Privacy (Openly Australia) Code 2021 - DRAFT

Version: 4.0.0
Updated: 23 February 2021
Public Release: Yes

Table of Contents

Part 1 – Introduction 4
1 Name of APP code 4
2 Commencement 4
3 Authority 4
4 Preamble 4
5 Definitions 4
6 Objectives 5
7 Entities bound by this APP code 5
8 Eligibility and coverage 6
Part 2 – Transparency, compliance, and governance 7
9 Application of Part 2 of this APP code 7
10 Designated Privacy Contact 7
11 Privacy, Security and Safety Plan 7
12 Internal privacy review 8
13 Privacy training and awareness 9
14 Handling privacy complaints 9
Part 3 – Privacy Policy 10
15 Application of Part 3 of this APP code 10
16 Disclosure of APP code participation 10
17 Disclosure of opt-in to Privacy Act 10
18 Privacy complaints 10
19 Third party recipients 11
20 Overseas recipients 11
Part 4 – Collection of children data 12
21 Application of Part 4 of this APP code 12
22 Prevent unfair collection of personal information from children 12
Part 5 – Limitation of secondary use 14
23 Application of Part 5 of this APP code 14
24 Limitation of use and disclosure 14
Part 6 – Direct Marketing 15
25 Application of Part 6 of this APP code 15
26 Use and disclosure for direct marketing 15
Part 7 – Governance 16
27 Code Administrator 16
28 Tasks of the Code Administrator 16

29 Privacy Code Integrity Committee 17
30 Tasks of the Privacy Code Integrity Committee 17
Part 8 – Independent Code Review 18
31 Independent Code Review 18
Part 9 – Compliance 19
32 Monitoring 19
33 Breaches of this APP code 19

Part 1 – Introduction

1 Name of APP code

(1) This APP code may be cited as the Privacy (Openly Australia) Code 2021.

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

2 Commencement

This APP code comes into force under the *Privacy Act 1988* (Privacy Act) when it is included on the Codes Register kept under subsection 26U(1) of that Act and will remain in force until such time that it is repealed.

3 Authority

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

4 Preamble

This APP code has been developed by Openly Australia, on its own initiative. This APP code is a written code of practice that applies to Openly Certified Entities that have been granted privacy certification by Openly. The primary purpose of this APP code is to provide Openly Certified Entities with greater clarity around how APP 1, APP 3, APP 6 and APP 7 are to be complied with, while incorporating higher standards of privacy protection than is required by the Privacy Act.

5 Definitions

Several expressions used within this APP code are defined in the Act and have the same meaning in this APP code including the following:

(a) APP code;
(b) APP entity
(c) Australian Link;
(d) Australian Privacy Principle;
(e) Codes Register
(f) Commissioner;
(g) consent;
(h) entity;
(i) holds;
(j) individual;
(k) overseas recipient;
(l) personal information;
(m) responsible person; and

(n) sensitive information.

In this APP code:

APP means Australian Privacy Principle as defined in the Act.

child has the meaning given by section 22.

contractor means an individual or entity that is or was a party to a contract and that is or was responsible for the provision of services to an entity under a contract.

Code Administrator means Openly Australia.

Designated Privacy Contact has the meaning given by section 10.

dispute resolution portal means a website operated by the Code Administrator that is used to lodge a complaint about an Openly Certified Entity.

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

high risk privacy project means a project that involves any new or changed ways of handling personal information that are likely to have an impact on the privacy of an individual/s.

OAIC means the Office of the Australian Information Commissioner.

OCE means Openly Certified Entity, an entity that has applied for and has been granted privacy certification by Openly Australia, and is an entity covered by the Privacy Act (including because they have opted-in under section 6EA of the Act, or because they have an Australian Link under section 5B of the Act).

online service means any device, service or product that sends or receives information using the internet including but not limited to: internet enabled gaming platforms, plug-ins, advertising networks, connected toys, Internet of Things (IoT) devices, voice over internet protocol (VOIP) services or internet enabled location-based services.

pre-filled link means a URL that includes the necessary parameters to load the relevant webpage without requiring additional user action or interaction.

Privacy, Security and Safety Plan has the meaning given by section 11.

