



Guidance for entities approved to participate in the Australian Government Digital ID System

Version 1

June 2025

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
© Commonwealth of Australia 2025

This work is copyright. In addition to any use permitted under the *Copyright Act 1968*, all material contained within this work is provided under a Creative Commons Attribution 4.0 Australia licence, with the exception of:

- the Commonwealth Coat of Arms
- the ACCC and AER logos
- any illustration, diagram, photograph or graphic over which the Australian Competition and Consumer Commission does not hold copyright, but which may be part of or contained within this publication.

The details of the relevant licence conditions are available on the Creative Commons website, as is the full legal code for the CC BY 4.0 AU licence.

Requests and inquiries concerning reproduction and rights should be addressed to the General Manager, Strategic Communications, ACCC, GPO Box 3131, Canberra ACT 2601.

Important notice

The information in this publication is for general guidance only. It does not constitute legal or other professional advice, and should not be relied on as a statement of the law in any jurisdiction. Because it is intended only as a general guide, it may contain generalisations. You should obtain professional advice if you have any specific concern.

The ACCC has made every reasonable effort to provide current and accurate information, but it does not make any guarantees regarding the accuracy, currency or completeness of that information.

Parties who wish to re-publish or otherwise use the information in this publication must check this information for currency and accuracy prior to publication. This should be done prior to each publication edition, as ACCC guidance and relevant transitional legislation frequently change. Any queries parties have should be addressed to the General Manager, Strategic Communications, ACCC, GPO Box 3131, Canberra ACT 2601.

ACCC 06/25_25-27

www.accc.gov.au

Contents

1.	Introduction	1
1.1	Guidance terminology	1
2.	Regulation of Digital ID	3
2.1	Legal framework	3
2.2	Agency roles	4
2.3	About the ACCC	5
3.	Communicating with the Regulator	6
3.1	Submitting forms and supporting evidence	6
4.	Responsibilities of approved entities	7
4.1	Compliance with conditions	7
4.2	Voluntariness	8
4.3	Restricted attributes	9
4.4	Notifying reportable incidents	10
4.5	Record keeping	15
4.6	Data standards	15
4.7	Privacy obligations	15
5.	Changes to AGDIS approval	16
5.1	Entity initiated changes	16
5.2	Regulator initiated changes	18
6.	Compliance and enforcement approach	20
6.1	Compliance monitoring tools	20
6.2	Enforcement action	22
7.	Review of Regulator decisions	24
	Appendix A – Exemption application assessment factors	26

1. Introduction

The purpose of this guidance is to assist entities that have been approved to participate in the Australian Government Digital ID System (AGDIS) in understanding their ongoing obligations under the Digital ID legislation and the processes for applying for, or notifying the Australian Competition and Consumer Commission (ACCC) of, changes to their AGDIS approval.

The guidance also explains the ACCC's approach to promoting compliance with the Digital ID legislation and its powers as the Digital ID Regulator.

The ACCC may update this guidance periodically and entities should visit the [Digital ID System website](#) to ensure they are reading the latest version.

Organisations that are interested in applying for approval to participate in the AGDIS should refer to the *Applying for approval – Guidance for organisations seeking to become approved in the Australian Government Digital ID System* document available on the [Digital ID System website](#).

The ACCC's guidance does not replace the requirement for applicants and approved entities to have a full understanding of the Digital ID legislation. Entities should seek their own professional advice about the Digital ID legislation. Organisations should also ensure that they are familiar with any guidance or other information concerning the Digital ID legislation prepared by the Office of the System Administrator (System Administrator), the Office of the Australian Information Commissioner (OAIC) and the Digital ID Data Standards Chair.

1.1 Guidance terminology

When this guidance refers to **approved entities**, it is describing both accredited entities approved to participate in the AGDIS and participating relying parties.

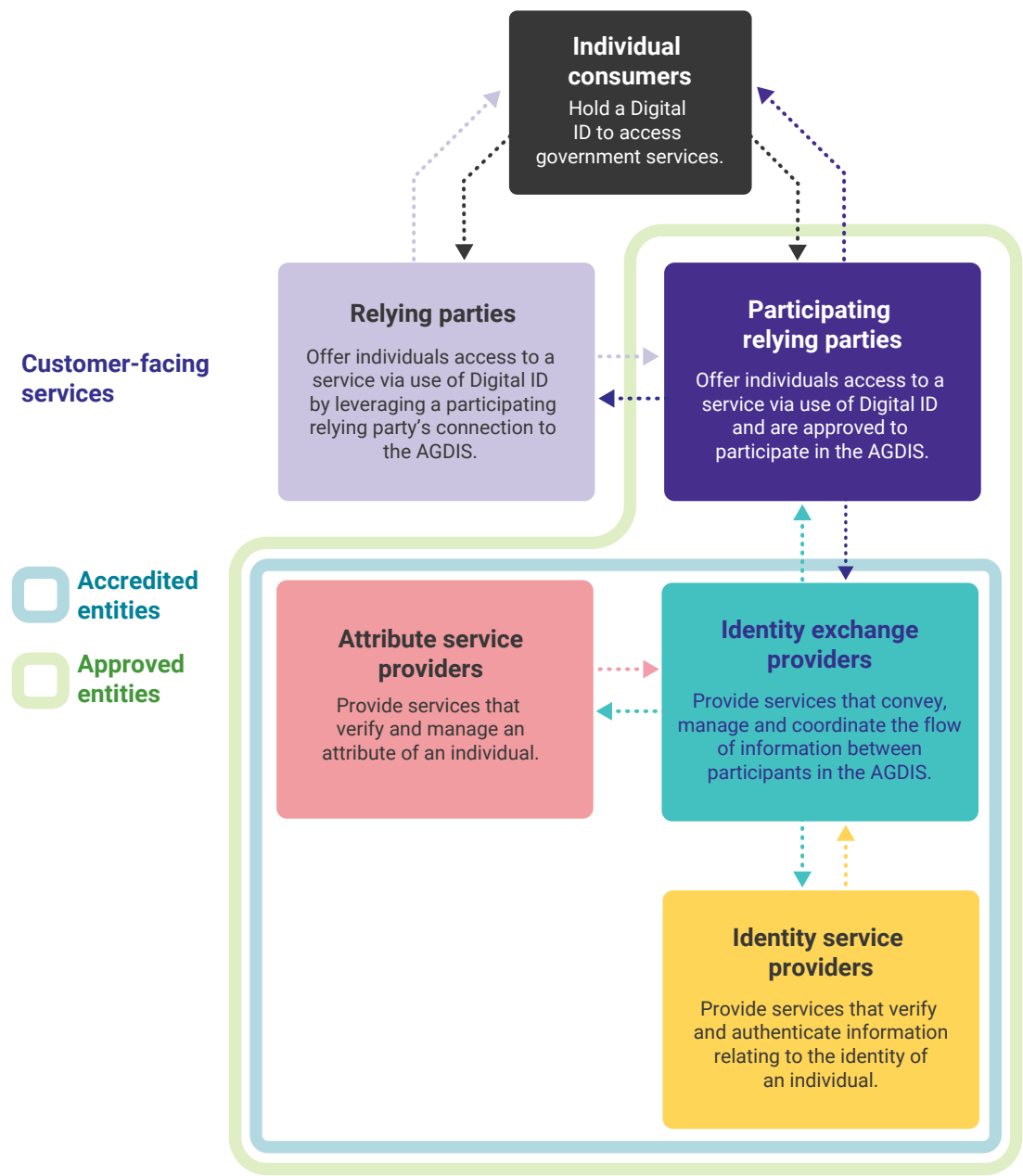
Most of the obligations discussed in this guidance apply to all approved entities. Some of the obligations discussed in this guidance apply specifically to:

