



Certification Guidelines - DRAFT

Version: 4.0.0

Updated: 23 February 2021

Public Release: Yes

Table of Contents

Table of Contents.....	2
Glossary of terms	3
1. Introduction.....	5
2. Background	6
3. Why apply for certification?	7
4. How to apply for certification	8
4.1 Starting an application	8
4.2 Lodging a valid application	8
4.3 Amending an application.....	8
4.4 Withdrawing an application.....	8
4.5 Providing false or misleading information.....	8
5. The application process.....	9
5.1 Initial assessment and validation check.....	9
5.2 Certification Agreement	9
5.3 Application fees	10
5.4 Self-assessment	10
5.5 Audit	10
5.6 Requests for further information.....	10
5.7 Opting in to the Privacy Act.....	11
5.8 Overseas entities	11
6. Certification decisions	12
7. Commencement of certification	13
8. Inclusion on the Openly Certification Register.....	14
9. Ongoing Compliance	15
10. Annual re-certification	15
11. Transfer, surrender, revocation and termination of certification.....	15
11.1 Transfer	15
11.2 Surrender.....	15
11.3 Revocation and Termination	16
12. Reporting	16
12.1 Annual Reporting	16
12.2 Reporting Notifiable Data Breaches.....	17
13. Privacy Statement	17
14. Dispute resolution summary.....	17
14.1 External review	18

Glossary of terms

Many terms used in this Code have their meaning defined in the Privacy Act. Further explanation of some of those terms in the Openly context is required, and the meaning of other key terms is also set out in this section:

APPs means the Australian Privacy Principles as published by the Office of the Australian Information Commissioner and accessible [here](#).

Applicant Entity ('Applicant') means an Entity applying to become Openly Certified.

Application Status means the status of the Entity's application, including:

Approved means a decision made by Openly to grant Openly certification to an Entity.

Manual review required means the decision by Openly to consider an applicant manually (rather than through an automatic decision).

Refused means the decision made by Openly not to grant an Entity Openly certification.

Certification Register means the Openly online public register on which the Status is listed for clients of Openly.

Office of the Australian Information Commissioner (OAIC) means the Federal independent statutory agency, headed by the Australian Information Commissioner in the Attorney-General's portfolio.

Openly Australia means Win3Pty Ltd trading as Openly Australia.

Openly Certification Agreement ('the Agreement') means the contractual agreement between an Openly Certified Entity and Openly Australia Pty Ltd duly entered into.

Openly Certification Guidelines ('the Guidelines') means this document.

Openly Certified Entity, ('Entity' or 'Entities') means an Entity that has been granted Openly Certification.

Openly Dispute Resolution Policy ('Dispute Resolution Policy') means the policy outlining how an individual or Entity may complain or provide feedback to Openly.

Openly for Business portal means the log-in system for Openly Certified Entities to log into their individual profiles.

Openly Privacy Code ('the Code') means the Openly Privacy Code (an APP Code developed under section IIIB of the Privacy Act).

Privacy Act means the Privacy Act (1988).

Status means the status of the Entity's certification on the Certification Register.

Symbol means the Symbol logo and any derivative works owned by Openly and related artwork made available by Openly to the Entity from time to time.

Symbol Device means the software code owned and supplied by Openly and embedded into the Entity's websites so as to enable display of the Symbol on the websites.

1. Introduction

Openly Australia (Openly) administers a Certification Register which lists entities who have voluntarily obtained Openly Privacy Certification.

Entities that wish to obtain Openly Privacy Certification are required to complete the application process as set out herein.

Openly Certified entities are required to comply with the Certification Guidelines (the Guidelines), the Privacy (Openly Australia) Code 2021 (the Code) and the Certification Agreement (the Agreement) at all times.

The Agreement, in conjunction with these Guidelines and the Code set out the criteria that Openly Australia will apply when considering an application for certification.

The Guidelines aim to provide guidance to assist applicants in lodging a valid application for privacy certification, outline other processes and provide further details around how Openly will interpret the Code and the Agreement.

As this is an evolving document, the Guidelines may be updated from time to time and are not to be interpreted as an exhaustive list of all aspects of the certification process.

When significant changes are made to these Guidelines, Openly will post the new version on its website.

Enquiries about Openly Privacy Certification that are not included in this document should be directed to Openly Business Support [via email](#).

