EXPLANATORY STATEMENT

Issued by authority of the Digital ID Data Standards Chair

Digital ID Act 2024

Digital ID (AGDIS) Data Standards 2024

Subsection 99(1) of the *Digital ID Act 2024* (the Digital ID Act) provides that the Digital ID Data Standards Chair (the Data Standards Chair) may, in writing, make one or more standards about the matters prescribed in that provision. Relevantly, data standards may be made about:

- technical integration requirements for entities to participate in the Australian Government Digital ID System (AGDIS);
- technical or design features that entities must have to participate in the AGDIS;
- technical, data or design standards if required to do so by the *Digital ID (Accreditation) Rules 2024* (Accreditation Rules) or the *Digital ID Rules 2024* (the Digital ID Rules) (rules made under section 168 of the Digital ID Act for the purposes of the provisions in which the term 'Digital ID Rules' occurs); and
- other matters prescribed by the Digital ID Rules.

For the purposes of paragraphs 99(1)(c) and (d), neither the Digital ID Rules nor the Accreditation Rules prescribe any matters that need to be included in these *Digital ID (AGDIS) Data Standards 2024* (the AGDIS Data Standards).

The purpose of the AGDIS Data Standards is to support the operation of the AGDIS established by the Digital ID Act, which aims to provide individuals with secure, convenient, voluntary and inclusive ways to verify their identity for use in online transactions with government and businesses. In particular, the AGDIS Data Standards facilitate and promote trust in the digital ID services provided within the AGDIS by providing:

- technical integration requirements for entities to participate in the AGDIS; and
- technical or design features that entities must have to participate in the AGDIS including how data must be structured to be transmitted across the AGDIS.

Accredited entities and relying parties participating in the AGDIS will be required to implement the technical requirements in the AGDIS Data Standards, in addition to the requirements in the Digital ID Rules (where relevant to the services they perform or consume in the AGDIS). For accredited entities participating in the AGDIS, the AGDIS Data Standards apply in addition to the Accreditation Rules, the Digital ID Rules and the *Digital ID (Accreditation) Data Standards 2024* (Accreditation Data Standards).

Section 167 of the Digital ID Act provides that the AGDIS Data Standards may make provision in relation to a matter by applying, adopting or incorporating, with or without modification, any matter contained in any other instrument or other writing as in force or existing from time to time, despite subsection 14(2) of the *Legislation Act 2003* (the Legislation Act).

The AGDIS Data Standards incorporate by reference technical standards contained in instruments published by the following bodies: the OpenID Foundation; the Internet Engineering Task Force; the International Telecommunications Union; and the Unicode Consortium. The incorporated instruments are free to access and publicly available on the internet. The version of each instrument incorporated by reference in the AGDIS Data Standards is the version that was in force at the time the AGDIS Data Standards commence. To allow readers to easily locate the incorporated instruments, the URL for each instrument appears in notes in the AGDIS Data Standards.

An exposure draft of the AGDIS Data Standards and accompanying consultation materials were released for public consultation from 8 July 2024 to 12 August 2024.

The Department received 16 submissions on the draft AGDIS Data Standards. A variety of stakeholders provided feedback, including individual contributors, private organisations, and agencies across the Commonwealth and States and Territories. Submissions provided feedback on the clarity and accuracy of the draft AGDIS Data Standards, requirements about privacy and data use, and suggested technical corrections. Stakeholder feedback was considered and is reflected in the policy underpinning the AGDIS Data Standards.

Accordingly, the above consultation process satisfied the statutory preconditions in both section 100 of the Digital ID Act and section 17 of the Legislation Act.

Details of the AGDIS Data Standards are set out in **Attachment A**.

Subsection 99(4) of the Digital ID Act provides that the Digital ID Data Standards is a legislative instrument, but that section 42 (disallowance) of the Legislation Act does not apply to them. Paragraph 44(2)(a) of the Legislation Act provides that section 42 does not apply in relation to a legislative instrument if an Act declares, or has the effect, that section 42 does not apply in relation to the instrument or provision. The AGDIS Data Standards are therefore a legislative instrument for the purposes of the Legislation Act but are not subject to disallowance.

The AGDIS Data Standards rely on section 4 of the *Acts Interpretation Act 1901*, as they are made in contemplation of commencement of section 99 of the Digital ID Act. The AGDIS Data Standards commence at the same time the Digital ID Act commences.

The Office of Impact Analysis (OIA) has been consulted in relation to the AGDIS Data Standards and advised that an Impact Analysis is **not required** as the standards do not create any additional impact other than what has already been assessed in the Impact Analysis for the Digital ID Act (OIA reference number: OBPR23-04323).

As the AGDIS Data Standards are not a disallowable legislative instrument, a statement of compatibility with human rights is not required to be prepared under subsection 9(1) of the *Human Rights (Parliamentary Scrutiny) Act 2011* or section 15J of the Legislation Act. However, a statement of compatibility has been prepared as a matter of best practice.

A Statement of Compatibility with Human Rights is at **Attachment B**.

The AGDIS Data Standards are compatible with human rights, and to the extent that they may limit human rights, those limitations are reasonable, necessary and proportionate.

GLOSSARY

This Explanatory Statement uses the following abbreviations and acronyms.

