AUSTRALIAN COMPETITION & CONSUMER COMMISSION

Applying for approval

Guidance for organisations seeking to become approved in the Australian Government Digital ID System

Version 1
November 2024

Acknowledgment of country

The ACCC acknowledges the traditional owners and custodians of Country throughout Australia and recognises their continuing connection to the land, sea and community. We pay our respects to them and their cultures; and to their Elders past, present and future.

Australian Competition and Consumer Commission
Land of the Ngunnawal people
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

ACCC 11/24_24–79

www.accc.gov.au

Contents

1.	Introduction	1
2.	Regulation of Digital ID	4
3.	Before applying	6
4.	Regulator's assessment	8
5.	Conditions on AGDIS approval	9
6.	AGDIS application steps	11
7.	Applying to participate as an accredited entity	15
8.	Applying as a participating relying party	16
9.	Review of Regulator decisions	24
10.	Following approval to participate	26
11.	Compliance obligations	29

1. Introduction

1.1 Australia's Digital ID System

Australia's Digital ID System aims to provide consumers with a secure, convenient, voluntary and inclusive way to verify their identity online.

By using a digital ID, consumers can gain greater control over their personal information and reduce the number of copies of their identity documents out in the world.

This guidance focuses on Australia's Digital ID System, which has been designed to protect consumers' privacy and security. Reflecting this, there is a robust, independent regulatory framework built into the scheme.

Australia's Digital ID System is broadly made up of 2 interconnected initiatives:

- A voluntary accreditation scheme for Digital ID providers throughout the economy.
- The Australian Government Digital ID System (AGDIS).

1.2 Participants in the AGDIS

There are separate processes for becoming accredited and approved to participate in the AGDIS. Accredited providers that wish to participate in the AGDIS are required to submit a separate application for AGDIS approval.

There are 3 types of accredited entities that can participate in the AGDIS:

- **Identity service provider** – provides services that:
  - generate, manage, maintain or verify information relating to the identity of an individual
  - generate, bind, manage or distribute authenticators to an individual
  - bind, manage or distribute authenticators generated by an individual.
- **Attribute service provider** – provides services that verify and manage an attribute of an individual.
- **Identity exchange provider** – provides services that convey, manage and coordinate the flow of information between participants in the Digital ID System.

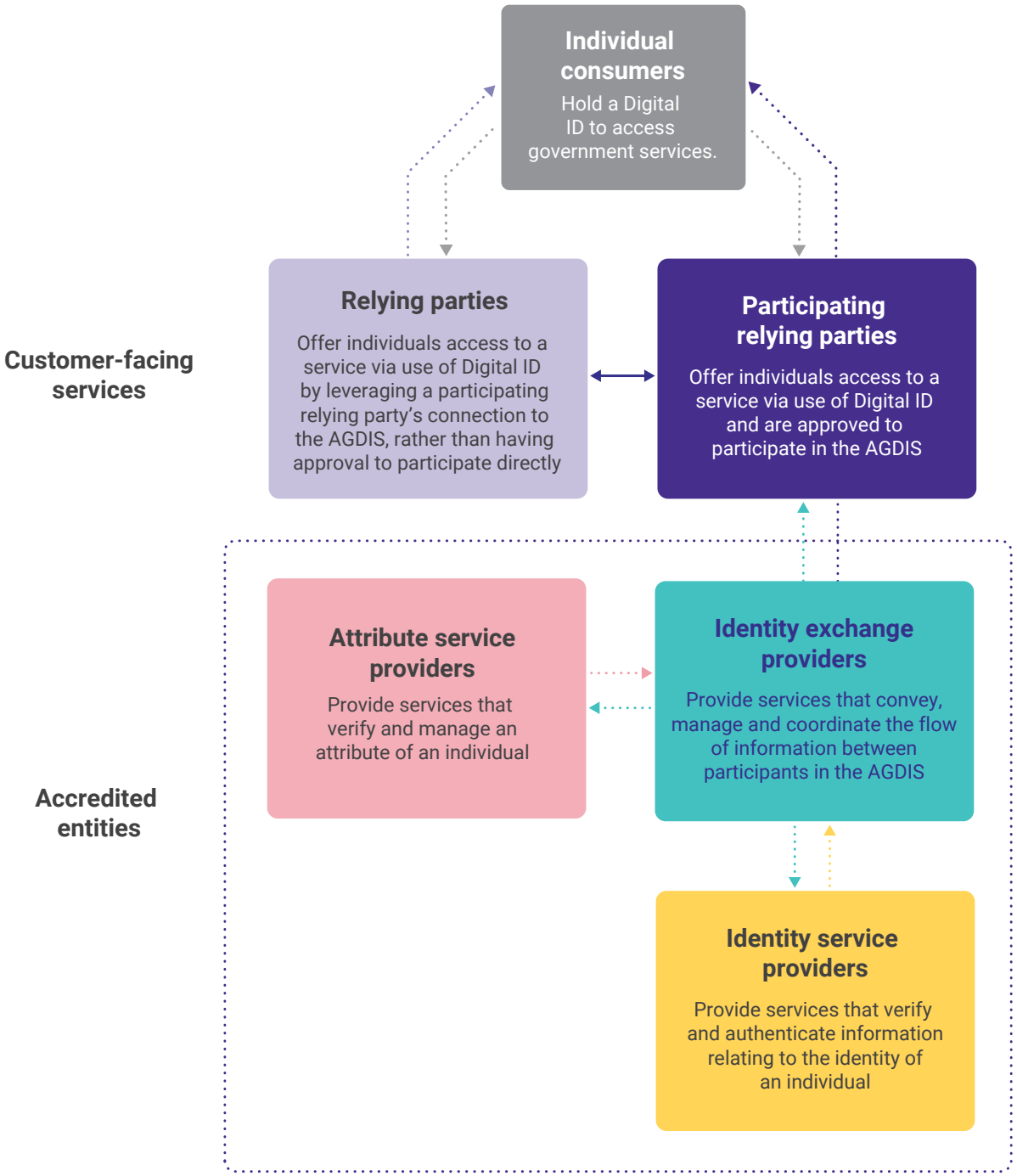
Identity service providers, attribute service providers and identity exchange providers cannot be approved to participate in the AGDIS unless they have first been accredited.

A "relying party" is an organisation that provides a service, or access to a service, to consumers by verifying the consumer's identity or attributes through an accredited entity. A relying party that wishes to participate in the AGDIS is required to apply for approval, but does not need to be accredited. Once a relying party has been approved to participate in the AGDIS and its participation start date has passed, it is known as a "participating relying party".

Eligibility to participate in the AGDIS is being phased. Currently, only government entities are eligible to apply to participate (see section 3.1).

Figure 1 represents the relationships between the parties in the AGDIS. The dotted lines indicate connections subject to the relevant Digital ID Data Standards (see section 2).