2. Background

Openly is a privacy-tech start-up that exists to develop products, tools and resources for individuals that increase digital literacy, enhance privacy, build trust and promote online safety.

To make it easier for consumers to understand their privacy rights and compare business privacy practices, Openly has established Openly Certified which acts as a privacy certification scheme. Entities are assessed against a common set of standards and are granted certification upon successful completion of the program requirements.

To strengthen compliance with the requirement of the scheme, Openly has created a Privacy Code which imposes additional compliance requirements upon entities over and above the Privacy Act. When this Code becomes a registered APP Code, Openly Certified will become a voluntary but legally binding code that can be applied to any entity that is seeking privacy certification.

3. Why apply for certification?

By successfully obtaining privacy certification, entities are demonstrating their adherence to additional privacy standards that exceed the requirements of the Privacy Act and the APPs, furthering privacy protections for their customers, staff and individuals.

Additionally, by obtaining Openly Privacy Certification, Entities are demonstrating that they comply with the APPs and the Code, which will reduce the risk of regulatory compliance issues and may reduce the risk of negative privacy events.

4. How to apply for certification

4.1 Starting an application

An application for certification must be made through the Openly website using the electronic form located on the Openly website [here](#).

4.2 Lodging a valid application

To lodge a valid application, the electronic application form must be completed in full. It cannot be saved and must be completed in one sitting.

4.3 Amending an application

Applications can be amended in instances of mistakes or omissions, however an application cannot be amended once a certification decision has been made. This measure protects the integrity of the certification process and avoids attempts to circumvent automated flagging of applications.

Requests to amend an application should be made [via email](#).

4.4 Withdrawing an application

An application can be withdrawn at any time during the application process [via email](#). The email should include the application reference number, the Entity's name and the contact person listed on the application form. If an application is withdrawn after the application fee has been paid, the application fee is non-refundable.¹

4.5 Providing false or misleading information

Providing false or misleading information in an application (including by way of material omission) may result in revocation of certification. [Australian Consumer Law \(ACL\)](#) prohibits misleading or deceptive conduct and false or misleading representations. False, deceptive, or misleading declarations made throughout the application process will be referred to the Australian Competition and Consumer Commission (ACCC) for investigation and may result in monetary fines and/or further action.

¹ Openly Certification Agreement 2020 clause 11.4 (b)

5. The application process

5.1 Initial assessment and validation check

The application form requires information about the authorised Entity representative and the Entity. This information is used to assess the application for certification, populate the Certification Register or otherwise administer the certification program.

Information sought includes:

- Information relating to the authorised Entity representative;
- A secure password to access the dashboard;
- The trading name, ABN, website address and primary address of operation for the Entity;
- The number of employees and type of Entity;
- Information relating to historical privacy related events, types of data collection and information;
- Declarations of compliance with relevant laws, truth, and accuracy;
- Recognition of certification or accreditation with other privacy schemes; and
- Any other information requested by Openly.

Once an application has been submitted, an assessment is conducted to validate that the application meets the criteria for certification. An application will then be granted an Application Status of 'approved', 'manual review required' or 'refused'.

Applicants should use the resources available on Openly's website to ensure they meet the criteria for certification prior to commencing the application process.

5.2 Certification Agreement

Once an application has progressed through the initial assessment and validation checks, the applicant will be required to review and sign the Certification Agreement.

The Agreement must be reviewed and signed by an authorised representative of the Entity within 10 business days from the date of delivery. On the 11th day from the date of delivery², the Certification Agreement will be deemed as void, and the application will be granted an Application Status of refused.

The Certification Agreement is a legally binding contract between Openly and the Entity and cannot be altered by the Entity unless there has been prior written approval. The Agreement must be accepted or declined by the Entity in the form it is received in.

² Refer to Certification Agreement clause 15 for more information about when notice is deemed to be received.

5.3 Application fees

Once the Agreement has been accepted by the Applicant, an invoice with the application fee will be and is payable to Openly within 14 business days.

The application fee must be made within 14 days for the Applicant to have use of the Code, the Privacy Certified by Openly Device Symbol³ and to be listed on the Certification Register.

If an Applicant does not complete an application or if the Applicant is refused certification after the application fee has been paid, this fee will be forfeited. The application fee is non-refundable regardless of the certification decision.⁴

5.4 Self-assessment

The self-assessment is conducted via the Openly For Business online portal, and assesses the policies, procedures, and processes of the Applicant.