Abbreviation	***Definition***
Accreditation Data Standards	*Digital ID (Accreditation) Data Standards 2024*
Accreditation Rules	*Digital ID (Accreditation) Rules 2024*
AGDIS	Australian Government Digital ID System
Data Standards Chair	Digital ID Data Standards Chair
Digital ID Act	*Digital ID Act 2024*
Digital ID Rules	*Digital ID Rules 2024*
Transitional Act	*Digital ID (Transitional and Consequential Provisions) Act 2024*
Transitional Rules	*Digital ID (Transitional and Consequential Provisions) Rules 2024*

ATTACHMENT A

Details of the *Digital ID (AGDIS) Data Standards 2024*

Chapter 1—Preliminary

Section 1.1 Name

1.1 This section provides that the name of this instrument is the *Digital ID (AGDIS) Data Standards 2024*.

Section 1.2 – Commencement

1.2 The AGDIS Data Standards commence at the same time as the Digital ID Act commences.

Section 1.3 – Authority

1.3 The AGDIS Data Standards is made under section 99 of the Digital ID Act.

Section 1.4 – Definitions

1.4 This section sets out the definitions of expressions in the AGDIS Data Standards.

1.5 Notes 1, 2, 3 and 4 under section 1.4 relevantly provide that a number of expressions in the AGDIS Data Standards are defined in the Digital ID Act, the Transitional Act, the Accreditation Rules and the Digital ID Rules.

1.6 Subsection 1.4(1) provides those expressions defined in the Digital ID Act, the Transitional Act, the Accreditation Rules and the Digital ID Rules have the same meaning in the AGDIS Data Standards, unless otherwise specified.

1.7 By way of example of specified exceptions, the note to subsection 1.4(1) provides:

- the expressions 'ASP', 'ISP' and 'IXP', which are used in the Accreditation Rules, have a different meaning in subsection 1.4(2) of the AGDIS Data Standards; and
- the expression 'IXP', which is used in the Digital ID Rules, has a different meaning in subsection 1.4(2) of the AGDIS Data Standards.

1.8 A number of the expressions appearing in the AGDIS Data Standards are drawn from international standards. Subsection 1.4(2) outlines a variety of international standards for various bodies including the International Telecommunications Union, the OpenID Foundation, the Internet Engineering Task Force and the Unicode Consortium.

1.9 Further information appears in the notes on section 1.8 (Key words) and section 1.9 (Incorporated instruments) below.

Section 1.5 – Meaning of *federation protocol*

1.10 This section defines what the term 'federation protocol' means in the AGDIS Data Standards, and how a federation protocol operates within the AGDIS. The AGDIS federation protocol will establish the authentication of a digital ID through a relationship among 5parties:

- the participating accredited attribute service provider;
- the participating accredited identity service provider;
- the participating accredited identity exchange provider;
- the participating relying party; and
- the individual/user.

1.11 Subsection 1.5(1) provides that a ‘federation protocol’ means an open protocol that enables participating entities to communicate with each other and share attributes of individuals in a trusted manner.

1.12 Subsection 1.5(2) provides that, at the time the AGDIS Data Standards were made, Schedule 2 (AGDIS OpenID Connect Profile) to the AGDIS Data Standards is the only federation protocol for the AGDIS.

Section 1.6 – Meaning of *technical relying party*

1.13 This section defines the term ‘technical relying party’ to distinguish between the terms ‘relying party’ and ‘participating relying party’ defined in section 9 of the Digital ID Act, and to align certain technical concepts with industry standards.

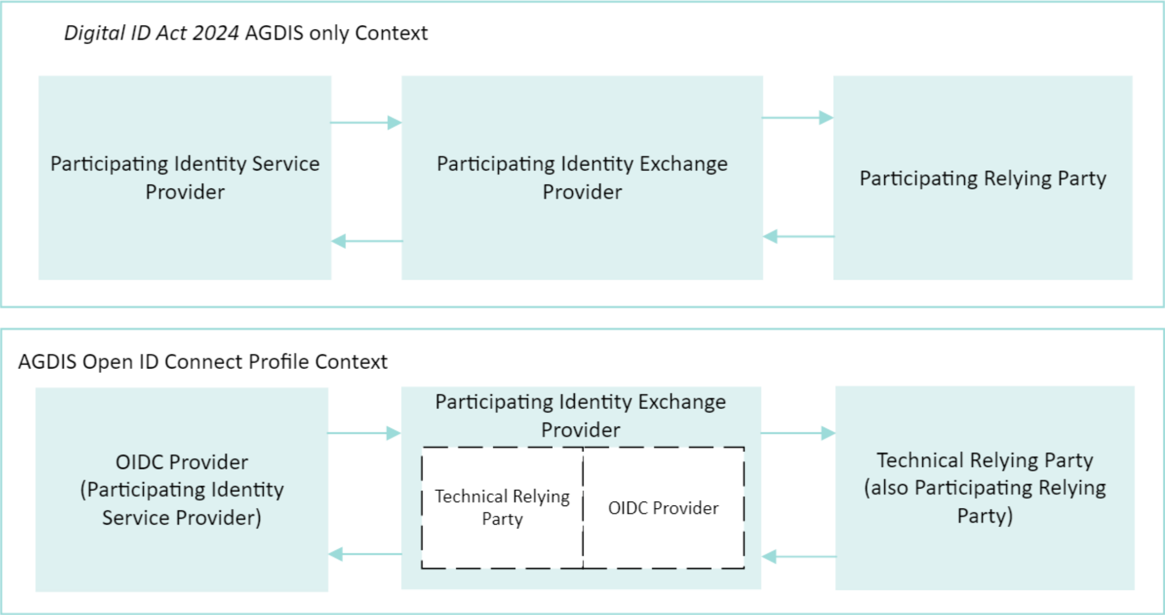
- Paragraph 1.6(a) provides that one of the meanings of a technical relying party is a participating accredited identity exchange provider’s OpenID Connect Core 1.0 software used to co-ordinate the flow of data or information between entities participating in the AGDIS.
- Paragraph 1.6(b) provides that another meaning of a technical relying party is a participating relying party’s OpenID Connect Core 1.0 software used to authenticate the participating relying party with the participating accredited identity exchange, and to request and receive information or data from the participating accredited identity exchange.
- Paragraph 1.6(c) provides that the final meaning of a technical relying party is a participating accredited attribute service provider’s OpenID Connect Core 1.0 software used to authenticate the participating accredited attribute service provider with the participating accredited identity exchange, and to request and receive information or data from the participating accredited identity exchange.
- The note to section 1.6 provides that, to avoid doubt, a technical relying party is not a relying party as defined in section 9 of the Digital ID Act.

