the Information Commissioner directly.

1.3 An APP entity (or a body or association representing them) can develop a written code of practice for the handling of personal information, called an APP code. An APP code sets 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.

1.4 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.

1.5 The purpose of a code is to provide individuals with transparency about how their information will be handled. 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.

1.6 An entity bound by a registered code must not do an act, or engage in a practice, that breaches that code (ss 26A (APP codes) and 26L (CR code)). A breach of a registered code will be an interference with the privacy of an individual under s13 of the Privacy Act and subject to investigation by the Information Commissioner under Part V of the Privacy Act.

---

[3] In this guide, unless otherwise indicated, any references to sections of an Act are to sections of the *Privacy Act 1988* as amended by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012.*

[4] The Australian Information Commissioner is the head of the Office of the Australian Information Commissioner. The Information Commissioner is supported by two other statutory officers: the Privacy Commissioner and the Freedom of Information Commissioner. More information is available at: www.oaic.gov.au.

1.7 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 to apply or comply with one or more APPs or to meet higher standards of personal information handling than required by one or more of the APPs. It would also cover governance or administrative items that must be included in a code (s26C(2)), or which are directly related to the handling of personal information by entities bound by the code. Other administrative and governance issues should be dealt with separately (see Part 3 on Code governance).

1.8 Section 26V of the Privacy Act provides the Information Commissioner with the power to make written guidelines relating to codes.[5] 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 the requirements set out in these guidelines.

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
- 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 his or her own initiative
- outline matters that need to be addressed in the development and registration of a code
- outline matters related to reviewing, varying and removing registered codes.

[5] 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.

Why develop an APP code?

1.11 The primary purpose of an APP code is to set out how one or more of the APPs are to be applied or complied with. 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:

- 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 IIIA[6]
- 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, in particular, the APPs. Information to assist entities is available on the Office of the Australian Information Commissioner (OAIC) website.

1.14 An entity that develops a code should have in place properly resourced administrative mechanisms to develop the code. This may include an entity using a code developer or 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

[6] • 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.

- scoping and drafting the code
- seeking legal or professional advice
- involving stakeholders (including consumers) in effective consultations on the draft code
- establishing and financing a code administrator to oversee the operation of the code, including reporting on the operation of the code and initiating regular reviews of the code
- 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 A code developer should notify the Information Commissioner of their intention to develop a code. A code developer should also keep the Information Commissioner informed throughout the code development process.

1.17 In the first instance, a code developer should consult these guidelines, the Privacy Act and related publications. Additionally, OAIC staff may be able to provide some general (non-legal) advice to a code developer and a code administrator. However, any advice would not fetter the discretion of the Information Commissioner in deciding whether to register the code.

1.18 If requested, the OAIC will provide a link from its website to assist stakeholder consultation.

Part 2 – Developing codes

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 should not form part of the code to be registered by the Information Commissioner.

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 (ss 26E(1)and 26E(2)).

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
- set out the period during which the code is in force (which must not start before the day the code is registered on the Code Register). For example, the code will be in force for 5 years from the day of registration.

2.6 Generally, an APP code will commence operation on registration. 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.

The CR code

2.7 The Information Commissioner may request an appropriate entity to develop the CR code (s 26P(1)).

2.8 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. The CR code should bind all credit providers and other entities subject to Part IIIA in whole or in part.

2.9 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.[7]

Other matters that may be included in a code

APP codes

2.10 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
- 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.

2.11 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.

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

---

[7] Explanatory Memorandum, p 208, available at www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r4813.

The CR code

2.13 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).

2.14 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.

2.15 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

2.16 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 (s26C(3)(b)).[8] For example, exempt acts or practices that may be the subject of an APP code include the handling of employee records by organisations.

2.17 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 (s 26D).

Consultation on codes

2.18 Under the Privacy Act, a code developer is required to undertake a public consultation before making an application to register a code (ss 26F(2) (APP codes) and 26Q(2) (CR code)). Specifically, a code developer must:

- make a draft of the code publicly available, for example on the code developers website or some other suitable website

[8] This provision covers exempts acts or practices within the meaning of subsection 7B(1), (2) or (3).

- 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[9]
- give consideration to any submissions made within the specified period.

2.19 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 include:

- individuals and entities that may be impacted by the code
- relevant community and industry associations.

2.20 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 newspapers 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.

2.21 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.

2.22 When considering whether to register a code, the Information Commissioner will have particular regard to the views of stakeholders provided during the consultation. A code developer should make a reasonable effort to work with stakeholders to resolve issues before a code is submitted to the Information Commissioner for registration. 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 obligations under the code. Failure to make reasonable efforts to

[9] 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, or the expected impact of the provisions in the code on the practices or procedures of stakeholders.

resolve issues with stakeholders could adversely affect the Information Commissioner's decision to register a code.

