Approval to participate in AGDIS form

Warning: It is a serious criminal offence under the Commonwealth Criminal Code to provide false or misleading information. False or misleading information in an application (including a material omission) may also be grounds to revoke any approval granted based on that information.

Personal information

Some of the information you provide in your application for approval to participate in the Australian Government Digital ID System (AGDIS) may constitute personal information for the purposes of the *Privacy Act 1988* and the *Digital ID Act 2024*. This notice is intended to inform you of matters related to our collection of personal information contained in your application and should be read in conjunction with the ACCC's Privacy Policy.

Why we are collecting personal information

Information, including any personal information, contained in your application is being collected by the ACCC as the Digital ID Regulator for the purposes of:

- assessing your application for approval to participate in the AGDIS in accordance with the *Digital ID Act 2024;* and
- administering, and otherwise facilitating the proper functioning of the *Digital ID Act 2024*.

What happens if you do not provide requested personal information.

If you do not provide personal information relevant to your application for approval to participate in the AGDIS, that may impact our ability to assess your application.

Whom we may disclose personal information to

Information contained within AGDIS approval applications, including personal information, may be disclosed to:

- other Commonwealth agencies (for example, the Office of the Australian Information Commissioner and Services Australia in their capacity as the System Administrator);
- State and Territory police forces;
- international regulators and law enforcement bodies;
- external consultants engaged by us

to assist our assessment of AGDIS approval applications.

The information, including any personal information, contained in AGDIS approval applications is collected, and stored on servers, in Australia, in a secure environment. As above, personal information contained in AGDIS approval applications may be disclosed overseas to relevant

international regulators and law enforcement bodies to assist our assessment of AGDIS approval applications.

Information about how to access your personal information, how to correct your personal information and how to complain about our handling of your personal information (and how we'll deal with such a complaint) is set out in the ACCC's Privacy Policy.

By ticking the box below, you confirm that you have obtained the consent of any individual to whom personal information contained in your AGDIS approval application relates to disclose their personal information to the ACCC (as the Digital ID Regulator) to be collected, used and disclosed for the purposes set out above.

☐ **Yes**

Screening check

☐ If your organisation is applying to become an Accredited Entity in the AGDIS, it must receive accreditation before approval can be granted.

☐ Your organisation must be an eligible entity type to participate.

☐ I acknowledge that my organisation must comply with all Digital ID legislation including *the Digital ID Act 2024*, Digital ID Rules, the Accreditation Rules, the Digital ID Data Standards and the service levels relevant to your organisation's approval to participate.

☐ Your organisation must commence participating in the AGDIS on its participation start date.

Before applying, your organisation must have plans and procedures in place relating to its participation in the AGDIS for the following:

- ☐ Effective written procedures to notify the System Administrator promptly of planned or unplanned outages or downtime affecting your organisation's IT system where these will or could be reasonably expected to have a material effect on the operation of the AGDIS.
- ☐ Effective written procedures to notify the System Administrator promptly of planned or unplanned outages which may have material effects on the operation of the AGDIS.
- ☐ Cyber security plan (includes conducting a risk assessment)
- ☐ Digital ID fraud management plan (includes conducting a risk assessment)
- ☐ Disaster recovery and business continuity plan

☐ I acknowledge my organisation is responsible for the operation of the service(s) in the AGDIS, including providing contact information and responding to any event.

Service

1. Specify the service

2. What service type is your organisation applying for approval to participate in the AGDIS?

- ☐ Attribute provider (ASP)
- ☐ Exchange provider (IXP)
- ☐ Identity provider (ISP)
- ☐ Participating Relying Party (PRP)

Approval details

1. Are other organisations responsible for the delivery of the service?

☐ Yes ☐ No

If yes, who are the other organisations? What are their roles?

2. Is the service eligible to participate in the AGDIS?

☐ Yes ☐ No

System Administrator testing and onboarding

1. Has your organisation engaged with the System Administrator to conduct testing?

☐ Yes ☐ No

If yes, what is your organisation's Key Identifier provided by the System Administrator?

Address for notices

1. Does the organisation consent to notices and other documents under the Digital ID framework being given by email?

   ☐ Yes ☐ No

2. What is the email address which may be used to give the organisation any notice or other document under the Digital ID framework by email?

3. What is the physical address which may be used to give the organisation any notice or other document under the Digital ID framework?

4. What is the postal address which may be used to give the organisation any notice or other document under the Digital ID framework?