6 Objectives

The objectives of this APP code are to:

(a) set out the specific requirements that an OCE must comply with, including how the APPs within the Act are to be applied and complied with by the OCE;

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

(c) build community confidence and trust in the privacy practices of the OCE; and

(d) encourage strong privacy governance from the OCE to create and sustain a culture of respect for the privacy of individuals.

7 Entities bound by this APP code

This APP code is binding upon all OCE's as defined in section 5 of this APP code.

8 Eligibility and coverage

(1) An APP entity will be bound by this APP code upon being granted privacy certification by the Code Administrator. From such time, the APP entity becomes an OCE.

(2) A current register of OCE's, and therefore of APP entities bound by this APP code, is maintained at www.openly.com.au.

(3) Any APP entity is eligible to become an OCE provided that the APP entity meets the requirements of privacy certification as determined by the Code Administrator.

Note 1: Under section 5B of the Act, an organisation may be considered an APP entity despite not being located in Australia if the organisation has an Australian Link.

Note 2: An act or practice overseas will not breach an Australian Privacy Principle or this APP code if the act or practice is required by an applicable foreign law (see sections 6A and 6B of the Act).

(4) Electing to become an OCE, and therefore electing to be bound by this APP code, is voluntary however this APP code is binding upon all OCE's as defined in section 5.

Part 2 – Transparency, compliance, and governance

9 Application of Part 2 of this APP code

For the purposes of paragraph 26C(2)(a) of the Act, Part 2 of this APP code sets out how APP 1.2 is to be complied with by an OCE.

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

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

10 Designated Privacy Contact

(1) An OCE must, at all times, have a Designated Privacy Contact. A Designated Privacy Contact may be an employee, or an externally appointed representative that can act on behalf of the OCE.

(2) The Designated Privacy Contact is the main point of contact for privacy matters relating to the OCE. The OCE may have more than one Designated Privacy Contact.

(3) An OCE must, at all times, maintain the accuracy of the contact details for the Designated Privacy Contact/s with the Code Administrator and within their privacy policy.

(4) An OCE must ensure that the Designated Privacy Contact shall have at least the following tasks:

(a) management of privacy inquiries, privacy complaints, requests for access to or correction of personal information made under the Act;

(b) assist in the development and maintenance of the Privacy, Security and Safety Plan as required by section 11;

(c) partake in the internal privacy review as required by section 12;

(d) provide reporting and to cooperate with the Code Administrator as required; and

(e) monitor compliance with the Act and this APP code.

(5) An OCE must ensure that the Designated Privacy Contact is sufficiently resourced to fulfil their functions as required by sub-section 10(4)(a)-(e).

(6) If the Designated Privacy Contact has other roles or functions, the OCE must ensure that the Designated Privacy Contact is able to perform their duties and tasks as required by sub-section 10(4)(a)-(e) in an independent manner.

11 Privacy, Security and Safety Plan

(1) An OCE must have a Privacy, Security and Safety Plan that is reviewed at least annually.

(2) The OCE must make its Privacy, Security and Safety Plan available to all employees and any contractor who handles, or who may handle personal information.

(3) A Privacy, Security and Safety Plan is a document that details at least the following:

(a) who the Privacy, Security and Safety Plan applies to within the OCE;

(b) how the OCE considers the impact of high-risk privacy projects;

(c) how the OCE manages and reviews privacy documentation, including its privacy policy;

(d) how the OCE manages the secure disposal of personal information;

(e) how the OCE manages information security including the physical, technical and administrative safeguards implemented to protect personal information against risks including, but not limited to:

i. accidental loss;

ii. unauthorised access;

iii. unauthorised destruction;

iv. unauthorised use;

v. unauthorised modification; or

vi. unauthorised disclosure.

(f) how the OCE manages the risk of cyber-bullying and cyber-abuse within the OCE, including reference to applicable policies;

(g) how the OCE manages the risk of online scams and identity theft within the OCE, including reference to applicable policies;

(h) the steps taken by the OCE to ensure consistent compliance with the APPs and this APP code; and

(i) where sub-section 22(1) applies, how the OCE safeguards the privacy, security and safety of children.