2.23 A code developer must not infer agreement to, or acceptance of, a code from silence or a lack of response from members. A code developer must demonstrate a sufficient level of support for the code from entities that the code proposes to bind.

2.24 A code developer may also need to consult with 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 encourage anti-competitive conduct.[10]

2.25 A code developer must submit a statement of consultation with the application to register 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.

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

Developing explanatory material

2.27 A code developer may wish to prepare explanatory material in relation to a code.

2.28 While a code developer should include all relevant obligations in the code itself, the Information Commissioner recognises that there may be instances where additional explanatory material is necessary. For example, practical examples about how the code may be complied with, or other material that may assist with understanding the obligations set out in the code.

2.29 A code developer should bring any explanatory material that is developed in relation to a code to the Information Commissioner's attention, either at the time of the application, or if it is prepared at a later time, at that later time. Although the Information Commissioner is not required to consider the explanatory material, the Information

[10] In drafting a code, entities should be mindful of the *Competition and Consumer Act 2010* (CCA) which prohibits various forms of anti-competitive conduct. Further information regarding the CCA can be obtained from the ACCC's website at www.accc.gov.au.

Commissioner may use the explanatory material to inform his or her understanding of the intended operation of the code.

2.30 The Information Commissioner will not approve the explanatory material nor will the Information Commissioner be bound by the explanatory material.

Drafting style

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

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

2.33 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.[11] For example, where it is consistent with the proposed code content, a code developer should adopt the definition of terms and language contained in the Privacy Act.

2.34 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, the Information Commissioner expects the code to include definitions that clearly explain such terms.

Openness and transparency

2.35 APP 1 requires APP entities to set out in a document their clearly expressed and up to date policies about how they manage personal information. This includes information about how an individual may complain about a breach of the APPs, or a registered APP code that binds the entity, and how the entity will deal with such a privacy

[11] 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.

complaint (APP 1.4(e)). The APP entity must take reasonable steps to make this document available to anyone who requests a copy (APP 1.5 and 1.6).

2.36 Part IIIA of the Privacy Act states that CRBs and credit providers must have a clearly expressed and up to date policy about the management of credit-related information.[12] The policy of the CRB or credit provider must include information on how an individual may complain about a failure of the body or provider to comply with the registered CR code and how the body or provider will deal with such a complaint (ss 20B(4)(h) and 21B(4)(g)). A CRB or credit provider must also take reasonable steps to make this policy available free of charge and in an appropriate form (ss 20B(5)(a)–(b), 20B(6), 21B(5)(a)–(b) and 21B(6)).

2.37 To assist in making these policies easily available, codes should contain provisions which require entities bound by a code to have these policies and information about the code, and links to it, easily accessible on their website.

2.38 Additionally, to ensure that a code operates in an open and transparent way, code administration committees (see Part 3 Code governance) should have representatives from relevant stakeholder groups and be transparent in their operations.

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 2.18–2.25).

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 (ss 26E(2) (APP codes) and 26P(1) (CR code)).

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

[12] Obligations regarding credit information and eligibility information management policies for CRBs and credit providers are contained in ss 20B(3) – (6) and 21B(3)–(7) respectively.

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 will 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 (ss 26E(3)(a) (APP codes) and 26P(2)(a) (CR code)). 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 2.18–2.26). If necessary, the Information Commissioner may extend the period for whatever period of time that the Information Commissioner considers appropriate in the circumstances (ss 26E(4)(b) (APP codes) and 26P(3)(b) (CR code))
- inform a code developer that a code is a binding instrument which contains enforceable obligations on code members once registered (ss 26E(3)(b) (APP codes) and 26P(2)(b) (CR code))
- be publicly available as soon as practicable after a request to a code developer is made (ss 26E(7) (APP codes) and 26P(5) (CR code)). 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 (ss 26E(5) (APP codes) and 26P(4) (CR code)). 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 (s 26E(6)). 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 general 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 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
- is generally representative of the entities in the sector or industry to which the code will apply.

Development of codes by the Information Commissioner

2.50 The Information Commissioner has the option of developing a code (ss 26G (APP codes) and 26R (CR code)):

- 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.

2.51 Before the Information Commissioner develops an APP code, the Information Commissioner must be satisfied that it is in the public interest to do so (s 26G(2)). 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.