- accredited entities (and not participating relying parties)
- participating relying parties (and not accredited entities)
- approved entities whose participation start day has not yet passed, and/or
- entities who have had their approval to participate in the AGDIS suspended or revoked.

The guidance specifically states where this is the case.

Figure 1 represents the relationships between the parties in the AGDIS. The dotted lines represent the data flow between these parties.

Figure 1: The Australian Government Digital ID System



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 – the Act, the Rules and the data standards, collectively referred to as the Digital ID legislation.

Organisations are responsible for ensuring they familiarise themselves with and understand their obligations under the Digital ID legislation.

The Digital ID legislation (including Explanatory Statements) is available on the [Federal Register of Legislation](#).

	Name	Explanation
Acts – The acts are supported by the below rules and data standards	<i>Digital ID Act 2024 (the Act)</i>	This is the primary act governing both the accreditation scheme and the AGDIS.
	<i>Digital ID (Transitional and Consequential Provisions) Act 2024</i>	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	<i>Digital ID Rules 2024 (the Digital ID Rules)</i>	These rules set out the requirements for services participating in the AGDIS, and the obligations and conditions for using the Digital ID Accreditation Trustmark.
	<i>Digital ID (Accreditation) Rules 2024 (the Accreditation Rules)</i>	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.
	<i>Digital ID (Transitional and Consequential Provisions) Rules 2024 (the Transitional Rules)</i>	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	<i>Digital ID (AGDIS) Data Standards 2024</i>	These standards cover the technical integration and design requirements for entities to participate in the AGDIS.
	<i>Digital ID (Accreditation) Data Standards 2024 (the Accreditation Data Standards)</i>	These standards cover the technical requirements of the accreditation scheme relating to biometric testing and the use of authentication technologies.

2.2 Agency roles

ACCC

The ACCC, in its role as the Digital ID Regulator, is responsible for promoting compliance with the Digital ID legislation. This includes:

- accrediting entities that provide digital ID services under the Digital ID legislation
- approving entities to participate in the AGDIS
- undertaking compliance and enforcement activities.

References to ‘the Regulator’ throughout this guidance mean the ACCC in its role as the Digital ID Regulator.

OAIC

The OAIC is the privacy regulator of the Digital ID system 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 in respect of the privacy aspects of the Act
- performing Notifiable Data Breach scheme functions in relation to the Digital ID System
- undertaking assessments of the handling and maintenance of personal information in accordance with the Act.

The privacy obligations in the Digital ID legislation operate in addition to existing privacy obligations under either the Privacy Act 1988 or relevant state or territory privacy legislation.

Office of the System Administrator

The Office of the System Administrator (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.

More information about the System Administrator’s role in the AGDIS is in *Applying for approval: guidance for organisations seeking to become approved in the Australian Government Digital ID System*, available on the [Digital ID System website](#).

Digital ID Data Standards Chair

The Digital ID Data Standards Chair makes Digital ID Data Standards for various matters, including technical integration and design requirements for organisations to participate in the AGDIS, and other technical requirements associated with the accreditation scheme. The Data Standards Body supports the Digital ID Data Standards Chair in the delivery of its functions and powers.

2.3 About the ACCC

The ACCC is an independent Commonwealth statutory authority. As well as being the 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. Communicating with the Regulator

Approved entities and applicants can contact the Regulator via email at DigitalIDRegulator@accc.gov.au.

Where this guidance lists requirements to provide information to or contact the Regulator, this is to be done via the above email address.

3.1 Submitting forms and supporting evidence

This guidance sets out the names of forms associated with certain requests, which are available on the [Digital ID System website](#). Importantly, all forms must be submitted by a person who is authorised to act on behalf of the entity.

Where there are forms or supporting evidence associated with requests or notifications to the Regulator, these documents should be provided via a secure link provided by the Regulator.

Entities that received a secure link during the application stage can continue to use that link. Entities that do not have a link or require it to be re-sent, can email the Regulator via the above email address to request a link.