The self-assessment consists of fifteen mandatory modules, assessing compliance with best practice, the Code, the Guidelines, the Agreement and Australian Privacy Law.

Once the Applicant has completed those modules, Openly will receive automated notice of the completion and will then complete an audit of the Applicant's responses.

5.5 Audit

In the audit phase, Openly will validate the Applicant's self-assessment and will cross-check responses against publicly available information.

Openly may also investigate operation of the Applicant's website and may use third-party tools to evaluate privacy compliance.

The audit consists of up to forty validation points, and Openly may request further information from the Applicant during this phase. To ensure the efficient progression of the application process, Openly may request specific information in relatively short timeframes.

5.6 Requests for further information

At any time, Openly may request further information to assist in assessing an application.

A request for further information may be made to the Applicant by way of an interview, in writing, by phone or through any other electronic means.

³ Openly Certification Agreement 2020 clause 3

⁴ Openly Certification Agreement 2020 clause 11.2 (b)

Openly Australia may also seek further information from third party sources or through use of publicly available information. This information can be used to assist in assessing an application.

5.7 Opting in to the Privacy Act

Entities that would not ordinarily be bound by the Australian Privacy Act due to turnover or other exemptions are required to opt-in to the Act through the privacy opt-in register.

Information about the privacy opt-in register is located at [here](#).

The Office of the Australian Information Commissioner (OAIC) requires a copy of the Entity's privacy policy and the form to opt-in to the register can be located [here](#).

Once OAIC has accepted the Entity's application to opt-in and has been listed on the [Register](#), the Entity should contact Openly to provide evidence of this. Openly may confirm with OAIC the status of the Entity's application if it is not yet publicly accessible.

5.8 Overseas entities

Under section 5B of the Privacy Act, an overseas entity may be considered an APP entity despite not being located in Australia if the organisation has an Australian Link. If an overseas entity has a verifiable Australian Link, Openly will accept their application for certification.

6. Certification decisions

Openly assesses all applications based on merit.

If an Applicant has successfully submitted a valid application and has satisfactorily completed the requirements as set out in section 5 of these Guidelines, the Applicant will be granted certification.

If Openly is not satisfied that an Applicant has successfully submitted a valid application, or if the Applicant has not satisfactorily completed the requirements set out in section 5 of these Guidelines, the Applicant will be refused Openly certification.

Openly maintains a Dispute Resolution Policy that sets out how an Applicant can dispute a certification decision.

7. Commencement of certification

Certification commences from the date in which an Entity is notified that their application has been approved and certification has been granted.

The notice of decision is delivered by email to the authorised Entity representative and contains information including the:

- Date of notice
- Application number
- Application outcome

If the Entity is successfully granted certification, it will also receive:

- A copy of the Openly Certification Device⁵
- Technical Information about how to implement the Openly Certification Device⁶

⁵ Openly Certification Agreement clause 3

⁶ Openly Certification Agreement clause 3

8. Inclusion on the Openly Certification Register

Certified entities will be included on the publicly available [Openly Certification Register](#) located on the Openly website.

The Openly Certification Register is maintained by Openly.

The Register may include information such as the Entity's name, trading name and other available publicly available information or information provided by the Entity throughout the application process but will not include confidential information about the Entity.

Approved entities will be added to the Openly Certification Register within 3 business days from the date in which certification commences.

Openly reserves the right to review an Entity's status as per the processes in the Openly Dispute Resolution Policy, including revoking an Entity's certified status, removing the Entity's ability to use the Openly Certified Device or any other restrictive action as required.

9. Ongoing Compliance

Openly will assess the Entity's ongoing compliance with these Guidelines, the Code and the Agreement.

If Openly is not satisfied that an Entity has successfully demonstrated ongoing compliance, Openly may impose conditions, request remediation, or in some circumstances, revoke certification.

10. Annual re-certification

Entities are required to complete re-certification every twelve months.

Openly will contact Entities nearing their re-certification with further information about the re-certification process.

11. Transfer, surrender, revocation and termination of certification

11.1 Transfer

Certification cannot be transferred, even between related bodies corporate.

For the avoidance of doubt, certification usually only covers one website or one privacy policy. A body corporate that wishes to attain certification across multiple entities will usually need to apply for a separate certification for each Entity.