12 Internal privacy review

(1) An OCE must regularly review and update its internal privacy policies, processes and procedures, to ensure consistent compliance with the APPs and this APP code. The scope of this review must include at least:

(a) any privacy policy prepared for compliance with APP 1;

(b) any privacy notice prepared for compliance with APP 5;

(c) any privacy complaint handling process or policy prepared for compliance with section 14 of this APP code; and

(d) any Privacy, Security and Safety Plan prepared for compliance with section 11 of this APP code.

13 Privacy training and awareness

(1) An OCE must implement a privacy training and awareness program that is regularly delivered to employees across the OCE.

(2) An OCE must ensure that employees and contractors who handle, or who may handle, personal information as a part of their role understand their privacy obligations under this APP code and the APPs.

14 Handling privacy complaints

(1) An OCE must handle privacy complaints received by individuals courteously and ensure that individuals will not be treated unfavourably, including in the way the OCE communicates and provides services both during its consideration of the privacy complaint and once the privacy complaint is finalised.

(2) An OCE must accept privacy complaints in writing, by phone, by email or by other electronic means.

(3) An OCE must take reasonable steps to resolve a privacy complaint within 21 days.

(4) If an OCE is not able to resolve a privacy complaint within 21 days, the OCE must:

(a) inform the complainant of this fact prior to the end of that period and provide a reason for the delay, the expected timeframe to resolve the complaint and seek their agreement to an extension for a period that is reasonable in the circumstances; and

(b) advise that the complainant may complain to Code Administrator and provide a pre-filled link to the Code Administrator's dispute resolution portal.

(5) An OCE must report annually to the Code Administrator about privacy complaints relating to this APP code. This report covers the 12 month period to 30 June and must detail the at least the following:

(a) the number of privacy complaints received;

(b) the nature of privacy complaints received;

(c) the outcome of privacy complaints received;

(d) the average time taken to resolve privacy complaints; and

(e) information about the remedies awarded in finalising privacy complaints.

Part 3 – Privacy Policy

15 Application of Part 3 of this APP code

For the purposes of paragraph 26C(2)(a) of the Act, Part 3 of this APP code sets out how APP 1.4 is to be complied with by an OCE.

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

Note 2: In addition to complying with this APP code, an OCE may need to take additional steps in order to satisfy its obligations under APP 1.4.

16 Disclosure of APP code participation

(1) An OCE must disclose, within its privacy policy, that it is bound by this APP code. The disclosure must include:

(a) a pre-filled link to the Code Administrator's public register;

(b) the date from which the OCE was bound by this APP code; and

(c) a link to this APP code.

17 Disclosure of opt-in to Privacy Act

(1) Where an OCE is required to opt-in to the Privacy Act, the OCE must disclose that it is bound by the Act. This disclosure must include:

(a) a link to the OAIC Privacy Opt-In Register; and

(b) a link to the APPs.

18 Privacy complaints

(1) The OCE must make information about its privacy complaints handling process available within its privacy policy. This must include, but is not limited to:

(a) how privacy complaints can be made;

(b) how privacy complaints will be handled;

(c) the criteria used for assessing privacy complaints;

(d) how privacy complaints may be resolved;

(e) the timeframes for investigating and responding to privacy complaints; and

(f) the contact details of the Designated Privacy Contact as required by section 10.

Note: In addition to complying with this APP code, an OCE may need to take additional steps in order to satisfy its obligations under APP 1.4(e).

19 Third party recipients

(1) Where an OCE discloses, or is likely to disclose, personal information to a third party recipient, the OCE must include at least the following information within its privacy policy:

(a) the name of the third party recipient;

(b) the purpose for disclosure to the third party recipient; and

(c) the safeguards in place to ensure the overseas recipient handles personal information in compliance with the APPs and this APP Code.

20 Overseas recipients

(1) Where an OCE discloses, or is likely to disclose, personal information to an overseas recipient, the OCE must include at least the following information within its privacy policy:

(a) the name of the overseas recipient;

(b) the purpose for disclosure to the overseas recipient;

(c) the country in which the overseas recipient is located; and

(d) the safeguards in place to ensure the overseas recipient handles personal information in compliance with the APPs and this APP Code.

Note: To avoid doubt, this subsection enhances the OCE's obligations under APP 1.4(g).

Part 4 – Collection of children data

21 Application of Part 4 of this APP code

For the purposes of paragraph 26C(2)(a) of the Act, Part 4 of this APP code sets out how APP 3.5 is to be complied with by an OCE.