1.14 Readers of the AGDIS Data Standards (such as technical specialists and platform architects) are likely to understand the scope of the term ‘relying party’ to be broader than the definition used in the Digital ID Act, including to cover:

- an application or website that outsources its user authentication function; and/or
- software that requests tokens either for authenticating a user or for accessing a resource.

1.15 The defined term ‘technical relying party’ is intended to capture the roles and operation of the OpenID Connect Core 1.0 software and how information is requested and received within the AGDIS context, as illustrated in Figure 1 below:

Figure 1: Technical Relying Party Context Diagram


Digital ID Act 2024 AGDIS only Context
Participating Identity Service Provider
Participating Identity Exchange Provider
Participating Relying Party
AGDIS Open ID Connect Profile Context
OIDC Provider (Participating Identity Service Provider)
Participating Identity Exchange Provider
Technical Relying Party
OIDC Provider
Technical Relying Party (also Participating Relying Party)

Section 1.7 – Abbreviations

1.16 This section defines a number of abbreviations used in the AGDIS Data Standards including its Schedules. Most of the abbreviations relate to terms defined in subsection 1.4(2) of the AGDIS Data Standards.

1.17 The abbreviations ‘ASP’, ‘ISP’ and ‘IXP’ appearing in this section are also used in the Accreditation Rules, where they have a different meaning. Similarly, the abbreviation ‘IXP’ is used in the Digital ID Rules, where it has a different meaning. While all the abbreviations refer to attribute service providers, identity service providers and identity exchange providers who are accredited, in the AGDIS Data Standards the abbreviations refer specifically to those accredited entities who are also approved to participate in the AGDIS.

- The intent of using the same abbreviations with different meanings is to minimise the likelihood of confusion for the intended audience, being technical experts and platform architects, by introducing new terminology to define substantially similar subject matter.

- This section defines the abbreviated terms to mean accredited entities approved to participate in the AGDIS. Accredited entities not approved to participate in the AGDIS are not required to comply with standards in the AGDIS Data Standards applying to an ‘ASP’, ‘ISP’ and ‘IXP’.

Section 1.8 – Key words

1.18 This section defines key words used in the AGDIS Data Standards and each incorporated instrument (see notes on section 1.9 (Incorporated instruments) below) to describe the requirements of participants in the AGDIS.

1.19 The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “NOT RECOMMENDED”, “MAY” and “OPTIONAL” are intended to be interpreted in a way that is not inconsistent with RFC 2119.

1.20 RFC 2119 (as modified by RFC 8174) is considered the internet best practice standard to communicate to a technical audience how a technical requirement or specification in an RFC is to be implemented in a specific setting. RFC 2119 is an established and well-known standard within the internet industry.

1.21 The intended readers of the AGDIS Data Standards, who are technical specialists and platform architects, will be familiar with key words used throughout the internet industry. However, the key words in RFC 2119 incorporate a degree of optionality and flexibility.

1.22 As the Digital ID Regulator will have responsibility for enforcing the AGDIS Data Standards, the key words section translates the technical key words into the context of the Digital ID Act’s legislative framework to enable the Digital ID Regulator to determine whether a standard or condition on participation in the AGDIS has, or has not, been met.

- The terms “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, and “SHALL NOT”, refer to absolute requirements. A participant in the AGDIS has no discretion in its behaviour.
- The terms “MAY”, “OPTIONAL”, “RECOMMENDED”, “NOT RECOMMENDED”, “SHOULD” and “SHOULD NOT” refer to optional requirements and the participating entity has discretion to do certain behaviour. In limited circumstances (such as where a condition on the entity’s participation would not permit the behaviour, or such behaviour would prevent interoperability), the entity does not have discretion to do that behaviour.

Section 1.9 – Incorporated instruments

1.23 The AGDIS Data Standards incorporate by reference various documents as in force at the commencement of the AGDIS Data Standards.

1.24 Incorporating documents as in force from time to time is not appropriate because the AGDIS Data Standards is a non-disallowable legislative instrument. This means that any changes to these documents after the commencement of the AGDIS Data Standards will not automatically be incorporated into the AGDIS Data Standards.

1.25 Subsection 1.9(2) clarifies that where an incorporated document, such as an RFC, references another document that is not expressly incorporated by the AGDIS Data Standards, the reference to the other document, is a reference to the other document as in force at the commencement of the AGDIS Data Standards.