2.52 Any APP code developed by the Information Commissioner will not cover exempt acts or practices (s 26G(2)).[13]

2.53 In developing a code, the Information Commissioner will undertake consultation on the code (ss 26G(3) (APP codes) and 26R(2) (CR code)). 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 submission may be made will be at least 28 days. Matters the Information Commissioner might take into account in considering whether a period longer than 28 days 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.

2.54 The Information Commissioner will only be required to undertake this consultation period when the code has been developed by the Information Commissioner (ss 26G(3) (APP codes) and 26R(2) (CR code)). 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 (ss 26E(1)and 26E(2)) and where appropriate consultation has been undertaken by the code developer.

2.55 However, in deciding whether to register the code, the Information Commissioner may also consult any person he or she considers appropriate (ss 26H(2)(a) (APP codes) and s 26S(2)(a) (CR code)).

[13] This is despite s 26C(3)(b) which states than an APP code may cover an act or practice that is exempt.

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 a code. The Information Commissioner will consider, amongst other things, the governance arrangements of a code upon receiving an application for code registration (see the Appendix).

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 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 code.

APP codes

3.4 An APP code administrator will generally oversee:

- the maintenance of an accessible record of code members (paragraphs 3.11)
- regular monitoring and reporting on compliance with the code (paragraphs 3.15–3.24)
- 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).

The CR code

3.5 It is expected that the oversight responsibilities of the CR code administrator will vary from the responsibilities of APP code administrators as there are already compliance monitoring and reporting obligations built into Part IIIA of the Privacy Act. For example, Part IIIA of the Privacy Act requires CRBs to 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.[14] However, it is expected that the CR code administrator would be responsible for the commencement of regular independent reviews of the CR code to ensure it remains effective and relevant, initiating code variations and reporting on systemic issues.

[14] Obligations regarding quality and security of credit reporting information for CRBs and credit providers are contained in s20N and 20Q respectively.

Entities bound by codes

APP codes

3.6 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 (s 26C(2)(b)). APP entities bound by an APP code may be subject to privacy complaints for not complying with the code.

3.7 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

3.8 Under Part IIIA of the Privacy Act, the CR code must bind all CRBs (s26N(2)(c)).

3.9 The CR code should also bind 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.[15]

Identifying entities bound by APP codes

3.10 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.

3.11 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.

3.12 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

[15] 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.

- 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.

3.13 Regardless of the approach adopted in identifying entities bound by a code, a 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.

3.14 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

3.15 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.

3.16 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 (eg 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 (eg conciliate, withdrawal, referrals to an EDR scheme)[16]
- statistical information about the remedies awarded in finalising the complaint (eg compensation, apology, staff training).

[16] 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.

3.17 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.

3.18 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[17] for serious or repeated interferences with privacy[18] or systemic issues[19] related to compliance with the code.

The CR code

3.19 CRBs have functions and duties in the credit reporting system requiring them to effectively monitor compliance with the provisions of the new 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 (s20N and s20Q).

3.20 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.

Reporting on compliance with a code

APP codes

3.21 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.

---

[17] 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.

[18] 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.

[19] 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.

- 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.

3.22 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

3.23 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. 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.

3.24 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.

General

3.25 Entities bound by an APP code or the CR code, as well as a code administrator (or CRB), should report systemic issues or serious and repeated breaches of the code to the Information Commissioner as soon as they become aware of them.

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[20] 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 (s 41(1)(dd).

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 (ss 20B(2) and 21B(2)). 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.

[20] 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.

4.4 Credit providers must also be members of a recognised EDR scheme to be able to disclose information to CRBs (s21D).

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 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 (s 40(1B)).

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 by the Information Commissioner, should consult guidance issued by the Information Commissioner, such as the *Privacy Complaints Practice and Procedure Manual*, the *Enforcement Guidelines*, the *Determination Guidelines*, practice notes, case notes and determinations, which are available on the OAIC's website.[21]

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 (ss 26C(3)(c)–(d) (APP codes) and 26N(3)(b)–(c) (CR code)). 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

[21] Links will be provided to the *Enforcement Guidelines* and the *Determination Guidelines* once they have been published. The OAIC will publish these Guidelines before commencement of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*.

require entities bound by the code to be members of an external dispute resolution scheme[22] 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.

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

[22] 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)).

- 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 e-mail 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 (ss 30 and 32(1)(b) of the *Australian Information Commissioner Act 2010*). 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 3.21–3.22.

The CR code

4.16 The Information Commissioner seeks to report on the CR code in the OAIC's Annual Report. It is expected that the CR code would 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 3.23–3.24.

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 by the Information Commissioner. A code developer must apply to the Information Commissioner for the registration of a code (ss 26F(1) (APP codes) and 26Q(1) (CR code)). 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 consider the application.