Figure 1: Australian Government Digital ID System (AGDIS)



1.3 This guidance

The purpose of this guidance is to assist organisations that are interested in applying for approval to participate in the AGDIS with lodging a valid application for approval.

The guidance also explains the legal framework governing Australia's Digital ID System, and how the Australian Competition and Consumer Commission (ACCC), in its role as the Digital ID Regulator, assesses applications for approval.

The ACCC may update this guidance periodically. Organisations should visit the Digital ID System website to ensure they are reading the latest version of this guidance. The website contains detailed information for applicants and approved entities, including the forms for applying for accreditation or approval to participate in the AGDIS, and an explanation of their purpose and use.

While this guidance provides general information to help organisations lodge a valid application for approval, it is not an exhaustive statement of all requirements for an application. Organisations should seek their own professional advice about the Digital ID legislation.

The ACCC's guidance does not replace the requirement for applicants and approved entities to have a full understanding of the Digital ID legislation (see section 2.1).The ACCC has prepared separate guidance to assist organisations applying for accreditation: see *Applying for accreditation: Guidance for organisations seeking to become accredited in Australia's Digital ID System*, available on the Digital ID System website.

Organisations should also ensure they are familiar with any guidance or other information prepared by the System Administrator, the Office of the Australian Information Commissioner (OAIC) and the Data Standards Chair.

1.4 Communicating with the Regulator

All organisations that wish to make an application for AGDIS approval must first email the ACCC at DigitalIDRegulator@accc.gov.au to receive details of the submission process for completed applications.

More information about the application process is detailed throughout this guidance.

The ACCC encourages organisations to engage with the System Administrator as early as possible to conduct testing. This can occur before an application is submitted to the ACCC. Organisations should complete the registration of interest form with the System Administrator, which is available on the Digital ID System website (see section 3.3).

Approved entities that need to submit an application (for example, to add or vary a condition) should email the ACCC at DigitalIDRegulator@accc.gov.au to receive details of the submission process.

2. Regulation of Digital ID

2.1 Legal framework

The legal framework governing Australia's Digital ID System is made up of the following 3 components:

	Name	Explanation
Acts – The acts are supported by the below rules and data standards	*Digital ID Act 2024 (the Act)*	This is the primary Act governing both the accreditation scheme and the AGDIS.
	Digital ID (Transitional and Consequential Provisions) Act 2024	This Act establishes the mechanism for how entities accredited or approved to participate in the AGDIS under the Trusted Digital Identity Framework transition into the new legislated framework.
Rules	*Digital ID Rules 2024 (the Digital ID Rules)* and corresponding Explanatory Statement	These rules set out the requirements for services participating in the AGDIS, and the obligations and conditions for using the Digital ID Accreditation Trustmark.
	Digital ID (Accreditation) Rules 2024 (the Accreditation Rules) and corresponding Explanatory Statement	These rules cover the requirements entities must meet to become and remain accredited, including to manage fraud, security, privacy, accessibility, and usability, and to undertake annual reviews.
	Digital ID (Transitional and Consequential Provisions) Rules 2024 (the Transitional Rules) and corresponding Explanatory Statement	These rules provide the transitional arrangements for entities that were accredited under the Trusted Digital Identity Framework and/or participating in the unlegislated AGDIS to transition to the legislated accreditation scheme and/or to participate in the legislated AGDIS.
Standards	*Digital ID (AGDIS) Data Standards 2024* and corresponding Explanatory Statement	These standards cover the technical requirements of the AGDIS.
	Digital ID (Accreditation) Data Standards 2024 (the Accreditation Data Standards) and corresponding Explanatory Statement	These standards cover the technical requirements of the accreditation scheme.

2.2 Agency roles

The ACCC, in its role as the Digital ID Regulator, is responsible for promoting compliance with the Act and other legislative instruments. This includes:

- accrediting entities that provide Digital ID services under the Digital ID legislation
- approving entities to participate in the AGDIS
- undertaking compliance monitoring and enforcement activities for non-privacy aspects of the Digital ID legislation.

References to "the Regulator" throughout this guidance refer to the ACCC in its role as the Digital ID Regulator.

The System Administrator is responsible for administering operational aspects of the AGDIS, including the security, integrity, and performance of the system. The System Administrator also manages applicant testing and onboards organisations that have been approved to participate in the AGDIS. Organisations wishing to participate in the AGDIS should register their interest in testing with the System Administrator via the Digital ID System website (see section 3.3).

The OAIC is the privacy regulator of Digital ID and is responsible for ensuring individuals' privacy is protected. Specifically, the OAIC's role includes:

- providing oversight of the new 'additional privacy safeguards' (that apply to all accredited entities in their provision of accredited services), including developing guidance, complaint-handling, conducting investigations and taking enforcement action
- performing Notifiable Data Breach scheme functions in relation to the Digital ID System
- undertaking assessments of Digital ID System compliance.

The Data Standards Body supports the Digital ID Data Standards Chair on the implementation and operation of data standards for Australia's Digital ID System.

2.3 About the ACCC

The ACCC is an independent Commonwealth statutory authority. As well as being the Digital ID Regulator, the ACCC administers and enforces the *Competition and Consumer Act 2010* (Cth) and other legislation to promote competition and fair trading in markets for the benefit of all Australians. The ACCC also regulates national infrastructure services.

More information about the ACCC's purpose, role and structure is available at About the ACCC.

Section 90 of the Act provides that the ACCC is the Digital ID Regulator.

3. Before applying

3.1 Eligibility to participate in the AGDIS

Participation in the AGDIS is being rolled out in phases.

The eligibility requirements to apply to participate in the AGDIS vary depending on whether the organisation is seeking to provide accredited services or to become a participating relying party.

Organisations seeking to provide accredited services in the AGDIS must be:

- a non-corporate Commonwealth entity, or
- a state or territory government department or authority, or
- a state or territory owned corporation.

Organisations seeking to be a participating relying party in the AGDIS must be:

- a Commonwealth entity (including corporate Commonwealth entities), or
- a state or territory department or authority, or
- a state or territory owned corporation.

After December 2026, private sector organisations will be able to apply to participate in the AGDIS as either relying parties or accredited entities.

See section 61 of the Digital ID Act for the specific eligibility requirements.

The Minister for Finance has the power to manage the expansion of the AGDIS. See the Digital ID (Phasing-in of Participation in the Australian Government Digital ID System) Determination 2024 that has been made by the Minister for Finance.

3.2 Voluntariness

While Australia has moved to a legislated Digital ID system, it remains voluntary for individuals to use a Digital ID to access government services through the AGDIS.

Digital ID does not replace traditional identification documents such as a birth certificate or driver's licence. Participating relying parties in the AGDIS must maintain alternative verification methods and must not require a user to create a Digital ID to access a service.

These alternative means must be reasonably accessible and not result in a service being provided on substantially less favourable terms.

The Act has limited exceptions to the voluntariness requirements. These include where an individual is accessing a service while acting on behalf of another organisation in a professional or business capacity.