1.26 This section does not affect the operation of sections 2, 10 and 46 of the *Acts Interpretation Act 1901*, which provide in effect that legislative instruments referred to in the AGDIS Data Standards are incorporated as amended or re-enacted from time to time.

1.27 This rule is authorised by subsection 167(3) of the Digital ID Act.

Table 1: List of incorporated instruments

Instrument title	Meaning	Published by	Availability	Where to obtain
ITU E.164	the standard for international public telecommunication structures.	International Telecommunication Union	Free, online	https://www.itu.int/rec/T-REC-E.164-201011-I/en
OpenID Connect Core 1.0	the standard for an identity layer which operates on top of RFC 6749.	OpenID Foundation	Free, online	https://openid.net/specs/openid-connect-core-1_0.html
OpenID Connect Discovery 1.0	The specification titled *OpenID Connect Discovery 1.0 incorporating errata set 2*.	OpenID Foundation	Free, online	https://openid.net/specs/openid-connect-discovery-1_0-final.html.
OpenID Connect Extended Authentication Profile (EAP) ACR Values 1.0	the standard used to request specific authentication context classes.	OpenID Foundation	Free, online	https://openid.net/specs/openid-connect-eap-acr-values-1_0.html
RFC 2119	the RFC numbered 2119 and titled *Key Words for use in RFCs to Indicate Requirement Levels*.	Internet Engineering Task Force	Free, online	https://datatracker.ietf.org/doc/html/rfc2119.
RFC 3339	the RFC numbered 3339 and titled *Date and Time on the Internet: Timestamps*.	Internet Engineering Task Force	Free, online	https://datatracker.ietf.org/doc/html/rfc3339.
RFC 3629	the RFC numbered 3629 and titled *UTF-8, a transformation format of Unicode and ISO 10646*.	Internet Engineering Task Force	Free, online	https://datatracker.ietf.org/doc/html/rfc3629.
RFC 3696	RFC numbered 3696 and titled *Application Techniques for Checking and Transformation of Names*.	Internet Engineering Task Force	Free, online	https://datatracker.ietf.org/doc/html/rfc3696.
RFC 3986	the RFC numbered 3986 and titled *Uniform Resource*	Internet Engineering Task Force	Free, online	https://datatracker.ietf.org/doc/html/rfc3986.

Instrument title	Meaning	Published by	Availability	Where to obtain
	Identifier (URI): Generic Syntax.			
RFC 4122	the RFC numbered 4122 and titled *A Universally Unique IDentifier (UUID) URN Namespace*.	Internet Engineering Task Force	Free, online	https://datatracker.ietf.org/doc/html/rfc4122.
RFC 5321	the RFC numbered 5321 and titled *Simple Mail Transfer Protocol*.	Internet Engineering Task Force	Free, online	https://datatracker.ietf.org/doc/html/rfc5321.
RFC 5322	the RFC numbered 5322 and titled *Internet Message Format.*	Internet Engineering Task Force	Free, online	https://datatracker.ietf.org/doc/html/rfc5322.
RFC 5646	the RFC numbered 5646 and titled *Tags for Identifying Languages*.	Internet Engineering Task Force	Free, online	https://datatracker.ietf.org/doc/html/rfc5646.
RFC 6749	the RF numbered 6749 and titled *The OAuth 2.0 Authorization Framework.*	Internet Engineering Task Force	Free, online	https://datatracker.ietf.org/doc/html/rfc6749.
RFC 6750	the RFC numbered 6750 and titled *The OAuth 2.0 Authorization Framework: Bearer Token Usage*.	Internet Engineering Task Force	Free, online	https://datatracker.ietf.org/doc/html/rfc6750.
RFC 6819	the RFC numbered 6819 and titled *OAuth 2.0 Threat Model and Security Considerations*.	Internet Engineering Task Force	Free, online	https://datatracker.ietf.org/doc/html/rfc6819.
RFC 7009	the RFC numbered 7009 and titled *OAuth 2.0 Token Revocation*.	Internet Engineering Task Force	Free, online	https://datatracker.ietf.org/doc/html/rfc7009.
RFC 7517	the RFC numbered 7517 and titled *JSON Web Key (JWK).*	Internet Engineering Task Force	Free, online	https://datatracker.ietf.org/doc/html/rfc7517.
RFC 7591	the RFC numbered 7591 and titled *OAuth 2.0 Dynamic Client Registration Protocol*.	Internet Engineering Task Force	Free, online	https://datatracker.ietf.org/doc/html/rfc7591.

Instrument title	Meaning	Published by	Availability	Where to obtain
RFC 7636	the RFC numbered 7636 and titled *Proof Key for Code Exchange by OAuth Public Clients*.	Internet Engineering Task Force	Free, online	https://datatracker.ietf.org/doc/html/rfc7636.
RFC 7662	the RFC numbered 7662 and titled *OAuth 2.0 Token Introspection*.	Internet Engineering Task Force	Free, online	https://datatracker.ietf.org/doc/html/rfc7662.
RFC 8141	the RFC numbered 8141 and titled *Uniform Resource Names*.	Internet Engineering Task Force	Free, online	https://datatracker.ietf.org/doc/html/rfc8141.
RFC 8174	the RFC numbered 8174 and titled *Ambiguity of Uppercases vs Lowercases in RFC 2119 Key Words*.	Internet Engineering Task Force	Free, online	https://datatracker.ietf.org/doc/html/rfc8174.
RFC 8259	the RFC numbered 8259 and titled *The JavaScript Object Notation (JSON) Data Interchange Format*.	Internet Engineering Task Force	Free, online	https://datatracker.ietf.org/doc/html/rfc8259.
RFC 8446	the RFC numbered 8446 and titled *The Transport Layer Security (TLS) Protocol Version 1.3*.	Internet Engineering Task Force	Free, online	https://datatracker.ietf.org/doc/html/rfc8446.
UTF-8	the standard for encoding electronic communications.	Unicode Consortium	Free, online	https://www.unicode.org/versions/Unicode15.1.0/