5.2 The registration of a code is at the discretion of the Information Commissioner (ss 26H(1) (APP codes) and 26S(1) (CR code)). Each code will be assessed by the Information Commissioner on its merits.

5.3 A code developer is required to undertake a public consultation before making an application to register a code (see paragraphs 2.18–2.265). In deciding whether to register the code, the Information Commissioner may also consult any person he or she considers appropriate (ss 26H(2)(a) (APP codes) and s 26S(2)(a) (CR code)).

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 (ss 26F(4) (APP codes) and 26Q(4) (CR code)). 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.

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 (Sections 26F(3) (APP codes) and 26Q(3) (CR code)).

5.6 An application to register a code must be made in writing.[23] 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

[23] The Information Commissioner prefers receipt of all documentation in electronic format, preferably in Microsoft Word, in addition to any other format. As well, formatting of documentation that will assist making it as accessible as possible when published on the web is preferred. The OAIC can be contacted for assistance relating to the preferred formatting.

- 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.

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 2.25)
- a copy of any explanatory material that has been prepared in relation to the code
- 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.

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 (ss 26H(2)(a) (APP codes) and 26S(2)(a) (CR code)). The Information Commissioner will name all parties consulted with under ss 26H(2)(a) and 26S(2)(a) in an explanatory statement 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.

5.11 See the Appendix for a non-exhaustive checklist of matters the Information Commissioner will consider when deciding whether to register a code.

Timeframes

5.12 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 any accompanying materials
- 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 his or her own consultation
- whether all documentation has been provided to the OAIC at the time the code is submitted for registration.

Notification

5.13 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 an explanatory statement outlining the reasons for approving the code.

5.14 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 (ss 26H(3) (APP codes) and 26S(3) (CR code)).

The Codes Register

5.15 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 (s 26U(1)). Where the Information Commissioner approves a variation to an APP code or CR code, the Codes Register will include the relevant code as varied (ss 26J(6)(b) (APP codes) and 26T(5)(b) (CR code)). However, the Codes Register will not include any code that the Information Commissioner has removed from the Register (s 26U(2)). Variations and the removal of codes are discussed in Part 6.

5.16 The Codes Register will always include one, and only one, CR code (s 26S(4)).

5.17 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 (s 26U(3)).

Registration of codes – what this means

5.18 An APP code and the CR code come into force once they are registered by the Information Commissioner on the Codes Register. Once in force, the codes are legally binding for identified entities (ss 26B(1) (APP codes) and 26M(1) (CR code)).[24]

5.19 The Privacy Act states that registered codes are legislative instruments. Legislative instruments must be registered on the Federal Register of Legislative Instruments – (FRLI).[25] The Information Commissioner is responsible for registering the code on the FRLI.

5.20 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 FRLI. 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 FRLI.

Review by the Administrative Appeals Tribunal

5.21 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.

[24] Also see 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 and comes into force, it will at that point be a legislative instrument.

[25] The registration of legislative instruments on FRLI is governed by the *Legislative Instruments Act 2003.*

Part 6 – Reviewing, varying and removing registered codes

Review of registered codes

Review of registered codes initiated by a code administrator

6.1 The governance arrangements for both registered APP codes and the CR code should include a code administrator initiating regular independent reviews of the operation of the code. This will ensure the code remains effective and relevant (see paragraphs 3.4–3.5). A code review should be overseen by a suitably independent person and where practicable supported by a steering group which should include at least one representative from a relevant consumer group.

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 codes effectiveness and relevance[26]
- include a public consultation process with relevant stakeholders(eg 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 A code administrator 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 registered code (see paragraphs 3.18 and 3.19) 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 (s 26W). A review of a registered code may occur where the Information Commissioner becomes aware, amongst other matters:

- of a change in industry practices, technology or consumer expectations that may impact the effective operation of the code
- that there may be a lack of compliance with a registered code.

6.5 The Information Commissioner may ask a code administrator to assist the review by conducting an investigation and analysis of specific issues and report on those issues.

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

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 APP code (s 26J) and or the CR code (s 26T). 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 (s 26J(3)). 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, the Information Commissioner will undertake a consultation (ss 26J(4) (APP codes) and 26T(3) (CR code)), which may include:

- making a draft of the variation publicly available on the OAIC website
- consulting any person the Information Commissioner considers appropriate about the variation.

6.10 In deciding whether to consult regarding a variation, the Information Commissioner will consider the extent to which entities bound by the code and members of the public have been given an opportunity to comment on the variation. If considered appropriate, the Information Commissioner may consult industry groups that represent those 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 variation.