The Regulator may, in very limited circumstances, grant an exemption to the voluntariness requirements to participating relying parties if it is satisfied it is appropriate. The Regulator will have

regard to whether the exemption would unduly undermine access to services of the kind for which the exemption is sought.

Exemptions to voluntariness will be assessed strictly on a case-by-case basis. See section 8.3 for the process for participating relying parties to seek an exemption from the voluntariness requirement.

3.3 Applying to test with the System Administrator

All organisations that wish to apply to participate in the AGDIS should complete a registration of interest form to undertake testing with the System Administrator. *The AGDIS registration of interest form* is available on the Digital ID System website.

Organisations can start testing before or after applying to the Regulator for approval to participate in the AGDIS; however, approval to participate will not be granted until testing is completed. Successful completion of testing does not mean an application for approval will be granted.

4. Regulator's assessment

4.1 Completeness check

For the Regulator to assess an application to participate in the AGDIS, the applicant must have submitted a completed *Application to participate in the AGDIS form* (see section 6.2), and associated documents.

4.2 Assessment

If an application is complete, it will proceed to the assessment stage. If the Regulator identifies any gaps or deficiencies during the completeness check, it will advise the applicant and identify the issues requiring rectification prior to re-submission.

To approve an application to participate in the AGDIS, the Regulator must be satisfied that:

- the applicant will comply with the relevant Digital ID Data Standards that apply both to the applicant and to participation in the AGDIS
- the applicant will comply with the Act and any requirements of the Digital ID Rules and Accreditation Rules, if applicable
- the applicant has effective plans and procedures as required by the Digital ID Rules
- it is appropriate to approve the applicant, which may include whether the applicant is a fit and proper person.

In undertaking its assessment, the Regulator may request further information or documentation if required.

The Regulator may also:

- engage with the applicant to seek clarification or ask for further information on an application
- consult or share information with other Australian Government authorities such as the OAIC, national security agencies, or similar authorities overseas
- consult with independent assessors on whether the applicant will be able to comply with the relevant legislative requirements.

4.3 Decision

The Regulator will notify the applicant in writing about its decision to grant or refuse approval to participate in the AGDIS.

If the Regulator decides to not grant approval, it will provide reasons for the decision and information about the applicant's rights to have the decision reviewed (see section 9 for further information about reviewable decisions).

5. Conditions on AGDIS approval

If granted approval, entities must comply with the relevant conditions on their approval. Failure to do so may result in suspension or revocation of an entity's approval.

For accredited entities, conditions applied to their accreditation will be automatically applied to any AGDIS approval, should it be granted. Additional conditions may be applied to AGDIS approvals. Conditions applying to an accredited entity's approval cannot be more permissive than the conditions the entity holds as an accredited service provider.

5.1 Conditions requested by an applicant

Applicants may apply for conditions to be imposed during the approval application process (see section 6.2). If approval is granted, entities may also apply for conditions to be imposed, varied or revoked. See section 10.3 for information about the application process for a condition to be imposed, varied or revoked.

Applicants should review the default conditions under the Act, Accreditation Rules, and Digital ID Rules before applying to the Regulator for a condition to be imposed.

Applicants applying for conditions to be imposed are required to provide details, justification and supporting evidence relevant to the condition(s) they are seeking. Supporting evidence might include plans and procedures for how an applicant will comply with the condition.

5.2 Default conditions

Default conditions are automatically applied by the Act, the Digital ID Rules, and the Accreditation Rules, depending on the kind of services being provided.

Default conditions include that AGDIS participants must comply with:

- all legislative requirements
- requirements in the Digital ID Rules relating to the use and display of the Digital ID Accreditation Trustmark
- requirements in the Accreditation Rules, including in relation to the collection and disclosure of restricted attributes and biometric information of individuals
- the requirement to begin to participate in the AGDIS on their participation start date.

See sections 16-19 of the Digital ID Act, Part 7.2 of the Accreditation Rules, and Chapter 3 Part 2 of the Digital ID Rules for information about conditions.

5.3 Conditions imposed by the Regulator or Minister

The Regulator will impose conditions to define the scope of approved services the entity can provide or provide access to.

Additional conditions can also be imposed by the Regulator at any time if it considers it appropriate in the circumstances, such as:

- whether the entity is authorised to collect or disclose a restricted attribute and/or biometric information
- to direct entities to engage in certain conduct or take certain action, including:
  - directing an entity to take certain actions before suspending or revoking its approval
  - directing an entity to maintain adequate insurance against any liabilities arising in connection with the obligations under the statutory contract between entities participating in the AGDIS.

The Regulator must impose conditions if directed to do so by the Minister for Finance for reasons of national security.

5.4 Services

The services an entity is approved to provide, or provide access to, will be listed as a condition of its approval. If an entity wishes to add, vary or no longer offer (revoke) a service, it will need to submit an application to impose, vary or revoke a condition. See section 10.3 for information about the application process for a condition to be imposed, varied or revoked.

6. AGDIS application steps

6.1 Registration

As part of making an application, an organisation should submit the following forms, available on the Digital ID system website:

- *Organisation and Authorised Officer form* – used by an organisation to provide the Regulator with information about:
  - the organisation that is applying to be approved
  - the Authorised Officer, which is a person who is authorised to act on behalf of the organisation
  - the primary contact person/s for the organisation.
- *Service and Contact Person form* – used by an organisation to provide the Regulator with information about:
  - a service seeking approval, or already approved, to participate in the AGDIS under the Act
  - the contact person/s for the service.