4. Responsibilities of approved entities

It is the responsibility of each approved entity to be aware of and comply with its legal obligations under the Digital ID legislation, including the Act and all rules and standards.

This chapter summarises some of the key obligations of approved entities; however, it is not a comprehensive or exhaustive list and approved entities should seek their own legal advice regarding their specific obligations.

These obligations include:

- complying with the conditions that apply to the approved entity
- complying with the voluntariness requirement (relevant to participating relying parties)
- complying with restrictions on collection of restricted attributes of individuals
- notifying the Regulator or the System Administrator of reportable incidents, including matters relevant to the fit and proper person assessment
- complying with record keeping and data standards requirements
- complying with privacy obligations under the Act and other relevant legislation.

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.

Failure to meet compliance obligations may result in enforcement action by the Regulator, including suspension or revocation of AGDIS approval and civil penalty proceedings seeking injunctions and/or substantial pecuniary penalties.

4.1 Compliance with conditions

Approved entities must comply with all conditions imposed on their approval.

Some conditions are imposed by default by the Act and the Digital ID Rules. For example, a default condition that applies broadly is simply that approved entities must comply with the Act (see section 64 of the Act).

Accredited entities

If the entity is an accredited entity, a default condition on its AGDIS approval is that it must participate in the AGDIS only as the kind of accredited entity it is accredited and approved to participate as and must provide only its accredited services in the AGDIS.

Another set of conditions that accredited entities participating in the AGDIS may need to comply with are those specified in rule 7.3 of the Accreditation Rules, which are common conditions imposing limitations on the collection and disclosure of restricted attributes and the biometric information of individuals. The application of these conditions will vary depending on the kind of accredited services being provided and an entity's circumstances.

Participating relying parties

If the entity is a participating relying party, default conditions on its AGDIS approval require it to:

- notify the Regulator of a proposed change to its contact details within 7 days
- notify the System Administrator of any changes to IT systems or planned or unplanned outage or downtime affecting the entity's IT systems as set out in item 2 of rule 3.4 of the Digital ID Rules
- collect and store pairwise identifiers as specified in item 3 of rule 3.4 of the Digital ID Rules.

Conditions imposed on approval

Approved entities are also required to comply with any conditions that are imposed by the Regulator either at the time of approval or subsequently.

Failure to comply with a condition may result in the suspension or revocation of an entity's AGDIS approval.

Conditions can be imposed, varied or revoked at any time. This may occur following a request by an approved entity (see section 5.1) or by the Regulator acting on its own initiative or as directed by the Minister for Finance (see section 5.2).

See sections 16–19 and 64 (1) of the Digital ID Act, Part 7.2 of the Accreditation Rules, and Chapter 3 Part 2 of the Digital ID Rules for further details on default conditions.

4.2 Voluntariness

Subject to the limited circumstances discussed below, the creation or use of a digital ID to access a service through the AGDIS must be voluntary (the voluntariness obligation).

To comply with the voluntariness obligation, participating relying parties must:

- provide consumers with an alternative means of accessing the service; or
 - the alternative means of accessing the service must be reasonably accessible and not result in the service being provided on substantially less favourable terms
 - acceptable alternative means of accessing a service will depend on the relevant circumstances, including the type of service and the nature and characteristics of the potential users of the service. Alternatives could include the option to access the service through email, online (for example, via a secure link or username and password), or a physical location reasonably accessible to all potential users
- meet an exception to the voluntariness obligation; or
 - the Act has limited exceptions to the voluntariness obligation. These include where an individual is accessing a service while acting on behalf of another entity in a professional or business capacity
- hold an exemption to the voluntariness obligation granted by the Regulator.

Failure to comply with the voluntariness requirement is non-compliance with the Act and may lead to enforcement action.

Eligibility for voluntariness exemption

An eligible participating relying party may apply for an exemption from the voluntariness requirement.

The Regulator must not grant an exemption to a participating relying party that is:

- a Commonwealth entity, or a Commonwealth company, within the meaning of the *Public Governance, Performance and Accountability Act 2013*
- a person or body that is an agency within the meaning of the *Freedom of Information Act 1982*, or
- a body specified, or the person holding an office specified, in Part I of Schedule 2 to the *Freedom of Information Act 1982*.

Applying for a voluntariness exemption

The Regulator may grant an exemption if it is satisfied that it is appropriate to do so.

The Regulator's assessment will be guided by the requirements and objects of the Act, which include to provide individuals with secure, convenient, voluntary and inclusive ways to verify their ID in online transactions. **Given this objective, the Regulator will generally only grant exemptions to the voluntariness obligation in exceptional circumstances.**

The application form for an exemption to the voluntariness obligation contains broad questions. Applicants are encouraged to provide fulsome and accurate information, with reference to the assessment factors, to enable the Regulator to efficiently assess their application. If the applicant provides minimal or inaccurate information, the exemption is less likely to be granted.

The assessment factors presented in Appendix A provide an indication of the range of factors that the Regulator may have regard to when considering an exemption from the voluntariness requirement. The list is not exhaustive, and the Regulator will consider each application on its merits, taking into account any matters relevant to a particular case.

Participating relying parties can apply for an exemption by completing and submitting the *AGDIS exemptions for participating relying parties form*, available on the [Digital ID System website](#).

Applicants will be given written notice of a decision to grant or to refuse to grant an exemption. If an exemption is granted, the Regulator may subsequently revoke it if it considers it appropriate to do so.

See section 74 of the Digital ID Act for further details on voluntariness.

4.3 Restricted attributes

The Regulator may impose a condition on an entity's approval to participate in the AGDIS that authorises the entity to collect or disclose restricted attributes of an individual (restricted attributes condition).

An entity can submit a request for a restricted attributes condition to be imposed at the time it applies for approval to participate in the AGDIS, or at any time while it holds an approval to participate in the AGDIS.

As conditions applying to approved entities cannot be more permissive than the conditions the entity holds as an accredited service provider, an accredited entity must have a condition authorising the collection or disclosure of restricted attributes granted as part of their accreditation.