Section 1.10 – Application – transitioned participating relying parties

1.28 This section applies to a transitioned participating relying party specified in subsection 10.1(1) when participating in the AGDIS in relation to a transitioned participating relying party service specified in subsection 10.1(1). This section also applies to the Designated Identity Exchange Provider.

- A transitioned participating relying party is a relying party that is taken to be a participating relying party in accordance with subitem 4(2) of Schedule 1 to the Transitional Act. See also rules 2.3 and 2.4 of Part 2 of Chapter 2 of the Transitional Rules.
- A transitioned participating relying party service, in relation to a transitioned participating relying party, is the service that the entity is approved to provide, or provide access to, in accordance with subitem 4(2)

of Schedule 1 to the Transitional Act. See also rules 2.3 and 2.4 of Part 2 of Chapter 2 of the Transitional Rules.

1.29 Under a preceding accreditation policy framework (known as the Trusted Digital Identity Framework (TDIF)), entities could use either the OpenID Connect Core 1.0 protocol (now reflected in Schedule 2 (AGDIS OpenID Connect Profile) to the AGDIS Data Standards) or a protocol based on Security Assertion Markup Language (SAML). The TDIF has now been superseded by the accreditation scheme established by the Digital ID Act.

1.30 Subsections 1.10(2), (3) and (4) provide for 3 alternative scenarios to prevent unintended non-compliance with the AGDIS OpenID Connect Profile. The scenarios are only relevant to the transitioned participating relying parties specified in subsection 1.10(1). All other transitioned participating relying parties (who are currently using the AGDIS OpenID Connect Profile) must comply with every provision in the AGDIS Data Standards in accordance with its terms.

1.31 The AGDIS OpenID Connect Profile is the preferred federation protocol within the AGDIS because it is generally understood to be easier to implement than SAML and to have a lower risk of implementation vulnerabilities. The AGDIS OpenID Connect Profile is more accessible and is better suited to implementing on mobile applications.

1.32 However, implementing the AGDIS OpenID Connect Profile would require changes to the listed entities’ current authentication configurations. This would require extensive coordination with the System Administrator and the Digital ID Regulator. Until a decision is made to require all entities to use a federation protocol based on OpenID Connect Core 1.0, specified entities currently using SAML can continue to rely on a SAML adapter operated by Services Australia (as the sole identity exchange provider participating in the AGDIS) to convert information to and from OpenID Connect Core 1.0 to SAML for the entity’s purposes.

1.33 The first scenario in subsection 1.10(2) is the default arrangement – it applies if either of the other 2 scenarios (subsections 10.1(3) or 10.1(4)) do not apply.

- In this scenario, subsection 1.10(2) provides that a transitioned participating relying party does not need to comply with the AGDIS OpenID Connect Profile, or other provisions, or parts of a provision that are about the AGDIS OpenID Connect Profile. It is, in effect, an exception to the requirement to comply with the AGDIS OpenID Connect Profile.
- This exception is time limited – it only applies in relation to the entity’s transitioned participating relying party service specified in subsection 1.10(1) and up to the ‘specified day’ (being the day that is 5 years after the day on which the AGDIS Data Standards commence, e.g., 1 December 2029 – see note on subsection 1.10(6) below).
- The exception is limited in scope – it only applies to the AGDIS OpenID Connect Profile. The entity must comply with every other provision, or every other part of a provision, in accordance with its terms and on, and from the commencement of the AGDIS Data Standards.

1.34 The second scenario in subsection 10.1(3) applies if: a decision is made to require one or more transitioned relying parties or services to implement the AGDIS OpenID Connect Data Profile at a particular time earlier than the ‘specified day’ (e.g., 1 December 2029 – see note on subsection 1.10(6) below); and that decision is given effect by the Data Standards Chair making a Digital ID Data Standard or amending these AGDIS Data Standards.

- In this scenario, the entity must comply with the AGDIS OpenID Connect Profile in relation to that service at that particular time.
- To avoid doubt, on and from the particular time specified, transitioned participating relying parties and the Designated Identity Exchange Provider must comply with every provision in the AGDIS Data Standards in accordance with its terms.

1.35 The third scenario in subsection 1.10(4) applies if the Data Standard Chair makes a Digital ID Data Standard, or amends these AGDIS Data Standards, to provide an alternative federation protocol to support SAML before the 'specified day' (e.g., 1 December 2029 – see note on subsection 1.10(6) below).

- In this scenario, the entity must comply with the alternative federation protocol for SAML when that Digital ID Standard or an amendment to these AGDIS Data Standards commence.
- The introduction of any alternative SAML federation protocol would be subject to the consultation requirements in section 100 of the Digital ID Act.