6.2 AGDIS Application Form

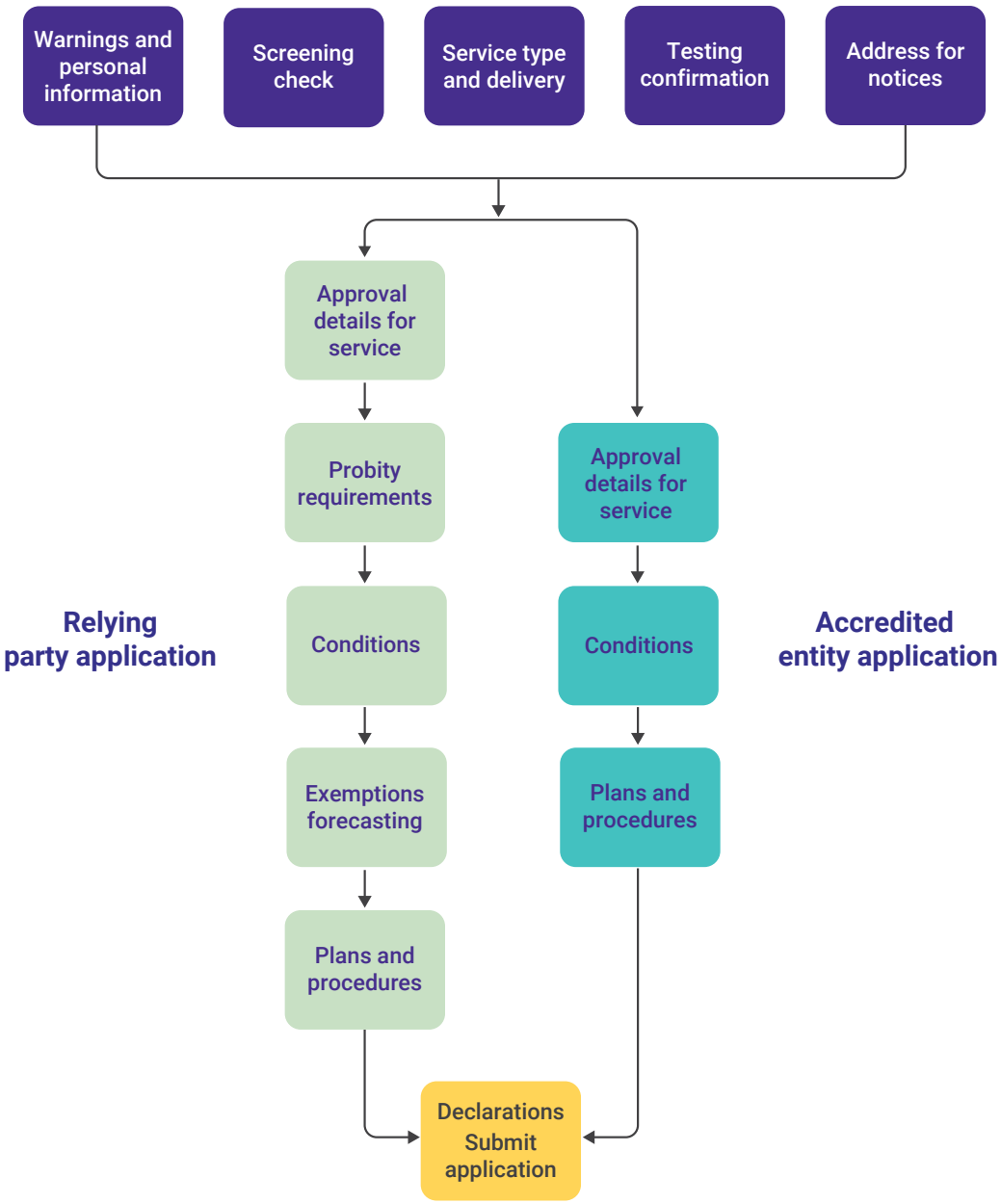
An organisation seeking to become approved to participate in the AGDIS is required to use the Regulator's *Application to Participate in the AGDIS form* (application form). This form is available on the Digital ID System website and must be submitted to the Regulator. All applicants should familiarise themselves with this form to support them in preparing the required application.

Where an organisation is applying to become approved to participate in the AGDIS for the first time, a separate application form will be required for each service requested. If approval is granted and the organisation wishes to add additional services, they must request this via the *Conditions on Accreditation and AGDIS Approvals form* (see section 10.3).

Completing an application

The AGDIS application process is represented in Figure 2. For the Regulator to assess an application to participate in the AGDIS, the applicant must have submitted the completed application form with all required documents.

Figure 2: AGDIS application process



6.3 Screening Check

All organisations applying for approval to participate in the AGDIS must complete a screening check as part of the application form.

The screening check is to ensure applicants have all required information and documents before applying. It is also designed to ensure applicants understand and agree to critical requirements before commencing their application, including:

- eligibility requirements
- the requirement to comply with all Digital ID legislation, including the Act, Digital ID Rules, Accreditation Rules, Digital ID Data Standards and the services for which they are seeking approval
- the requirement to commence participating in the AGDIS on the specified participation start date (see section 10.1)
- having in place all plans and written procedures for required matters.

6.4 Approval type and details

After the screening check, all applicants will need to select the service and the type of approval they are applying for. The participating entity types are:

- Attribute provider
- Exchange provider
- Identity provider
- Participating relying party.

Applicants can only add one service per application. However, applicants can submit separate applications if they are seeking approval to provide multiple services or become multiple provider types.

Service connections

Participating relying parties can offer services which connect directly to the AGDIS or via a 'broker' connection.

The broker connection enables multiple services to access the AGDIS using a single connection rather than requiring each service to connect directly to the AGDIS, regardless of who owns the service. The broker connection means relying parties can leverage their relationships with participating relying parties to verify individuals' attributes and Digital ID in the AGDIS, rather than seeking approval to participate individually.

Services accessing the AGDIS via a broker connection cannot collect or disclose restricted attributes. If an organisation wishes to seek a condition for a service to collect or disclose restricted attributes, that service will need to have a direct connection to the AGDIS.

To support visibility of these arrangements, applicants will be required to confirm:

- what service they are seeking to have approved
- who owns the service
- whether other organisations are responsible for the delivery of the service and, if so, who they are and what roles they hold
- whether the service they are applying for will access the AGDIS directly or via a broker connection. If an applicant intends to access the AGDIS via a broker, it will be required to detail which broker connection it intends to use.

Organisations are required to apply and have all services approved as a condition, regardless of whether the service connects directly to the AGDIS or via a broker connection. The broker is also required to be approved as a service.

It is important for applicants to understand that, if approved to participate in the AGDIS, they are responsible for providing contact information and responding to any events notified to them by the Regulator or the System Administrator regarding the provision of the service for which they are approved. This includes where the service has multiple organisations responsible for its delivery.

Applicants are also responsible for any compliance issues arising in relation to the approved service, even where the service has multiple organisations responsible for its delivery.

6.5 Application form

The *Application to Participate in the AGDIS form* has 2 separate work streams:

- Applying to participate as an accredited entity (see section 7).
- Applying to participate as a participating relying party (see section 8).

6.6 Declarations

Prior to finalising an application, all applicants will be required to:

- confirm they understand their legal obligations under the Act, Rules, and Data Standards, via the signed declaration form: *Declaration for compliance for all entities Seeking approval to participate in the AGDIS,* available on the Digital ID System website
- confirm that all information provided as part of the application is true and complete via the signed declaration form: *Final Declaration for all entities seeking approval to participate in the AGDIS,* available on the Digital ID System website.

Participating relying parties will also be required to declare their organisation has in place the required written procedures to notify the System Administrator, written cyber security plan, digital ID fraud management plan and written disaster recovery and business continuity plan via the signed declaration form: *Plans and procedure declarations for relying parties applying to participate in the AGDIS,* available on the Digital ID System website.

Accredited entities will also be required to declare their organisation has in place the required written procedures to notify the System Administrator via the signed declaration form: *Plans and procedures declaration for accredited entities seeking approval to participate in the AGDIS*, available on the Digital ID System website.

All declarations are to be submitted with the application.