When the Regulator decides whether to impose a restricted attributes condition, it must have regard to the matters in section 65(2) of the Act. Entities applying for a restricted attributes condition should provide:

- justification as to why restricted attributes need be collected or disclosed, including:
 - reasons why an outcome cannot be achieved without collection or disclosure of restricted attributes
 - what alternatives have been explored
 - what the consequences are for individuals and the AGDIS, if restricted attributes are not collected or disclosed
- a risk assessment and privacy impact assessment relating to the collection or disclosure of restricted attributes
- details of the entity's protective security, privacy and fraud control arrangements.

It is important for entities applying for a restricted attributes condition to provide sufficient information to support an informed decision by the Regulator.

If a restricted attributes condition is imposed, the Regulator will publish a statement of reasons for granting the condition on the [AGDIS Register](#) (also available on the [Digital ID System website](#)).

See section 65 of the Act for further details on conditions relating to restricted attributes of individuals.

4.4 Notifying reportable incidents

Approved entities are required to report certain incidents that have occurred, or are reasonably suspected to have occurred, while participating in the AGDIS.

These requirements are in addition to any existing notifiable data breach obligations under the *Privacy Act 1988* or relevant state or territory legislation.

For accredited entities, the requirements are also in addition to any other notification obligations they are subject to under their accreditation.

Approved entities are required to have robust notification procedures in place to allow for notification of incidents to the Regulator or the System Administrator within required timeframes.

The Digital ID Rules specify the notification timeframes and the information that must be provided to the Regulator or System Administrator in relation to a reportable incident.

Failure to comply with the provisions related to reportable incidents may give rise to substantial civil pecuniary penalties.

Notifications to the System Administrator

Notifications of reportable incidents	Digital ID rule	Timing requirement
For approved entities (including an entity that has had its approval to participate in the AGDIS suspended or revoked):		As soon as practicable, or no later than 1 business day after the entity becomes aware.
<ul style="list-style-type: none"> Cyber security incidents within the AGDIS. 	4.2	
<ul style="list-style-type: none"> Digital ID fraud incidents within the AGDIS. 	4.2	
For accredited entities:		
<ul style="list-style-type: none"> Proposed changes to IT systems that interact with the AGDIS if the change could reasonably be expected to have a material effect on the operation of the AGDIS. 	4.3(3)(a)	Within 5 business days
<ul style="list-style-type: none"> 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 operation of the AGDIS. 	4.3(3)(b)	Within 5 business days
For participating relying parties:		
<ul style="list-style-type: none"> Proposed changes to IT systems that interact with the AGDIS if the change could reasonably be expected to have a material effect on the operation of the AGDIS. 	3.4(1)(2)(a)(i)	Within 5 business days
<ul style="list-style-type: none"> 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 operation of the AGDIS. 	3.4(1)(2)(a)(ii)	Within 5 business days

Approved entities need to be familiar with and comply with the System Administrator's *AGDIS System Administrator Operational Handbook* available on the [Digital ID System website](#). This document sets out, amongst other things, how to notify the System Administrator of a reportable incident.

Cyber security and digital ID fraud incidents

The Digital ID Rules impose notification obligations in relation to cyber security and digital ID fraud incidents. These obligations apply to:

- approved entities
- entities that have had their approval to participate suspended
- entities whose approval has been revoked (if the incident occurred, or is reasonably suspected to have occurred, while the entity was participating in the AGDIS).

If a cyber security or digital ID fraud incident occurs, or is reasonably suspected to have occurred, in relation to any service provided or received within the AGDIS, the entity must notify the System Administrator.

A **cyber security incident** means one or more acts, events, or circumstances that involve:

- unauthorised access to, modification of or interference with a system, service or network (or an unauthorised attempt to access, modify, or interfere with a system, service or network), or
- unauthorised impairment of the availability, reliability, security or operation of a system, service or network (or an unauthorised attempt to impair the availability, reliability, security or operation of a system, service or network).

A **digital ID fraud incident** means an act, event or circumstance that occurs in connection with a service that a participating relying party is approved to provide, or provide access to, within the AGDIS and results in the compromise or unreliability of:

- a digital ID of an individual
- an attribute of an individual
- an authenticator relating to an individual
- a representation relating to an attribute of an individual, or
- a representation relating to a digital ID of an individual.

A cyber security incident and a digital ID fraud incident are defined in section 9 of the Act.

An example of a digital ID fraud incident may be where a digital ID used within the AGDIS has been compromised, or where a digital ID is created in the AGDIS that does not correspond to a real person. This could lead to major impacts for other parties within the AGDIS and the System Administrator needs to be notified.

Timing of notification

The notification must be made as soon as practicable after the incident, and in any event no later than one business day after the entity has been made aware of the incident or suspects an incident has occurred. The initial notification may be given orally. However, a written notification must be given within 3 business days after an oral notification.

Subrule 4.2(3) of the Digital ID Rules lists the information that must be included when notifying the System Administrator of a cyber security or digital ID fraud incident.

IT system changes and outages

The Digital ID Rules impose reporting obligations in relation to IT system changes and outages. These obligations apply to:

- accredited entities that are participating in the AGDIS
- accredited entities whose approval to participate in the AGDIS is suspended.

These entities must notify the System Administrator of the following incidents:

- Any proposed change to the entity's IT system that interacts with the AGDIS and may have a material effect on the operation of the AGDIS.
- Any planned or unplanned outage or downtime affecting the entity's IT system that may have a material effect on the operation of the AGDIS

A material effect includes any degradation or loss of functionality within the AGDIS, and any negative impact on other participants or users accessing the AGDIS.

The notification to the System Administrator must be made no later than 5 business days after the entity becomes aware that an incident has occurred, or reasonably suspects that the incident has occurred (whichever occurs first).