5. What type of provider is your organisation applying for approval to participate in the AGDIS?

   ☐ Accredited Entity [*answer all Accredited Entities questions on pages 5 – 6]*

   ☐ Participating Relying Party [*answer all Relying Party questions on pages 6 – 8]*

Accredited Entities - Approval details Service

1. What type of entity is your organisation?

   ☐ Non-corporate Commonwealth entity

   ☐ State and Territory Government entity

   ☐ None of the above

2. Does your organisation intend to offer this accredited service outside the AGDIS?

   ☐ Yes ☐ No

Accredited Entities - Conditions

1. Your organisation's application for approval will include any conditions applied to its accreditation. Does your organisation wish to make changes to these conditions?

   ☐ Yes ☐ No

2. Which accreditation conditions does your organisation wish to change?

3. What are the requested changes?

4. Does your organisation wish to apply for a condition?

5. Provide details of the condition your organisation is seeking.

6. Provide supporting evidence which may include justification, risk assessments and other relevant documents applicable to the condition.

7. Does your organisation wish to apply for another condition?

   ☐ Yes ☐ No

   If yes, please provide the information for each additional condition you are applying for in a separate document.

Accredited Entities - Plans and procedures

The Plans and procedures declaration for accredited entities seeking approval to participate in the AGDIS form to be downloaded from the Digital ID System website and must be attached with your application.

Relying Party – Approval details Service

1. What is your entity type?

   ☐ Commonwealth entity

   ☐ Commonwealth company

   ☐ State and Territory Government entity

   ☐ None of the above

2. Will the service access the AGDIS directly or via another service?

O Yes O No

If yes, which service?

3. Who owns the service?

4. Is the service only accessible using digital ID?

O Yes O No

If yes, does the service meet an exception to the requirement that creating and using a Digital ID be voluntary? Please provide details.

Relying Party - Probity requirements

Please attach the relevant fit and proper person or probity forms and associated evidence. Please refer to the Digital ID Rules and Digital ID Regulator's guidance for the template forms and more information.

Relying Party - Conditions

1. Does your organisation wish to apply for a condition?

- ○ Restricted attributes
- ○ Other condition
- ○ No

Restricted attribute condition questions

A participating relying party must not collect a restricted attribute unless authorised by a condition.

Examples of restricted attributes include health information, information about a criminal record, or an identifier of an individual contained on a government issued document.

1. Nominate each restricted attribute your organisation is seeking to collect and the circumstances in which each restricted attribute will be collected or disclosed (if approved).

2. Explain why each restricted attribute needs to be collected or disclosed.

3. Why can a similar outcome not be achieved without collecting or disclosing the restricted attribute(s).

4. Is the collection or disclosure of the restricted attribute regulated by other legislative or regulatory requirements?

   ☐ Yes ☐ No

   If yes, what legislation or regulation?

   and, how would your organisation comply with those regulatory requirements if the condition to collect and disclose the restricted attribute is granted?

5. Does your organisation wish to apply for another condition?

   ☐ Restricted attributes

   ☐ Other condition

   ☐ No

Other condition questions

1. Provide details of the condition your organisation is seeking.

2. Provide supporting evidence which may include justification, risk assessments and other relevant documents applicable to the condition.

3. Does your organisation wish to apply for another condition?

   ○ Yes ○ No

   If yes, please provide the information for each additional condition you are applying for in a separate document.

Relying Party - Exemptions forecasting

1. If approved to participate in the AGDIS, will your organisation be seeking an exemption from the requirement that creating and using a digital ID be voluntary for individuals?

   ○ Yes ○ No

2. Please provide details of why your organisation intends to seek an exemption, including details of the service(s) that would be impacted and why your organisation considers an exemption to be appropriate in the circumstances.

Relying Party - Plans and procedures

The Plans and procedure declarations for relying parties applying to participate in the AGDIS from to be downloaded from the Digital ID System website and must be attached with your application.

All entities – Declarations and submitting

The Declaration for compliance for all entities seeking approval to participate in the AGDIS and the Final Declaration for all entities seeking approval to participate in the AGDIS to be downloaded from the Digital ID System website and must be attached with your application.

I understand my organisation:

- is required to comply with all relevant Digital ID legislation

Please attach signed declaration. The Final Declaration for all entities seeking approval to participate in the AGDIS to be downloaded from the Digital ID System website and uploaded.