7. Applying to participate as an accredited entity

7.1 Applying for conditions

As outlined in section 5, conditions already applied to an accredited entity will be automatically applied to any AGDIS approval, should it be granted. Applicants can request additional conditions to be applied to their approval to participate in the AGDIS. However, these conditions must not be more permissive than the conditions applying to their accreditation.

Should an accredited entity wish to request approval conditions that are more permissive than conditions originally granted for its accreditation, it must first apply to vary its accreditation conditions (see the Regulator's *Guidance for organisations seeking to become accredited in Australia's Digital ID System*, available on the Digital ID System website). For example, accredited entities cannot offer services in the AGDIS which are not captured in their accreditation conditions as that type of provider. This rule does not apply if an accredited entity is applying to participate in the AGDIS as a participating relying party.

If the application to vary accreditation conditions is granted, it will be applied to the accredited entity's AGDIS approval.

Where an accredited entity seeks to apply conditions specifically to its AGDIS approval, the following details will be required:

- the condition being sought
- justification for the condition to be imposed
- whether the condition should have a specific start and end date
- any relevant supporting evidence.

7.2 Plans and procedures

Accredited entities must declare they have written procedures for notifying the System Administrator in the event:

- their IT system that interacts with the AGDIS changes in a material way
- an IT system outage (planned or unplanned) occurs that could have a material effect on the operation of the AGDIS.

The Regulator may request further information and documents as part of its assessment of this requirement.

See Rule 3.2 of the Digital ID Rules for the requirements relating to notifying the System Administrator.

8. Applying as a participating relying party

8.1 Appropriateness to participate in the AGDIS

Before approving an application to participate in the AGDIS, the Regulator must be satisfied it is appropriate to approve the applicant in light of the objects of the Act, which include promoting privacy, the security of personal information, and trust in digital ID services amongst the Australian community.

In deciding whether it is appropriate to approve an applicant to participate in the AGDIS, the Regulator may have regard to whether the organisation is a fit and proper person and any other matters the Regulator considers relevant.

To assist this determination, applicants for approval must complete the *Evidence it is Appropriate to Accredit or Approve the Organisation form* (evidence of appropriateness form) and submit the form and associated documents with the application. The evidence of appropriateness form is available on the Digital ID System website.

The evidence of appropriateness form allows an organisation to demonstrate it is appropriate for the Regulator to approve them, by electing to either:

- provide evidence in line with the fit and proper person test as set out in Chapter 2 of the Digital ID Rules, or
- provide alternative evidence to satisfy the Regulator.

Further information on these options is set out in the sections below.

Fit and proper person test or alternative evidence

When deciding whether to approve an applicant, the Regulator may have regard to whether the applicant is a 'fit and proper person'. If the Regulator does consider whether an applicant is a fit and proper person, it must consider the fit and proper person test set out in the Digital ID Rules, which set out a number of mandatory matters (including but not limited to whether the applicant has been convicted of a serious criminal offence or has a history of insolvency or bankruptcy).

Due to the broad range of organisations that may seek approval, including government organisations and private entities, the criteria in the fit and proper person test may not be relevant to all applicants. For some applicants, there may be alternative evidence that is more pertinent to determining if it is appropriate to approve the organisation to participate in the AGDIS. For this reason, the Regulator has discretion about whether it is necessary to consider the fit and proper person test for all applications.

Whether an applicant will be able to satisfy the Regulator it is appropriate to approve the organisation without providing evidence in line with the fit and proper person test set out in the Digital ID Rules will depend on the particular circumstances.

The Regulator expects most applicants to provide evidence in line with the fit and proper person test. However, examples of circumstances where it may be appropriate for an applicant to provide alternative evidence to satisfy the Regulator include:

- The organisation has **previously been accredited or approved to participate in the AGDIS** under the Act – for example, if an organisation accredited as an identity service provider later seeks to also be accredited as an attribute service provider.

  In this scenario, the Regulator would have already assessed the appropriateness of the organisation to be accredited and the organisation will be subject to ongoing reporting obligations in relation to their fitness and propriety.

- The organisation is currently **accredited under the Consumer Data Right regime**.

  The fit and proper person test under the *Competition and Consumer (Consumer Data Right) Rules 2020 (*Cth) and the fit and proper person test in the Digital ID Rules are substantially similar. Organisations accredited under the Consumer Data Right regime also have ongoing reporting obligations in relation to fitness and propriety.

- The organisation is a **non-corporate Commonwealth entity** such as a department of state, a parliamentary department, or an entity prescribed by legislation.

  These entities are subject to a high level of oversight and accountability obligations, and their officials are subject to ongoing statutory duties which relate to fitness and propriety, such as under the *Public Governance, Performance and Accountability Act 2013* (Cth). Alternative evidence of the organisation's oversight and accountability frameworks, and compliance with their ongoing statutory duties, may be more pertinent to the Regulator's assessment of appropriateness than some of the mandatory matters set out in the Digital ID Rules.

- The organisation is **subject to other significant regulatory controls** relating to oversight and accountability, character obligations of employees, and privacy obligations, or is **subject to other similar fit and proper person tests**.

An organisation that falls within one or more of the above categories may still prefer to provide evidence in line with the fit and proper person test set out in the Digital ID Rules.

Whatever evidence the applicant provides, the Regulator will request further information and documents if required to be satisfied it is appropriate to approve the applicant, in line with the objects of the Act. If an applicant chooses to provide alternative evidence, the Regulator may request it provide evidence in line with the fit and proper person test in the Digital ID Rules if the Regulator is not satisfied it is appropriate to approve the applicant on the basis of the alternative evidence provided. This may extend the timeframes for assessment of the application for approval.

Evidence in line with the fit and proper person test

The information in this section is relevant to an applicant that has elected to provide evidence in line with the fit and proper person test set out in the Digital ID Rules.

Documents to be submitted with the application

- ☐ Completed *Evidence it is Appropriate to Accredit or Approve the Organisation form*.
- ☐ Current organisation chart reflecting all relevant associated persons and their relationships with the organisation.
- ☐ If the organisation is a body corporate – current corporate structure chart that identifies the organisation and its associates and associated entities (within the meaning of the *Corporations Act 2001* (Cth)).
- ☐ Associated persons declarations via *the Fit and Proper Declaration for Associated Persons form* – the organisation must provide a separate signed declaration from each associated person. The template declaration form is available on the Digital ID System website.

To the extent any of this information has been provided in response to other sections of the approval application form there is no need to provide the information again – instead an organisation can refer to the relevant document or response.