Subrule 3.4(2) and subrule 4.3(4) of the Digital ID Rules list the information that must be included when notifying the System Administrator of IT system changes and outages.

See also sections 4.20–4.22 of the Digital ID Rules Explanatory Statement for further details on reporting IT system changes and outages.

Notifications to the Regulator

Notifications of reportable incidents	Digital ID Rule	Timing requirement
All approved entities (including an entity that has had its approval to participate in the AGDIS suspended):		
■ Any material changes in the entity's circumstances that may affect its ability to comply with its obligations under the Digital ID legislation (see rule 4.3(2)(a) of the Digital ID Rules).	4.3(2)(a)	Within 5 business days
■ Any matter that could reasonably be considered relevant to whether the entity, or an associated person of the entity, is a fit and proper person for the purposes of the Digital ID legislation (see subrule 4.3(2)(b) of the Digital ID Rules).	4.3(2)(b)	Within 5 business days
■ Any material changes to, or error in, any of the information provided to the Regulator (see rule 4.3(2)(c) of the Digital ID Rules).	4.3(2)(c)	Within 5 business days
For participating relying parties:		
■ Proposed changes to the entity's contact details.	3.4(1)	Within 7 days
For accredited entities participating in the AGDIS:		
■ if the entity 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.	4.4(2)	Within 28 days

A 'material change' is one that significantly influences an entity's ability to comply with the Digital ID legislation or impacts the performance or quality of services within the AGDIS.

Notifying the Regulator

To notify the Regulator of a reportable incident, entities must email the Regulator. The email subject line should identify the type of reportable incident and specify that it is a mandatory notification.

To notify the Regulator of any proposed changes to its contact details, a participating relying party can complete and submit the *Service and Contact Person form*, available on the [Digital ID System website](#).

Subrule 4.3(4) of the Digital ID Rules lists the information that must be included when notifying the Regulator.

Fit and proper person

Approved entities, including those whose approval is suspended, are required to notify the Regulator within 5 business days of any matter that could be relevant to whether they, or an associated person, are a fit and proper person for the purposes the Digital ID legislation. Importantly, this reporting obligation applies even if an entity did 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 AGDIS 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 whether the entity is a fit and proper person.

Matters that should be disclosed include:

- 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 entity. This may include criminal background checks.

Services outside of the AGDIS

Accredited entities approved to participate in the AGDIS, or that have had their approval to participate suspended, must notify the Regulator if they propose to use their IT system to provide or receive services within a digital ID system other than the AGDIS.

This notification must be made no later than 28 days before the use of the other digital ID system. The information that must be included in the notification email is explained in rule 4.4(3) of the Digital ID Rules.

See section 4.4 of the Digital ID Rules for further details on rules relating to using a digital ID system other than AGDIS.

4.5 Record keeping

Accredited entities participating in the AGDIS are subject to record-keeping requirements. These requirements also apply to accredited entities that have had their approval to participate suspended, and entities whose approval has been revoked.

Accredited entities must keep a prescribed record for the period that ends at the later of the following:

- 3 years after the date the record was created
- 3 years after the date the record was last used by the entity for the purpose of providing a service that the entity is, or was, accredited to provide.

In addition, accredited entities must comply with obligations regarding the destruction or de-identification of personal information in their possession or control that was obtained through the AGDIS. Non-compliance with these obligations is enforced by the OAIC. Failure to comply with these obligations may give rise to a substantial civil penalty.

See sections 135–136 of the Digital ID Act and rule 6.2 of the Digital ID Rules for further details on record keeping requirements, including destruction and de-identification of documents, and the definition of a prescribed record.

4.6 Data standards

Ongoing requirements relating to data standards for approved entities are described in the Digital ID (AGDIS) Data Standards.

The AGDIS Data Standards provide the technical integration requirements for approved entities, along with technical and design features that entities must have to participate in the AGDIS, including how data must be structured to be transmitted in the AGDIS.

For accredited entities participating in the AGDIS, both the AGDIS Data Standards and Accreditation Data Standards apply.

Failure to comply with the relevant Data Standards requirements can provide a basis for the Regulator to suspend or revoke an entity's approval to participate in the AGDIS.

4.7 Privacy obligations

The OAIC, as the privacy regulator, has produced guidance materials to assist entities to understand and comply with their privacy obligations under the AGDIS. These include Notifiable Data Breach obligations which apply where personal information is accessed or disclosed without authorisation or is lost. Entities should refer to the OAIC's materials on the [Digital ID System website](#) for more detailed information on how to report a data breach.

5. Changes to AGDIS approval

An approved entity may apply for changes to its approval, including by:

- submitting administrative changes such as change of contact details and authorised officers
- requesting the imposition, variation or revocation of a condition on its approval, such as service name changes
- adding or removing services it is approved to provide, or provide access to, in the AGDIS
- requesting the variation, suspension or revocation of its AGDIS approval.

Changes to conditions or AGDIS approvals can be requested by completing and submitting the *Conditions on accreditation or AGDIS approval form*, available on the [Digital ID System website](#).

The Regulator may also, on its own initiative, suspend or revoke an entity's approval, impose new conditions, or vary or revoke an existing condition on an entity's approval.

5.1 Entity initiated changes

Requesting administrative changes

An approved entity can email the Regulator to request administrative changes.

For changes to an approved entity's authorised officer or primary contact person/s, or an organisation's contact details, an entity should complete and submit the *Organisation and Authorised Officer form*, available on the [Digital ID System website](#).

For changes to service contact details, an entity should complete and submit a *Service and Contact Person form*, available on the [Digital ID System website](#).

Impose, vary or revoke conditions

An approved entity can apply for a condition to be imposed, varied or revoked by completing and submitting the *Conditions on accreditation or AGDIS approval form*, available on the [Digital ID System website](#).