If you are a body corporate, please [contact us](#) before starting an application to confirm whether separate certifications are required for each Entity.

11.2 Surrender

If an Entity no longer wishes to be certified it may apply to Openly to surrender certification. Applications to surrender certification must be made in writing.⁷

Openly will respond to the Entity's application to surrender certification in writing within 10 business days.

For the avoidance of any doubt, any application fees paid to Openly are non-refundable, including in the case of surrender.⁸

⁷ Refer to Certification Agreement clause 15 for more information about when notice is deemed to be received.

⁸ Openly Certification Agreement clause 11.2(b)

11.3 Revocation and Termination

Openly Australia may only revoke certification in certain circumstances, for example if:

- Openly reasonably believes that certification was granted on the basis of misleading or deceptive conduct or representations, or that the certification was improperly obtained; or
- Openly reasonably believes the Entity has contravened a law; or
- Openly reasonably believes that the Entity has contravened the Guidelines, the Agreement, or the Code; or
- Openly reasonably believes that it would be detrimental to the health, safety, security, privacy, or reputation of Openly, an Entity or an individual to not revoke certification; or
- Openly is directed to revoke certification by the OAIC or the ACCC.

If Openly Australia moves to revoke certification, the certified Entity will be notified of that fact and the certified Entity will be given reasonable time to respond.

Any application fees paid to Openly are non-refundable, including in the case of revocation or termination by either party.

Openly maintains a Dispute Resolution Policy that sets out how an Entity can dispute a revocation decision.

However, immediately upon termination of the Certification Agreement, the Entity must:

- comply with these Certification Guidelines;
- cease using the Licensed IP;
- remove the Symbol Device from the Websites;
- destroy any copies of the Licensed IP (in any form) in its possession and certify said destruction to Openly in writing; and
- pay to Openly all amounts owed to Openly under the Certification Agreement.

12. Reporting

12.1 Annual Reporting

Certified Entities are required to report to Openly, by June of each year, information about any complaints they received relating to the Code.

Openly will provide Certified Entities with a standardised template prior to the reporting deadline to ensure the correct information is reported.

12.2 Reporting Notifiable Data Breaches

Under the [Notifiable Data Breach \(NDB\) scheme](#) an organisation or agency must notify affected individuals and the OAIC about an eligible data breach.

An eligible data breach occurs when:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation or agency holds;
- this is likely to result in serious harm to one or more individuals, and;
- the organisation or agency hasn't been able to prevent the likely risk of serious harm with remedial action.

In addition to the obligations an Entity owes to OAIC, Openly Certified Entities are required to advise Openly of a notifiable data breach.⁹ The Entity should submit a copy of the notification form provided to OAIC via the Openly For Business dashboard.

Openly reserves the right to consider whether, as a result of the Notifiable Data Breach, the Entity has breached the Certification Agreement or the Code, and whether this has caused reputational damage or poses an ongoing risk to the public in determining whether the revoking of the Entity's certification is appropriate.

13. Privacy Statement

Openly will comply with all applicable Privacy Laws in relation to any Personal Information that is collected, stored, used, disclosed or otherwise dealt with under or in connection with the Certification Agreement.

Openly has opted-in to the OAIC's Privacy opt-in [register](#). Therefore, Openly is covered by the Privacy Act and the APP's and has made a public commitment to good privacy practice.

Openly's privacy policy can be located on the [Openly website](#).

14. Dispute resolution summary

Complaints about:

- the application process;
- the outcome of a certification decision;
- the decision to caution or direct remediation;
- the decision to take restrictive action; or

⁹ Further information about what a notifiable data breach is can be located at oaic.gov.au

- the decision to revoke certification,

should be raised directly with Openly in the first instance. The Dispute Resolution Policy outlines the specific requirements and actions Openly can take.

14.1 External review

An external review is only concerned with the legality of a decision, for example, whether Openly Australia had the authority to make the decision, whether it has considered an irrelevant fact or failed to consider a relevant fact, or whether the decision was so unreasonable that no reasonable decision maker could have made it.¹⁰

An Entity may apply to an approved third-party dispute resolution body for an external review on any question of law arising out of a decision of Openly's internal review. The initiating of an external review is at the cost of the applicant and must be conducted by an approved third-party dispute resolution body as outlined in the Openly Dispute Resolution Policy.

¹⁰ Openly Dispute Resolution Policy clause 7