The Regulator will consider whether the organisation, and associated person/s (see section on associated persons below) of the organisation, has:

- within the previous 10 years, been convicted or found guilty of a serious criminal offence or an offence of dishonesty against any law of the Commonwealth or of a State or Territory, or a law of a foreign jurisdiction
- been found to have contravened a law relevant to the management of its DI data environment or a similar law of a foreign jurisdiction. Which laws are relevant will depend on the organisation's circumstances, including the type of organisation, the industry it operates in and the data it proposes to handle. Laws likely to be relevant include, but are not limited to:
  - the Act, Accreditation Rules and Digital ID Rules
  - *Privacy Act 1988* (Cth) and similar State or Territory laws
  - *Corporations Act 2001* (Cth)
  - *Corporations Regulations 2001* (Cth)
  - *Security of Critical Infrastructure Act 2018* (Cth)
- been the subject of a determination under sections 52(1)(b) or 52(1A)(a)-(d) of the *Privacy Act 1988* (Cth), which relates to an interference with the privacy of an individual, or a finding or determination of a similar nature under a similar law of a State or Territory or a foreign jurisdiction
- a history of insolvency or bankruptcy, and/or
- been the subject of a determination made under an external dispute resolution scheme that included a requirement to pay compensation and was, at the time the determination was made, recognised under section 35A of the *Privacy Act 1988* (Cth) or section 56DA of the *Competition and Consumer Act 2010* (Cth) (which sets out recognised external dispute resolution schemes for the purposes of the Consumer Data Right).

If the organisation is a body corporate, the Regulator will also consider whether any of the directors of the organisation, or of an associated person of the organisation, have been disqualified from managing corporations or been subject to a banning order.

The Regulator will also have regard to whether the organisation has previously had an application to be accredited or approved to participate in the AGDIS refused. If the organisation is or has been accredited or approved, the Regulator will consider whether that accreditation or approval has been suspended or revoked.

An organisation should disclose any other matters that may negatively impact the Regulator's assessment of whether the organisation is a fit and proper person. This could include details of any:

- investigation or disciplinary action by a professional body
- inquiry or investigation by a government agency
- court proceedings initiated by a government agency
- data breaches that have impacted the organisation and the organisation's response.

The Regulator may conduct searches and undertake relevant checks to verify the information and documents provided by the organisation. This may include criminal background checks of associated persons.

Associated persons

An applicant providing evidence in line with the fit and proper person test is required to provide the names of all associated persons and their relationship to the organisation as part of the evidence of appropriateness form. An applicant must also provide a separate signed declaration from each associated person addressing the criteria in the fit and proper person test: *Fit and Proper Person Declaration for Associated Persons form*. The template declaration form is available on the Digital ID System website.

Identifying associated persons

'Associated person' is defined in rule 1.4 of the Digital ID Rules. It is essential that an organisation carefully considers the definition of 'associated person' and identifies all their associated persons, even if there is a substantial number of them.

When determining who their associated persons are, an organisation should:

- consider which persons – within or outside their organisation – make, or participate in making, decisions that affect the performance of the organisation's functions when operating in the AGDIS, or have the capacity to significantly affect the performance of the organisation's functions when operating in the AGDIS. This may include:
  - office holders, for instance a director or company secretary
  - operations managers or data security managers
  - accountable executives, for instance a senior executive of the organisation responsible for the overall management of the organisation's functions when operating in the AGDIS
  - any other staff who have influence over the work that could significantly affect or influence the performance of the organisation's functions when operating in the AGDIS
  - any relevant contractors

- if the organisation is a body corporate – also refer to the definitions of associate and associated entity in the *Corporations Act 2001* (Cth). These definitions encompass a wide group of individual and corporate persons associated with the organisation, including persons who belong to overseas entities. For example, an associated entity can include related bodies corporate such as a holding company or a subsidiary and an associate can include a director or company secretary of either of those entities.

An organisation may wish to seek appropriate professional advice to assist with identifying their associated persons.

Alternative evidence of appropriateness

The information in this section is relevant to an applicant that has elected to provide alternative evidence to satisfy the Regulator it is appropriate to approve them.

Documents to be submitted with the application

- ☐ Completed *Evidence it is Appropriate to Accredit or Approve the Organisation form.*
- ☐ Any documents that detail or support the information provided in the evidence of appropriateness form.
- ☐ If the organisation is a body corporate – current corporate structure chart that identifies the organisation, its subsidiaries, and its related bodies corporate.
- ☐ Current organisation chart identifying any persons who have the capacity to significantly affect the performance of the organisation's functions when operating in the AGDIS.

To the extent any of this information has been provided in response to other sections of the approval application form there is no need to provide the information again – instead an organisation can refer to the relevant document or response.

The Regulator will consider whether the organisation, and any persons that have the capacity to significantly affect the performance of the organisation's functions when operating in the AGDIS, possess appropriate qualities such as *competence, character, diligence, honesty, integrity, and judgement.* The Regulator will also consider whether the organisation has sufficient processes or controls in place to ensure the organisation and its key relevant persons maintain and act in accordance with these qualities.

Types of alternative evidence

The types of evidence an applicant should provide, as well as the level of detail required, will depend on its individual circumstances.

Information likely to be relevant includes:

- Details of any **relevant legislative or regulatory controls** that apply to the organisation or its employees, particularly controls relating to oversight and accountability, character obligations of employees, and privacy obligations. For example, authorised deposit-taking institutions are regulated by the Australian Prudential Regulation Authority, Commonwealth companies and entities are subject to the *Public Governance, Performance and Accountability Act 2013* (Cth) and Australian Public Service employees are subject to the *Public Service Act 1999* (Cth).

- Details of any **similar fit and proper person tests** under other regulatory regimes the organisation or its employees have been subject to, e.g. most entities accredited under the Consumer Data Right regime will have been subject to a similar fit and proper person test during that accreditation process. The more similar the other fit and proper person test is to the mandatory matters set out in the Digital ID Rules, the more likely it is to be relevant.
- Details of **pre-employment checks** the organisation conducts, e.g. whether relevant staff and/or directors are subject to police and/or security checks.

For government organisations, relevant information may also include:

- details of the organisation's status, e.g. whether the organisation is a central government agency or department, or, if the organisation is a corporation, who controls it
- whether there is an accountable authority responsible for the organisation and, if so, what the obligations of this authority are
- whether the organisation is generally subject to government policy and directions
- whether the organisation is subject to Ministerial or other governmental control over its operations
- whether the organisation is subject to reporting obligations to the relevant government
- whether the organisation is subject to auditing obligations to the relevant government
- whether the organisation is otherwise subject to oversight over its operations
- whether the organisation is subject to public interest disclosure obligations.

Adverse information

An applicant should also disclose any other matters that may negatively impact the Regulator's assessment of whether it is appropriate to approve it. This could include details of any:

- investigation or disciplinary action by a professional body
- inquiry or investigation by a government agency
- court proceedings initiated by a government agency
- details of any data breaches that have impacted the organisation and the organisation's response.

The Regulator may conduct searches and undertake relevant checks to verify the information and documents provided by the applicant. This may include criminal background checks.

Ongoing reporting requirements

Approved entities are required to notify the Regulator within 5 business days of any matter that could be relevant to a decision as to whether they are a fit and proper person. Importantly, this reporting obligation applies even if the entity does not provide evidence in line with the fit and proper person test as part of its application for approval.