6.11 In deciding whether to approve a variation, the Information Commissioner will consider the matters specified in these guidelines (ss 26J(5) (APP codes) and 26T(4) (CR code)). The decision will primarily be informed by whether the proposed variation effectively addresses the issues it seeks to resolve.

6.12 See the Appendix for a non-exhaustive checklist of matters the Information Commissioner will consider when deciding whether to vary a registered code.

6.13 If the Information Commissioner decides to vary a registered code, the Information Commissioner will:

- notify the code administrator, or the person/entity that applied for the variation and the code administrator, 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. During this period, a code administrator will inform the entities that are bound by the registered code of the date of the code's variation
- add the code as varied to the Codes Register and remove the original registered code (ss 26J(6) (APP codes) and 26T(5) (CR code))[27]
- publish a notice on the OAIC's website for 28 days following the date of variation stating that the original registered code has been varied.

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

6.14 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 (ss 26J(2) (APP codes) and 26T(2) (CR code)).

6.15 An application to vary a registered code must be made in writing.[28] 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 entity bound by the code, or the body/association representing one or more of the entities bound by the code, that is 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.

6.16 The application must also include:

---

[27] 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 in 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.

[28] The Information Commissioner prefers receipt of all documentation in electronic format, preferably in Microsoft Word, in addition to any other format. As well, formatting of documentation that will assist making it as accessible as possible when published on the web is preferred. The OAIC can be contacted for assistance relating to the preferred formatting.

- a copy of the variation as a marked up version of the current registered code, unless that is impracticable, and a separate document showing the complete code as varied
- submission 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.

Removal of a registered APP code

6.17 The Information Commissioner may remove a registered APP code from the Codes Register (s 26K).[29] In deciding whether to remove a registered APP code, the Information Commissioner will consider the matters specified in these guidelines (s 26K(4)).

6.18 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.

6.19 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 (s 26K(3)) (see 6.9).

6.20 For a non-exhaustive checklist of matters set out in these guidelines that will be considered by the Information Commissioner when deciding whether to remove a code from the register see the Appendix.

6.21 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

[29] 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.

- remove the registered APP code from the Codes Register on the specified date
- ensure that the registered APP code is noted as 'ceased' on FRLI
- publish a public notice that the registered APP code has been removed from the Codes Register on the OAIC's website for 28 days following the date of removal.

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

6.22 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 (s 26K(2)).

6.23 An application to remove a registered code must be made in writing.[30] 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.

[30] The Information Commissioner prefers receipt of all documentation in electronic format, preferably in Microsoft Word, in addition to any other format. As well, formatting of documentation that will assist making it as accessible as possible when published on the web is preferred. The OAIC can be contacted for assistance relating to the preferred formatting.

Appendix

Code registration checklist

This is a checklist of the primary matters the Information Commissioner will consider when deciding whether to register a code. This list is not exhaustive and not all matters apply (eg when the code has been developed by the Information Commissioner).

- whether a code developer has provided all relevant documentation with the application (paragraphs 5.6–5.7)
- 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 (paragraph 1.12).
- whether there are appropriate governance arrangements in place to administer the code (Parts 3 and 6)
- whether a code developer has demonstrated that they represent the APP entities that will be bound by the code (paragraph 2.39)
- whether there are appropriate reporting mechanisms (paragraphs 3.21–3.25)
- whether entities bound by the code are clearly identified (paragraphs 3.6–3.14)
- if there are standardised internal privacy complaint handling procedures, whether they satisfy the matters set out in Part 4
- whether there was initial notification of, and updates on, the code's development (paragraph 1.16)
- whether a code developer satisfied the public consultation requirements and considered views of stakeholders obtained during the consultation (paragraphs 2.18–2.265)
- whether the code meets the drafting style requirements (paragraphs 2.31–2.34)
- whether the openness and transparency matters have been addressed (paragraphs 2.385–2.378)
- any matters raised by any person whom the Information Commissioner consults (paragraphs 5.9–5.10)

Code variation checklist

This is a checklist of the primary matters the Information Commissioner will consider when deciding whether to vary a registered code. This list is not exhaustive and not all matters apply (eg when the variation is on the Information Commissioner's own initiative).

- whether the applicant has provided all relevant documentation with the application (paragraph 6.15)
- whether the proposed variation effectively addresses the issues it seeks to resolve (paragraph 6.11)
- whether adequate consultation has occurred and the views of the entities bound by the code and others about the proposed variation (paragraphs 6.10)

Code removal checklist

This is a checklist of the primary 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 (eg 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 3.15–3.215)
- 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 3.6–3.14)
- 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.