When applying, an entity will need to specify:

- whether the request is for a condition to be imposed, varied, or revoked
- whether the condition relates to the entity, the entity's service, or a service the entity provides, or provides access to
- the desired date for the condition, or its variation or revocation, to take effect, if any
- the desired date for the condition to cease, if any
- justification for the change and relevant supporting evidence for the Regulator to consider when assessing the entity's application for the condition or the variation or revocation of a condition.

An approved entity may wish to contact the Regulator via email to discuss the documentation required to support its application.

The Regulator may engage with the entity to discuss the purpose and proposed wording of the condition to ensure it is fit for purpose.

Once a decision has been made by the Regulator, the entity will receive a written notice of the Regulator's decision in relation to the application, stating the change and the day on which it takes effect. If the Regulator refuses to impose, vary or revoke the condition, it must give the entity a written notice of refusal, including reasons for the refusal.

The entity must not operate in accordance with the proposed change, its variation or revocation unless it has received the appropriate notice from the Regulator and until the effective date.

The Regulator may not provide a notice before changing a condition if the Regulator reasonably believes that the need to change the condition is serious and urgent.

The [AGDIS Register](#) will be updated to reflect a decision by the Regulator to impose, vary or revoke conditions on an entity's approval.

Adding, varying or revoking a service

The services an entity is approved to provide, or provide access to, is a condition of its approval.

If an entity wishes to add, vary or no longer offer (revoke) a service, it will need to apply to impose, vary or revoke a condition. To do so, an entity must complete and submit the *Conditions on accreditation or AGDIS approval form*, available on the [Digital ID System website](#), alongside supporting information.

An entity must not provide a service, or access to a service, within the AGDIS without approval, as this would be deemed a breach of its approval conditions and may lead to a suspension or revocation of the entity's AGDIS approval.

Vary, suspend or revoke approval

An approved entity can request the variation, suspension or revocation of its approval.

Varying an approval

An approved entity can apply to change the name recorded on its approval by completing and submitting the *Application to vary accreditation or AGDIS approval form*, available on the [Digital ID System website](#).

The entity will be asked to confirm the new name it would like displayed in the AGDIS Register and the date it would like this change to take place. It will also be asked to provide an attestation from an accountable executive to support the application for its details to be varied.

When applying for the amendment, the entity should provide supporting evidence of the change of the entity's name, such as updated ABN registration.

Entities should submit their form and accompanying documents as early as possible to avoid delays in future applications and ensure compliance with the Digital ID legislation.

The [AGDIS Register](#) will be updated to reflect a decision by the Regulator to vary the name recorded for the entity.

Where an approved entity is a government entity and is subject to a machinery of government change, it is important that they engage early with the Regulator to discuss the implications of the changes and whether a name variation is sufficient, or whether a new application for approval will be required.

Suspending an approval

An approved entity can apply for suspension of its AGDIS approval, or suspension of a specific service type, by completing and submitting the *Suspension of accreditation or AGDIS approval form*, available on the [Digital ID System website](#).

Suspension can be for a specific period, or it can be open ended.

The entity will be required to provide details and reasons for requesting the suspension, dates for the requested suspension, and an attestation from an accountable executive to support the application to suspend.

The Regulator has discretion to approve or reject an entity's application for suspension of its AGDIS approval (or a specific service type).

If the Regulator suspends the entity's approval (or a specific aspect of its approval) following the entity's application, the Regulator may revoke the suspension if the entity requests the suspension be revoked.

The Regulator will issue a notice of a decision to the entity.

The [AGDIS Register](#) will be updated to reflect any decisions to suspend an entity's accreditation.

Revoking an approval

An approved entity can apply to the Regulator for revocation of its approval to participate in the AGDIS by completing and submitting a *Revocation of Accreditation or AGDIS approval form*, available on the [Digital ID System website](#).

The entity will be asked to provide details and reasons for requesting its approval be revoked and will be asked to provide an attestation from an accountable executive to support the application.

Once an entity has applied for the revocation of its approval to participate in the AGDIS, the Regulator must grant the request for the service to be revoked. Revocation is not instantaneous and the date the revocation takes effect will be determined by the Regulator.

The [AGDIS Register](#) will be updated to reflect any decisions to revoke an entity's approval to participate in the AGDIS.

See section 70 –73 of the Digital ID Act for information on varying, suspending and revoking approval to participate in the AGDIS.

5.2 Regulator initiated changes

Impose, vary or revoke conditions

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

The types of conditions the Regulator may impose are not limited by the Act and may include conditions regarding actions an entity must take prior to the Regulator deciding to suspend or revoke an entity's approval.

For example, prior to suspending or revoking an approval, the Regulator may impose a condition requiring the entity to not generate any new digital IDs in the period until a final decision on the suspension or revocation is made.

If the Regulator intends to impose, vary or revoke a condition on its own initiative it will provide a notice to the entity, outlining the proposed change and requesting a written response from the entity.

However, the Regulator may not provide a notice before imposing a condition if directed by the Minister for Finance or changing a condition if the Regulator reasonably believes that the need to change the condition is serious and urgent.

Conditions imposed by the Regulator on an entity's approval will be published on the [AGDIS Register](#).

Suspend or revoke approval to participate

The Regulator has the power to suspend or revoke an entity's approval to participate in the AGDIS to protect other participants in the AGDIS and ensure the integrity and security of the AGDIS.

The Regulator must suspend or revoke an approval at the direction from the Minister for Finance for reasons of national security.

The Regulator may suspend or revoke an approval where:

- the Regulator reasonably believes there is non-compliance with the Digital ID legislation
- the Regulator reasonably believes there has been or there is suspected to have been a cyber security incident that risks the operation of the AGDIS (for suspension)
- the Regulator reasonably believes there has been a serious cyber security incident involving the entity (for revocation)
- the Regulator is satisfied it is no longer appropriate for the entity to be approved (including for reasons relating to whether the entity remains a fit and proper person)
- the entity is winding up or ceasing to carry on business.