The Regulator may suspend or revoke an entity's approval if it is satisfied that it is not appropriate for the entity to be approved. In deciding this, the Regulator may have regard to the fit and proper person test.

8.2 Applying for conditions

Participating relying party applicants may apply for conditions to be imposed at either the organisation level or the service level.

Where a participating relying party applicant seeks to apply conditions, the following details will be required:

- the condition being sought
- justification for the condition to be imposed
- whether the condition should have a specific start and end date
- any relevant supporting evidence.

Restricted attribute collection

The Act includes strong safeguards regarding restricted attributes of individuals.

Participating relying parties can only collect and disclose restricted attributes if they are necessary for the service that a customer is accessing, and a condition of their approval authorises them to do so. Examples of restricted attributes include health information, information about a criminal record, or an identifier of an individual contained on a government issued document.

See section 11 of the Digital ID Act for the meaning, as well as examples, of restricted attribute of an individual.

The *Application to Participate in the AGDIS form* requires information from applicants seeking a condition authorising the collection or disclosure of restricted attributes, including what is sought to be collected and why, as well as the potential harm of disclosure and community expectations around handling this information. The Regulator will have regard to the information provided when deciding whether to impose the condition.

As outlined above, if an organisation is seeking a condition to collect or disclose restricted attributes for a service, that service must connect to the AGDIS directly (not via a broker connection).

8.3 Exemptions forecasting (voluntariness)

Applicants are not eligible to apply for voluntariness exemptions until they become a participating relying party (i.e. after they are participating in the AGDIS). However, the *Application to Participate in the AGDIS form* seeks preliminary information as to whether a participating relying party applicant intends to seek an exemption from the voluntariness requirement for a service.

If the applicant is approved to become a participating relying party, it will then need to apply separately for exemption from the voluntariness requirement. The Regulator may grant this in very limited circumstances (see section 3.2).

The application for exemption is to be made via the *AGDIS exemptions for Participating Relying Parties form*, available on the Digital ID System website, and submitted to the Regulator.

The decision to refuse or grant an exemption will be provided to the applicant in writing. If the exemption is granted, it may be revoked by the Regulator if it considers it appropriate to do so.

See section 74 of the Digital ID Act for the requirements relating to exemptions.

8.4 Plans and procedures

Participating relying party applicants must have written procedures for notifying the System Administrator in the event:

- their IT system that interacts with the AGDIS changes in a material way
- an IT system outage (planned or unplanned) occurs that could have a material effect on the operation of the AGDIS.

See Rule 3.2 of the Digital ID Rules for the requirements relating to notifying the System Administrator.

Participating relying party applicants must have:

- conducted risk assessments to identify, evaluate and manage the risk of a cyber security incident and a digital ID fraud incident occurring in connection with a service that the organisation intends to provide, or provide access to, within the AGDIS

See Rule 3.3(1) of the Digital ID Rules for the requirements relating to risk assessments.

- written plans that address:
  - cyber security
  - fraud management
  - disaster recovery and business continuity.

These plans must have been approved by the organisation's governing body and address the requirements in the Digital ID Rules.

The Regulator may request further information and documents as part of its assessment of this requirement.

See Rule 3.3(2)(a-c) of the Digital ID Rules for the requirements relating to plans.

9. Review of Regulator decisions

Certain decisions of the Regulator are reviewable. This includes a decision to approve, or not approve, an entity to participate in the AGDIS. Some reviewable decisions are eligible for internal review by the Regulator, while others are only eligible for external review by the Administrative Review Tribunal or Federal Court.

See Chapter 9, Part 4 of the Digital ID Act for information about reviewable decisions

When the Regulator (the decision maker) advises an applicant of the outcome of a decision, the Regulator's correspondence to the applicant will include information on whether the decision by the Regulator is eligible for internal review or review by the Administrative Review Tribunal.

9.1 Internal review

A reviewable decision will be eligible for internal review if it is made by a delegate of the decision maker.

Information provided on whether the decision made by the Regulator is eligible for an internal review will include contact information for submitting a request for internal review. An application for internal review must be in writing and be made within 28 days after the day the decision first came to the notice of the applicant. A request for review of a decision made by the Regulator must be made by the affected entity.

The Regulator is required to make an internal review decision to either uphold, vary or revoke the original decision within 90 days of receipt of the request for review.

The applicant will be notified by the Regulator of the outcome of the internal review. If the Regulator's decision is to revoke the decision under review, the Regulator may make any other decision considered appropriate. The Regulator will provide the applicant with a written statement of its reasons for its decision.

9.2 Review by the Administrative Review Tribunal

A reviewable decision will be eligible for external review by the Administrative Review Tribunal if the decision was made by the decision-maker personally, or if the decision is an internal review decision of the reviewable decision made by the Regulator.

The Regulator will advise the applicant if the decision is eligible for external review by the Administrative Review Tribunal. An application to the Administrative Review Tribunal for review of a reviewable decision made by the Regulator must be made by the entity affected by the reviewable decision.

Information on applying to the Tribunal for a review of a decision is available on the Administrative Review Tribunal website.

9.3 Judicial review

Applicants or approved entities may apply to the Federal Court for judicial review of certain decisions made by the Regulator. Judicial review is concerned only with the legality of the decision and is limited to questions of law, such as:

- Whether the Regulator had the power to make the decision.
- Whether the decision-maker took an irrelevant consideration into account or failed to take a relevant consideration into account.
- Whether the decision was so unreasonable that no reasonable decision-maker could have made it.

Applicants may appeal to the Federal Court for judicial review of any decision of the Administrative Review Tribunal. Again, the Federal Court can rule only on questions of law, not on the merits of the decision.

Information on the process to apply to the Federal Court for judicial review of a decision is on the Federal Court of Australia website.

10. Following approval to participate

10.1 Participation start date

If an organisation's application to participate in the AGDIS is granted, it will be notified by the Regulator of the approval date and a participation start date. The organisation must begin participating in the AGDIS on its participation start date. Failure to commence participation on the organisation's participation start date will be non-compliance and may result in enforcement action.

The Regulator will coordinate the participation start date with the approved entity, the System Administrator and other entities already participating in the ADGIS.

If an approved entity is unable to start participating on its participation start date or becomes aware of issues which may impact its start date, it must notify the Regulator as soon as possible by submitting the *Application to vary participation start date for AGDIS approval,* available on the Digital ID System website.

10.2 AGDIS Register

All entities approved to participate in the AGDIS will be added to the AGDIS Register. The AGDIS Register is a public register available on the Digital ID System website and the ACCC website.

The AGDIS Register will be updated to reflect any changes to an entity's approval or conditions, as well as organisation names, service names, and any suspensions or revocations of approval. If an entity's approval to participate in the AGDIS is revoked, the information will remain on the AGDIS Register for 3 years after the day on which the revocation came into force.

Section 121 of the Digital ID Act details what the AGDIS Register must contain for each organisation.