Note: In addition to complying with this APP code, an OCE may need to take additional steps in order to satisfy its obligations under APP 3.5.

22 Prevent unfair collection of personal information from children

(1) This section only applies where:

(a) an OCE operates a website or online service that is primarily directed toward children; or

(b) an OCE operates a website or online service that is directed toward a general audience, but the OCE has actual knowledge that it collects personal information about children; or

(c) an OCE, through use of an ad network, third party tool or plug-in, has actual knowledge that it is collecting personal information about children.

Note: This subsection does not apply if the OCE is required to, by law, collect personal information relating to children.

(2) Where sub-section 22(1) applies, an OCE must:

(a) obtain consent from a responsible person before collecting personal information from a child;

(b) provide a plain language and easy to understand version of its privacy policy anywhere personal information may be collected from a child. This privacy policy must include:

i. the types of personal information collected about the child;

ii. how the personal information is collected;

iii. how the personal information will be used;

iv. whether it discloses personal information collected from children to third parties. If it does, its privacy policy must list the types of businesses it discloses information to and how third parties use the personal information; and

v. a description of the responsible person's rights, including how a responsible person can revoke consent on behalf of the child, view the child's personal information or delete the child's personal information.

(3) Where sub-section 22(1) applies, an OCE must not:

(a) collect more personal information from the child than is necessary to operate the core functionality of the website or online service; and

(b) use personal information collected from children to target direct marketing; and

(c) make changes to its privacy policy without notifying the responsible person that provided the consent.

(4) Where sub-section 22(1) applies, at the request of a responsible person, an OCE must provide a mechanism that allows the responsible person to:

(a) revoke consent on behalf of the child;

(b) view the child's personal information; and/or

(c) delete the child's personal information.

(5) For the purposes of this APP code, a child is any individual under 13 years of age.

Part 5 – Limitation of secondary use

23 Application of Part 5 of this APP code

For the purposes of paragraph 26C(2)(a) of the Act, Part 5 of this APP code sets out how APP 6.1 and APP 6.2 are to be complied with by an OCE.

24 Limitation of use and disclosure

(1) An OCE must not use or disclose personal information for any purpose other than the purpose for which it was originally collected (primary purpose) unless 24(2)(a)-(e) applies.

Note: To avoid doubt, this subsection enhances the OCE's obligations under APP 6.1.

(2) An OCE may only use or disclose personal information for a purpose other than the primary purpose if:

(a) the individual has consented to the use or disclosure of the information; or

(b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or

(d) a permitted health situation exists in relation to the use or disclosure of the information by the entity; or

(e) the OCE reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Note 1: To avoid doubt, this subsection enhances the OCE's obligations under APP 6.2.

Note 2: For permitted general situation, see section 16A of the Australian Privacy Principles guidelines. For permitted health situation, see section 16B of the Australian Privacy Principles guidelines.

Part 6 – Direct Marketing

25 Application of Part 6 of this APP code

For the purposes of paragraph 26C(2)(a) of the Act, Part 6 of this APP code sets out how APP 7.2 and APP 7.3 are to be complied with by an OCE.

26 Use and disclosure for direct marketing

(1) Despite APP 7.2 and APP 7.3, an OCE must not use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing unless 26(2)(a)-(d) or 26(3)(a)-(e) applies.

(2) An OCE may only use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

(a) the OCE collected the personal information from the individual directly; and

(b) the individual has consented to the use of the personal information for the purposes of direct marketing; and

(c) the OCE provides a simple means by which the individual may easily request not to receive direct marketing communications from the OCE; and

(d) the individual has not made such a request to the OCE.

(3) An OCE may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

(a) the OCE collected the information from someone other than the individual; and

(b) the individual has consented to the use of personal information for the purposes of direct marketing; and

(c) the OCE provides a simple means by which the individual may easily request not to receive direct marketing communications from the OCE; and

(d) in each direct marketing communication with the individual:

i. the OCE includes a prominent statement noting that the individual may make such a request; or

ii. the OCE otherwise draws the individual's attention to the fact that the individual may make such a request; and

(e) the individual has not made such a request to the OCE.