1.36 If a transitioned participating relying party changes its transitioned participating relying party service of its own volition so that it no longer uses SAML and implements the OpenID Connect Profile, it is not intended that subsection 1.10(4) would operate so as to require the entity to comply with both a SAML protocol and the Open ID Connect Profile. In this circumstance, it is envisaged the Data Standards Chair would remove the entity and its service from subsection 10.1(1) via a Digital ID Data Standard or an amendment to these AGDIS Data Standards. The entity would not be required to comply with the OpenID Connect Profile until the Data Standards Chair has removed the entity and it service from subsection 10.1(1).

1.37 Subsection 1.10(5) seeks to ensure the Designated Identity Exchange Provider will not be in breach of the AGDIS Data Standards to the extent it conveys, manages or coordinates the flow of data or other information in SAML within the AGDIS. This subsection clarifies that the Designated Identity Exchange Provider can facilitate a transitioned participating relying party to participate in the AGDIS to the extent necessary for the 3 scenarios described above.

1.38 Subsection 1.10(6) defines 'specified day' to mean the day that is 5 years after the day on which the AGDIS Data Standards commence. For example, if the AGDIS Data Standards commence on 1 December 2024, the specified day will be 1 December 2029.

Section 1.11 – Schedules

1.39 This section provides that the Schedules to the AGDIS Data Standards will be amended or repealed as set out in the applicable items in the Schedules. Any other provision (however described) in a Schedule to the AGDIS Data Standards has effect according to its terms.

Schedule 1 – AGDIS Onboarding Specifications

1.40 This Schedule sets out technical requirements for an accredited entity (as defined in the Digital ID Act) applying to participate in the AGDIS or approved to participate in the AGDIS.

1.41 Chapter 1 of this Schedule covers the common requirements that must be met by all participating accredited entities. It includes sub-requirements for security considerations, identity resolution and data sharing.

1.42 Chapter 2 of this Schedule covers the role specific requirements that must be met by a participating accredited identity exchange provider. This includes the sub-requirements for technical integration, identity service provider selection, user dashboard and data requirements. A key feature of this chapter and the AGDIS as a federated system is the blinding requirement in section 2.2.1 of this Schedule.

1.43 Section 2.2.1 of this Schedule sets out the requirement for blinding, which applies to participating accredited identity exchange providers. This section enables Services Australia (the only participating accredited identity exchange provider on commencement) to move from a 'double blind' to a 'single blind' approach, subject to the additional assurance and transparency requirements imposed by rule 2.2 of the Transitional Rules or any other conditions subsequently imposed by the Digital ID Regulator.

1.44 The double blind was a technical feature of the unlegislated AGDIS, establishing a technical barrier to the tracking and profiling of user behaviour across the system in the absence of the legislated privacy safeguards now in place. Under the double blind approach, the identity exchange that has brokered the flow of personal information throughout the unlegislated AGDIS has limited information sharing in 2 ways.

- First, the identity exchange has not disclosed to identity service providers the relying party services that each user accessed with their digital ID.
- Second, the identity exchange has not disclosed to relying parties which identity service provider was used to access their service. However, as there has only been one participating identity service provider, it has been implicit that users must have used myID, previously known as myGovID.

1.45 Section 2.2.1 provides that a participating accredited identity exchange must implement the first 'side' of the blind: they must not broker any information about the participating relying party requesting authentication to any of its identity service providers.

1.46 Under a single blind approach, implementing the second 'side' of the blind is not mandatory. The participating accredited identity exchange provider may inform participating relying parties which participating accredited identity service provider the individual used to authenticate (for example, whether the individual used myID or an alternative provider).

1.47 The purpose of supporting a single blind approach is to enable benefits in terms of:

- fraud detection - as a user's choice of identity service provider is information that can help participating relying parties to detect and prevent fraud;
- user experience such as making it easier to log in with myID;

- increasing participation in the AGDIS - as it removes a feature that some private sector stakeholders have noted would discourage them from joining as participating relying parties in the future, and some stakeholders may have legal requirements to know which entity conducted the identity proofing.

1.48 Chapter 3 of this Schedule covers the specific requirements that must be met by a participating accredited identity service provider. This includes the sub-requirements for technical integration and data requirements.

1.49 Chapter 4 of this Schedule covers specific requirements that must be met by a participating accredited attribute service provider. This includes the sub-requirements for technical integration, audit logging and attribute schema.

Schedule 2 – AGDIS OpenID Connect Profile

1.50 This Schedule sets out the OpenID Connect federation protocols which underpin how participants transmit information about authenticated sessions and users within the AGDIS. OpenID Connect is the preferred federation protocol given its relative ease of implementation compared with other protocols.

1.51 Chapter 1 of this Schedule provides the requirements for the OpenID Connect protocol requirements (in the AGDIS context) for a participating accredited identity exchange to implement to be able to facilitate secure digital ID transactions between participating entities. There are 12 sub-sections covering specific requirements for authorisation grant types, client types, client registration, redirect Uniform Resource Identifier (URI), connecting to authorisation servers, grant types, technical relying party profiles, identity exchange provider profiles, entity information, user consents, privacy considerations and security considerations.

1.52 Chapter 2 of this Schedule provides the requirements for the OpenID connect protocol (in the AGDIS context) for a participating accredited identity service provider to be able to facilitate secure digital ID transactions with a client. There are 10 sub-sections covering specific requirements for client types, client registration, redirect URI, client keys, grant types, technical relying party profile, identity provider profile, entity information, privacy requirements and security considerations.