10.3 Changes to conditions on AGDIS approvals

The Regulator may, on its own initiative, take action to impose new conditions, as well as vary or revoke an existing condition on an entity's approval, if it considers it appropriate to do so. The Regulator may also be directed by the Minister of Finance to impose new conditions on an entity's approval.

An entity can also apply to the Regulator to have a condition imposed on its approval, or to have an existing condition varied or revoked, by submitting the *Conditions on Accreditation and AGDIS Approval form,* available on the Digital ID System website, and accompanying evidence.

Approved entities applying for conditions to be imposed, varied, or revoked are required to provide details and justification for the condition(s) they are seeking, as well as supporting evidence for each condition. Supporting evidence might include plans and procedures for how the organisation will comply with the condition, as well as updates to existing plans and procedures that require changes as a result of the condition sought.

10.4 Varying an approval

The Regulator may vary an entity's approval to reflect a change in the approved entity's name.

Applications for approval to be varied to reflect a change to the approved entity's name can be submitted to the Regulator via the *Application to Vary Accreditation or AGDIS Approval form*, available on the Digital ID System website. The form requires information about the approved entity's new name and any relevant dates.

The AGDIS Register will be updated following a decision by the Regulator to vary the approved entity's name.

10.5 Suspending and revoking an approval

An entity's approval can be suspended or revoked in 3 instances:

- by direction of the Minister for Finance
- on the Regulator's initiative
- by application from the entity.

The Minister can direct the Regulator to suspend or revoke an approval

The Regulator must suspend or revoke an entity's approval if the Minister for Finance directs it to do so for reasons of security (within the meaning of the *Australian Security Intelligence Act 1979*), including because of an adverse or qualified security assessment in respect of a person.

The Regulator may suspend or revoke an approval

The Regulator may, on its own initiative, suspend or revoke an entity's approval in some circumstances, including where the Regulator reasonably believes:

- the entity has contravened or is contravening the Act
- there has been a cyber security incident involving the entity that involves a risk to the operation of the ADGIS, or
- it is not appropriate for the entity to be approved, for example by reference to the fit and proper person requirements in the Digital ID Rules.

An entity can apply to suspend or revoke its approval

An entity may apply to the Regulator to have its approval suspended or revoked. The application must be submitted via the *Suspension of Accreditation or AGDIS Approval form* or the *Revocation of Accreditation or AGDIS Approval form,* available on the Digital ID system website.

The application requires information about the service that is to be suspended or revoked, the reason for the request, and any relevant dates.

The Regulator has discretion to approve or reject an entity's application to suspend its AGDIS approval. However, if a revocation of an entity's approval is sought, the Regulator must accept that application, but the Regulator can determine the date that the revocation takes effect.

Once the Regulator has suspended the entity's approval, the suspension remains in force until the entity requests that it be revoked. The AGDIS Register will be updated to reflect any decisions to suspend or revoke an entity's accreditation.

11. Compliance obligations

Approved entities participating in the AGDIS have continuing compliance, disclosure and reporting obligations under the Digital ID legislation.

These obligations include:

- complying with the conditions that apply to the approved entity, including:
  - participating only as the kind of entity it has been accredited and approved to participate as
  - notifying the Regulator before adding new digital ID services or removing services (see section 11.3)
  - collecting and storing pairwise identifiers, where required
  - ensuring that the entity's approved services are secure, easy to use, voluntary, accessible, inclusive and reliable
- complying with restrictions on collection of restricted attributes of individuals (relevant to participating relying parties)
- notifying the Regulator or System Administrator of reportable incidents
- maintaining comprehensive records as required by the Act.

In addition, an entity must ensure that any representation it makes concerning its accreditation or approval status under the Act is accurate, and not misleading or deceptive.

An accredited entity, including one that is participating in the AGDIS, may only use the Digital ID Accreditation Trustmark in accordance with the requirements prescribed in the Act and Digital ID Rules. Such an organisation must also ensure that its use of the Digital ID Accreditation Trustmark complies with the Australian Consumer Law.

Failure to meet compliance obligations may result in **enforcement action** by the Regulator, including litigation seeking **injunctions** and/or substantial **civil pecuniary penalties in appropriate cases**.

This guidance contains a summary of some of the key obligations of approved entities, including:

- record keeping obligations
- reportable incident obligations.

This guidance contains general information about the obligations of approved entities. It is not legal advice and is not a comprehensive or exhaustive statement of all obligations approved entities must comply with. Organisations should seek their own professional advice about the Digital ID legislation.

11.1 Record keeping obligations

Approved entities must comply with the obligations prescribed in the Digital ID Rules that require prescribed records to be kept for at least 3 years or as otherwise prescribed.

In addition, approved entities must comply with destruction or de-identifying of personal information in their possession or control that was obtained though the AGDIS. Non-compliance with these obligations is enforced by the OAIC.

These obligations are civil penalty provisions under the Act with substantial pecuniary penalties.

See sections 135 and 136 of the Digital ID Act and Chapter 6 of the Digital ID Rules for the record keeping obligations.

11.2 Reportable incident obligations

Approved entities have obligations to report certain incidents that have occurred, or are reasonably suspected to have occurred, in connection with the AGDIS.

Some of these reporting requirements involve notifying the Regulator, while others require notifications to be made to the System Administrator. The following are examples of notification requirements for reportable incidents that approved entities must comply with:

	Notifications and reportable incidents
Notifications to the System Administrator	▪ Cyber security incidents. ▪ Digital ID fraud incidents. ▪ Proposed changes to information technology systems that interact with the AGDIS if the change could reasonably be expected to have a material effect on the operation of the AGDIS. ▪ Any planned or unplanned outage or downtime affecting the entity's IT system that could reasonably be expected to have a material effect on the AGDIS.
Notifications to the Regulator	▪ Any material changes in the organisation's circumstances that may affect its ability to comply with its obligations under the Digital ID legal framework. ▪ Any matters that could reasonably be considered relevant to a decision as to whether the organisation, or an associated person of the organisation, is a fit and proper person for the purposes of the Digital ID legal framework. ▪ Any material changes to, or error in, any of the information provided to the Regulator. An accredited entity participating in the AGDIS must also notify the Regulator if it proposes to use an IT system that it uses to provide services within the AGDIS to provide or receive services within a digital ID system other than the AGDIS. A participating relying party also needs to comply with a condition imposed by the rules to notify the Regulator of proposed changes to its contact details.

Failure to comply with certain notification requirements may result in enforcement action, including substantial civil pecuniary penalties.

These reporting obligations also apply to a participating entity whose approval is suspended in respect of reportable incidents that occurred or are reasonably suspected to have occurred while the entity was participating in the AGDIS.

See Chapter 4 of the Digital ID Rules for the reportable incidents and notification requirements.


AUSTRALIA


ACCC
AUSTRALIAN COMPETITION
& CONSUMER COMMISSION