Part 7 – Governance

27 Code Administrator

(1) The Code Administrator for this APP code is Openly Australia (ABN 83 612 417 259). In practice, this APP code is administered by the Openly Privacy Code Integrity Manager, under the direction of the Openly Board of Directors.

(2) Openly will fund the administration of this APP code in such manner as deemed adequate by the Openly Board of Directors, having regard for the resources required to effectively execute the tasks and responsibilities as defined in section 28.

28 Tasks of the Code Administrator

(1) In administering this APP code, the Code Administrator shall have at least the following tasks:

(a) assess each application to become an OCE on merit;

(b) maintain an accurate online public register of OCE's that are bound by this APP code;

(c) monitor and report on compliance with this APP code as required by Part 9;

(d) produce a quarterly public transparency report to demonstrate the integrity of this APP code;

(e) on the Openly website, make freely available, and maintain online copies of:

i. the in-force version of this APP code;

ii. information and supporting documentation relating to this APP code;

iii. contact details for the Code Administrator;

iv. the dispute resolution policy for complaints relating to alleged breaches of this APP code;

v. the annual report relating to compliance with this APP code;

vi. any other information that the Code Administrator considers relevant or necessary to demonstrate the integrity, transparency and proper function of this APP code.

(f) maintain the complaints handling process relating to alleged breaches of this APP code, and adequately handle any complaints relating to alleged breaches of this APP code;

(g) commission periodic reviews of this APP code in accordance with Part 8, and produce a written response to such a report;

(h) consider the need for any variation of this Code, and make any consequent applications;

(i) perform any such tasks as the Openly Board of Directors considers necessary or desirable to ensure the effective operation of this APP code.

29 Privacy Code Integrity Committee

(1) The Code Administrator will establish a Privacy Code Integrity Committee, comprising of an independent chair, at least one industry representative and at least one consumer representative.

(2) The Privacy Code Integrity Committee will convene at least quarterly.

30 Tasks of the Privacy Code Integrity Committee

(1) The Privacy Code Integrity Committee shall have at least the following tasks:

(a) ensure the integrity of the application process, and participate in any review of decisions relating to applications to become an OCE;

(b) ensure the transparent operation of this APP code;

(c) oversee the handling of complaints relating to breaches of this APP code;

(d) advise on consumer awareness initiatives relating to this APP code; and

(e) advise on the need for variation of this APP code.

(2) The Privacy Code Integrity Committee will advise the Code Administrator on the timing and conduct of the independent review as required by Part 8.

Part 8 – Independent Code Review

31 Independent Code Review

(1) An Independent Code Review of this APP code is required to be conducted at least every five years to ensure it is meeting its objectives and is operating effectively. Additionally, the Code Administrator may commission a review at any time it considers appropriate.

(2) The Code Administrator will appoint an independent reviewer for each Independent Code Review.

(3) The Code Administrator will fund the Independent Code Review in such manner as it considers appropriate, having regard to the resource requirements necessary for the effective execution of the review.

(4) The Code Administrator, with the assistance of the Privacy Code Integrity Committee, will define the scope of the Independent Code Review.

(5) As a part of the Independent Code Review, the Code Administrator will conduct adequate consultation with appropriate stakeholders regarding the operation and effectiveness of this APP code.

(6) The report resulting from the Independent Code Review will be made publicly available, alongside a response from the Code Administrator.

Part 9 – Compliance

32 Monitoring

(1) The Code Administrator will conduct regular audits to ensure OCE's maintain ongoing compliance with this APP code.

(2) The Code Administrator will report systemic issues or serious and repeated breaches of this APP code to the Commissioner.

(3) OCE's must notify eligible data breaches to the OAIC and otherwise comply with the Eligible Data Breach requirements of the Privacy Act. OCE's should also inform the Code Administrator of any such notification to ensure the transparent operation of this APP code.

33 Breaches of this APP code

(1) If the Code Administrator believes that an OCE has acted in breach of this APP code, the Code Administrator may direct the OCE to remedy the breach within a specified timeframe.

(2) If the Code Administrator believes that an OCE has acted in serious breach of this APP code, the Code Administrator may elect to take action against the OCE, as is permitted under the relevant policies and guidelines, up to and including revocation of the OCE's privacy certification.

(3) These provisions operate independently of the complaint provisions within the Privacy Act and the enforcement role of the Commissioner.