1.53 Chapter 3 of this Schedule provides the requirements for protocol brokering, specifically the OpenID Connect to OpenID Connect brokering mapping and parameters.

1.54 Chapter 4 of this Schedule provides the requirements for attributes that can be made available to participating relying parties, including access restrictions and mapping.

Schedule 3 – AGDIS Attribute Profile

1.55 This Schedule provides the operation of, and policies for, the use of attributes, which are the data transmitted in AGDIS. The structure of the Schedule is broken down into Chapters which articulate requirements for the handling and fulfilment of attributes and system metadata mapped to the AGDIS OpenID Connect Profile in Schedule 2.

1.56 Chapter 1 of this Schedule outlines how attributes and attribute sets are required to operate within the context of the AGDIS. Chapter 1 provides the components of an attribute sharing policy which applies to all participating accredited entities.

1.57 Any attribute or attribute set must be subject to an attribute sharing policy, otherwise it cannot be transmitted within the AGDIS. An attribute sharing policy must outline:

- the attribute or attribute set to which the policy is applied;
- the consent type applied to the attributes;
- the fulfillment requirements;
- the access policy; and
- the data representation.

1.58 Chapter 2 of this Schedule outlines the attribute sharing policy for the foundational attributes used to identify individuals within the AGDIS. In addition, this chapter provides the identity system metadata attributes which do not convey personal information but are essential to core AGDIS functionality – including authentication and identity proofing levels and identifiers used for auditing or transaction purposes.

1.59 Chapter 3 of this Schedule outlines the attributes and attribute sets which may be provided by participating accredited attribute service providers within the AGDIS. A participating accredited identity exchange provider must not provide the attributes under this chapter to participating accredited identity service providers.

1.60 Chapter 4 of this Schedule maps the transmission of attributes and attribute sets in the AGDIS and is essential for the operation of Chapter 2 in this Schedule. Chapter 4 provides the standards for interoperability amongst entities participating in the AGDIS making and fulfilling attribute requests, including metadata attributes. Chapter 4 also assigns the data types for each attribute and attribute set along with its representation.

ATTACHMENT B

Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

Digital ID (AGDIS) Data Standards 2024

The *Digital ID (AGDIS) Data Standards 2024* (the AGDIS Data Standards) is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011.*

Overview of the AGDIS Data Standards

The AGDIS Data Standards is a legislative instrument made by the Minister as the Data Standards Chair under section 99 of the *Digital ID Act 2024* (the Digital ID Act) and in accordance with section 4 of the *Acts Interpretation Act 1901.*

The AGDIS Data Standards is not a disallowable legislative instrument. Therefore, a statement of compatibility with human rights is not required to be prepared under subsection 9(1) of the *Human Rights (Parliamentary Scrutiny) Act 2011* or section 15J of the *Legislation Act 2003*. However, this statement of compatibility has been prepared as a matter of best practice.

The purpose of the AGDIS Data Standards is to support the operation of the Australian Government Digital ID System (AGDIS) established by the Digital ID Act, which aims to provide individuals with secure, convenient, voluntary and inclusive ways to verify their identity for use in online transactions with government and businesses. In particular, the AGDIS Data Standards facilitate and promote trust in the digital ID services provided within the AGDIS by providing:

- technical integration requirements for entities to participate in the AGDIS; and
- technical or design features that entities must have to participate in the AGDIS including how data must be structured to be transmitted across the AGDIS.

Human rights implications

The AGDIS Data Standards engage the following rights:

- The right to protection from arbitrary or unlawful interference with privacy contained in Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR), and also referred to in Article 16 of the *Convention on the Rights of the Child* (CROC) and Article 22 of the *Convention on the Rights of Persons with Disabilities* (CRPD).
- The rights to equality and non-discrimination, contained in Article 26 of the ICCPR and Article 2 of the CROC.

PROTECTION FROM ARBITRARY OR UNLAWFUL INTERFERENCE WITH PRIVACY

Article 17 of the ICCPR prohibits arbitrary or unlawful interference with privacy. It states that:

- No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
- Everyone has the right to the protection of the law against such interference or attacks.

Article 16 of the CROC and Article 22 of the CRPD contain similar rights.

The Digital ID Act requires that accredited entities continue to comply with existing privacy protections in the *Privacy Act 1988* (the Privacy Act) or, for State or Territory entities, their local privacy law. Where a State or Territory accredited entity is not subject to a local privacy law, and wishes to become an accredited identity service provider, the Digital ID Act prescribes that the entity must enter into a binding agreement that would require them to comply with the Australian Privacy Principles. Australian Government agencies that are subject to the Privacy Act are also subject to the privacy governance code. If an accredited entity is not an agency within the meaning of the Privacy Act, the Accreditation Rules requires the entity to comply with the privacy governance code in respect of its DI data environment and accredited services as if it were an agency for the purposes of the code.

The AGDIS Data Standards facilitates how attributes are collected, used and disclosed within the AGDIS. Attributes are defined in section 9 of the Digital ID Act to include personal information about an individual. All attributes (which may include personal information) must be subject to an attribute sharing policy which must outline:

- the attribute or attribute set to which the policy is applied;
- the consent type applied to the attributes;
- the fulfillment requirements;
- the access policy; and
- the data representation.