The Regulator must provide an entity with a show cause notice before suspending or revoking its approval. It must set out the grounds for suspending or revoking the entity's approval and allow the entity 28 days from the day the notice is given to respond with a written statement as to why its approval should not be suspended or revoked.

This provides the entity with an opportunity to engage with the Regulator and provide additional information to support the continuation of its AGDIS approval.

A show cause notice is not required for suspension if the reason for the suspension is on the grounds of an actual or suspected security or cyber security incident. A show cause notice is also not required for suspension or revocation directed by the Minister for Finance.

If the Regulator decides to suspend or revoke an entity's approval, a written notice of suspension or revocation will be issued to the entity. The notice will include the reasons for suspension or revocation and the date it takes effect.

The [AGDIS Register](#) will be updated to reflect that an entity's approval is suspended or revoked.

6. Compliance and enforcement approach

The Regulator exercises its compliance and enforcement powers independently and in the public interest. In deciding the appropriate compliance and enforcement response, the Regulator is guided by the ACCC [Compliance and Enforcement Policy](#).

The Regulator may use a range of flexible and integrated strategies and tools to promote compliance with the Digital ID legislation. These include:

- engaging with accredited and approved entities to provide general information and guidance
- encouraging a compliance culture among accredited and approved entities
- working collaboratively and sharing information as appropriate with other agencies

employing appropriate enforcement options, including by resolving possible contraventions administratively, or by litigation or other formal enforcement outcomes.



The Regulator’s enforcement options are outlined in section 6.2. They include powers to impose, vary or revoke conditions on an AGDIS approval, and powers to suspend or revoke an AGDIS approval.

6.1 Compliance monitoring tools

The Regulator has a range of information sources and monitoring tools to assess levels of compliance with the Digital ID legislation.

These compliance monitoring tools are outlined below.

Table 1: Overview of information sources and compliance monitoring tools

	<p>Direct reports by consumers and stakeholders</p> <p>Consumers can make reports to the Regulator through the ACCC website.</p> <p>Accredited and approved entities can submit reports of suspected non-compliance by other entities to the Regulator.</p>
	<p>Accredited and approved entity self-reporting</p> <p>Accredited and approved entities are encouraged to self-report suspected non-compliance to the Regulator.</p>



Notification requirements

Accredited and approved entities are required to notify the Regulator of prescribed reportable incidents (see section 4.4).

Assessment of information submitted with a required notification may reveal compliance issues for further investigation or prompt re-examination of an existing accreditation or approval.



Annual review and reports

Accredited entities must conduct mandatory annual reviews and submit annual reports to the Regulator, which will assist to identify compliance issues to be addressed, as well as concerning trends.



Cross-agency information sharing

The Regulator, System Administrator and OAIC are permitted to share information relating to potential non-compliance and have signed a tripartite MOU located on the [Digital ID System website](#). In particular:

- The System Administrator may provide information to the Regulator regarding reportable cyber security and digital fraud incidents, IT system changes and unplanned system outages to protect the security, integrity and performance of the AGDIS.
- The OAIC may provide information to the Regulator in accordance with its functions and duties.



Undertake compliance assessments

The Regulator may issue an accredited or approved entity a notice requiring it to undergo a Compliance Assessment, in circumstances including:

- to determine if an entity is complying with the Act, or
- if the Regulator suspects a specified incident has occurred such as:
 - a cyber security or digital ID fraud incident,
 - an incident that may materially impact on the operation of the AGDIS, or
 - a material change in the entity's operating environment that may materially impact its risk profile.



Information requests and compulsory notices




The Regulator may request that an accredited or approved provide information to the Regulator on a voluntary basis to assist investigations and inform compliance and enforcement activity.

The Regulator may issue compulsory notices to compel the provision of information or documents in circumstances permitted under the Act. Failure to comply with a compulsory notice may result in substantial civil pecuniary penalties under the Act.

6.2 Enforcement action

There are a range of enforcement options available to the Regulator under the Digital ID regulatory framework. An overview of some of these options is provided in the table below.

Table 2: Overview of enforcement options

	<p>Administrative resolutions</p> <p>The Regulator may decide to deal with a matter administratively. This may include:</p> <ul style="list-style-type: none">■ Drawing an issue to the entity's attention and providing information to help it gain a better understanding of the Digital ID legislation, and to encourage rectification and future compliance.■ Placing the entity on notice about the Regulator's concerns and the possibility of future investigation and action should the conduct continue or re-emerge.■ Dealing with the matter informally if the entity promptly and effectively corrects a possible contravention and implements measures to prevent recurrence.■ Accepting a voluntary written commitment to address less serious instances of non-compliance.
	<p>Infringement notices</p> <p>The Regulator may issue an infringement notice where it believes on reasonable grounds that there has been a contravention of a civil penalty provision under the Act.</p> <p>This may enable a matter to be resolved without legal proceedings.</p>
	<p>Court-enforceable undertaking</p> <p>The Regulator may accept a court-enforceable undertaking for a potential contravention of a civil penalty provision under the Act. The undertaking may include requirements that an accredited or approved entity will take, or refrain from taking, certain action.</p> <p>This may be appropriate if the entity agrees to address the issue of concern, accepts responsibility for its actions and reviews procedures to improve compliance.</p>



Directions

The Regulator has the power to:

- Direct an accredited or approved entity to do something or refrain from doing something, in connection with a decision related to an entity's accreditation or approval.
- Direct an approved entity to do something to protect the integrity or performance of the AGDIS.
- Direct an accredited entity to take remedial action.

Failure to comply with a direction may result in substantial civil pecuniary penalties under the Act.



Impose, vary or revoke conditions on an accreditation or approval to participate in the AGDIS

The Regulator may impose, vary or revoke conditions on the entity's accreditation or approval under certain circumstances (see section 5.2).



Suspend or revoke an accreditation or approval to participate in the AGDIS

The Regulator may suspend or revoke an entity's accreditation or approval under certain circumstances, for example if the Regulator reasonably believes the entity is breaching, or has breached, the Act (see section 5.2).