If an attribute is not subject to an attribute sharing policy in the AGDIS Data Standards, it cannot be transmitted within the AGDIS. An accredited identity exchange provider provides services involving the flow of information between other entities in a digital ID system, notably between a relying party and an identity service provider. Considering its essential role in the AGDIS, a participating identity exchange provider, which must be accredited, has additional obligations including restrictions on what attribute requests it may fulfill, and the provision of user dashboards which allow individuals to:

- view their consumer history;
- manage the express consent they have given; and
- manage participating relying parties.

The obligations with respect to attributes (which may include personal information) are not limited to participating accredited identity exchange providers. The AGDIS Data Standards enhance the privacy of individuals by ensuring attributes are also protected by other participating entities' services in the AGDIS.

There are additional requirements with respect to the collection, use and disclosure of metadata. Metadata are attributes which do not contain personal information; however, it is possible for metadata to be combined with other information to identify an individual. The requirements in the AGDIS Data Standards are proportionate as metadata attributes are essential to the functionality of the AGDIS – including authentication and identity proofing levels and identifiers used for auditing or transaction purposes.

The AGDIS Data Standards promote the growth of, and trust in, digital ID services throughout the economy. The possible impacts on a person's privacy are not arbitrary nor unlawful and are reasonable and proportionate to give effect the objectives of the Digital ID Act.

The AGDIS Data Standards engages the right to protection from arbitrary or unlawful interference with privacy by:

- prescribing standards regarding the collection, use and disclosure of attributes within the AGDIS; and
- expressly requiring entities who participate in the AGDIS to comply with data sharing and privacy constraints prescribed in the Digital ID Act and related legislative instruments.

Blinding requirements

Currently, the identity exchange provided by Services Australia (the Exchange) is the sole participating accredited identity exchange provider in the unlegislated AGDIS and implements a 'double blind' by limiting information sharing in 2 ways:

- the Exchange does not disclose to participating identity service providers the participating relying party services that each user accessed with their digital ID; and
- the Exchange does not disclose to participating relying parties which identity service provider was used to access their service. As there has only been one participating identity service provider it will have been implicit that users must have used myID, previously known as myGovID.

The double blind was implemented in the context of the unlegislated accreditation scheme, establishing a technical barrier to the tracking and profiling of user behaviour across the system in the absence of the legislated privacy safeguards that are now in place. These include section 53 of the Digital ID Act which prohibits data profiling to track online behaviour.

Section 2.2.1 of Schedule 1 of the AGDIS Data Standards allows for a 'single blind' where a participating accredited identity exchange provider:

- must not broker any information about the participating relying party requesting authentication to any of its identity service providers; and
- may inform participating relying parties which participating accredited identity service provider the individual used to authenticate.

The change to a single blind approach in the AGDIS Data Standards seeks to enable improved:

- user experience, such as making it easier to log into myGov with a digital ID;
- fraud detection, as an individual's choice of identity service provider is information which could help agencies such as the Australian Taxation Office to detect and

prevent fraud, particularly in a context where the threat environment is rapidly evolving; and

- private sector participation in the AGDIS, as the single blind would remove a feature that some private sector stakeholders have noted would discourage them from joining as participating relying parties in the future, and some private sector stakeholders may have legal requirements to know which entity conducted the identity proofing.

The shift to a single blind approach would have limited impacts on privacy. The key change is that participating relying parties could be made aware of an individual's choice of participating accredited identity service provider. From commencement, users will have a choice of one provider (myID). As more identity service providers participate in the AGDIS, there is potential for an individual's choice to convey additional information about them. For example, accredited identity service providers may join the AGDIS that are focused on serving particular segments of the community. This potential impact to privacy needs to be balanced against the broader benefits of enabling greater adoption of Digital ID, which allows people to prove their identity without needing to share extensive personal information such as copies of their identity documents.

During consultation on the AGDIS Data Standards, stakeholders acknowledged the potential benefits of adopting a single blind approach but raised concern that modifying a privacy protection – even if it would have limited actual impacts on privacy – could affect public confidence in the privacy safeguards offered by the AGDIS.

To support public confidence that a change to a single blind approach will enable the disclosure of no additional personal information to a participating relying party beyond an individual's choice of identity service provider, additional assurance and transparency requirements are imposed on the Exchange. Under item 2 of the table in rule 2.2 of the Transitional Rules, the Digital ID Regulator is taken to have imposed a condition, for the purposes of subsection 64(2) of the Digital ID Act, on the Exchange's approval to participate in the AGDIS. This condition requires the provider of the Exchange, for any reporting period where it informs a participating relying party which accredited identity service provider an individual used to authenticate, to do the following:

- arrange an independent audit of its functional compliance with the requirement that, if an individual's authentication method is disclosed to a participating relying party, this is limited to disclosing only the name of the identity service provider (as per section 2.2.1.4 and the data representation in Table 30 of Schedule 3 to the AGDIS Data Standards;
- provide the auditor's findings in relation to that reporting period to the Digital ID Regulator within the following reporting period; and
- publish a copy of the independent auditor's report on its website.

The AGDIS Data Standards, in conjunction with this condition, seek to minimise the interference with the right to privacy. Together, these safeguards engage with and support the right to privacy and otherwise ensure the residual privacy impact is reasonable, necessary and proportionate to the objectives of the change to a single blind.

Conclusion on overall compatibility with human rights

The AGDIS Data Standards is compatible with human rights because they promote the protection of human rights and, to the extent that it may limit human rights, those limitations are reasonable, necessary and proportionate.

Senator the Hon Katy Gallagher, Minister for Finance