An entity is prohibited from holding out that the entity is accredited or approved in the event of a revocation.



Court action

The Regulator may commence court action where, having regard to all the circumstances, it considers litigation is the most appropriate way to achieve compliance objectives.

The Regulator may seek injunctions for breaches of civil penalty provisions under the Act and/or substantial civil pecuniary penalties.

7. Review of Regulator decisions

Certain decisions of the Regulator are reviewable. This includes decisions of the Regulator to:

- refuse to approve an entity to participate in the AGDIS
- impose, vary or revoke a condition, or refuse to impose or vary a condition
- suspend or refuse to suspend an entity's approval to participate in the AGDIS
- revoke the AGDIS approval of entity.

A reviewable decision is eligible for internal review if it is made by a delegate of the decision maker. Other reviewable decisions are only eligible for review by the Administrative Review Tribunal or Federal Court (see below).

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

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

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 entity. A request for review of a decision made by the Regulator must be made by the affected entity.

An entity can submit a written request for internal review via email to the Regulator.

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 entity 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 entity with a written statement of its reasons for its decision.

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 (i.e. not a delegate), or if the decision is an internal review decision made by the Regulator.

The Regulator will advise the entity 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 Administrative Review Tribunal for a review of a decision is available on the Administrative Review Tribunal website.

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.

Entities 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.

Appendix A – Exemption application assessment factors

The Regulator will generally only grant exemptions to the voluntariness obligation in exceptional circumstances.

The following table lists the assessment factors the Regulator may consider in determining applications for exemptions.

Factor	Information to be provided by applicants
The type of applicant and services	
Whether the applicant is eligible for an exemption to the voluntariness obligation.	
The Regulator cannot grant an exemption to:	
<ul style="list-style-type: none">■ a Commonwealth entity, or a Commonwealth company, within the meaning of the <i>Public Governance, Performance and Accountability Act 2013</i>■ a person or body that is an agency within the meaning of the <i>Freedom of Information Act 1982</i>■ a body specified, or the person holding an office specified, in Part I of Schedule 2 to the meaning <i>Freedom of Information Act 1982</i>.	
Whether the applicant is a small business.	Provide details of the applicant’s organisation type and the number of employees, annual revenue and other factors relevant to the business size.
Being a small business does not guarantee that an exemption will be granted. The applicant must demonstrate why its circumstances are exceptional and justify an exemption being granted.	
Whether the applicant provides services, or access to services, solely online.	Provide details of the channels the applicant uses to provide products and services to its consumers.
Providing services solely online will not guarantee that an exemption will be granted. The applicant must demonstrate why its circumstances are exceptional and justify an exemption being granted.	
Impact of proposed exemption on the applicant, consumers and the AGDIS	
Whether the applicant has explored alternative options to facilitate compliance.	Provide details of alternative options the applicant explored to facilitate compliance with the voluntariness requirement and why these are not viable.

Whether the proposed exemption is only required for a limited time	<p>Provide details of the scope and duration of the proposed exemption.</p> <p>For example, is the proposed exemption for a limited time in response to a specific event, such as an emergency situation?</p>
Potential for any perverse consequences for the applicant, consumers or the AGDIS if the exemption is not granted.	Provide details of risk of negative consequences to the applicant, consumers or the AGDIS if the exemption is not granted, including the likelihood and impact of the risk/s eventuating.
<p>The number of consumers potentially affected if the exemption is granted.</p> <p>The more consumers affected, the less likely the exemption will be granted.</p>	<p>Provide details of the market/s the applicant provides services to, and the number of consumers expected to access the service/currently accessing the service.</p> <p>Provide details of the number of consumers expected to access the service, or currently accessing the service, who are known to use a digital ID.</p> <p>Provide details of the number of consumers potentially impacted if the exemption is granted, and how they will be impacted.</p>
<p>Whether the exemption affects vulnerable consumers.</p> <p>The greater the impact to vulnerable consumers, the less likely the exemption will be granted.</p>	<p>Provide details of any vulnerable consumer groups who are expected to or currently access the service.</p> <p>Provide details of consideration the applicant has given to the impacts on vulnerable consumers if the exemption is granted and how these impacts will be managed.</p>
Whether the exemption would unduly undermine access to services of that kind.	Provide details of the type and purpose of the service, including available alternatives to the applicant's provision of that service and the accessibility of those alternatives.
Whether the service directly or indirectly impacts other services and whether the exemption would directly or indirectly impact other services.	<p>Provide details of whether the service directly or indirectly impacts other services.</p> <p>Provide details of whether the exemption would impact other services in the AGDIS.</p> <p>Provide details of any risk to other services in the AGDIS if the exemption is/is not granted.</p>

Whether the applicant will otherwise meet its obligations under the Digital ID legislation	
<p>Other conditions or exemptions sought or granted.</p> <p>Where granting the exemption may result in other conditions imposed by the Regulator being contravened, the exemption is less likely to be granted.</p>	<p>Provide details of any other conditions imposed on the applicant under the Digital ID legislation (including conditions being sought or expected to be sought) and their interaction with the exemption.</p>
<p>Compliance history.</p> <p>If the applicant has demonstrated a history of non-compliance, the exemption is less likely to be granted. However, a history of compliance does not guarantee the exemption will be granted.</p>	<p>Provide details of any incidents of non-compliance with the Digital ID legislation.</p>
<p>Proactive engagement with the Regulator.</p> <p>A lack of proactive engagement with the Regulator will make an exemption less likely to be granted. However, proactive engagement does not guarantee the exemption will be granted.</p>	
<p>Provided evidence and clear justification in support of the application.</p>	<p>Provide a clear justification, and evidence in support, for why the exemption should be granted.</p>
<p>Other</p>	<p>Provide details of any other factors that the applicant considers may be relevant to the Regulator's assessment of the exemption application.</p>

