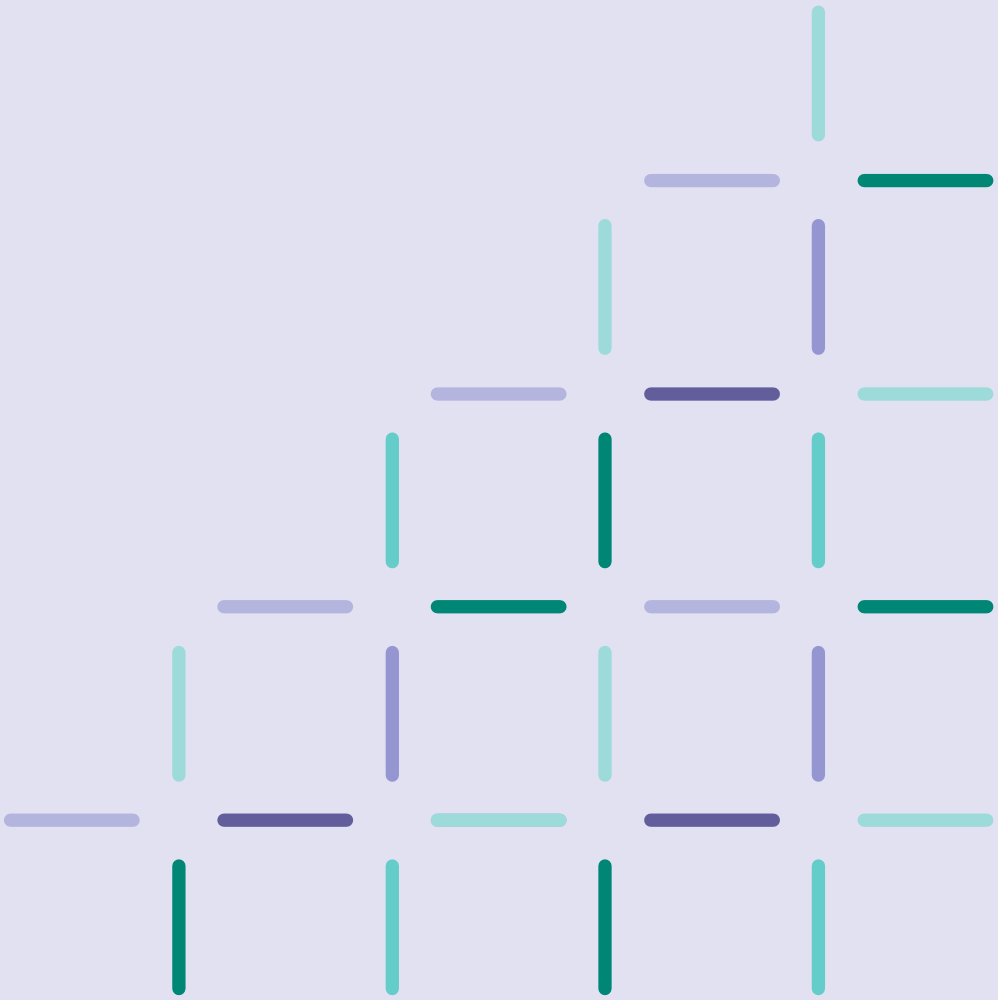
Australian Government

Australia's Digital ID System



31 July 2025

AGDIS System Administrator Data Sharing Principles

System Administrator
Australian Government Digital ID System (AGDIS)

digitalidsystem.gov.au

Contents

1 Purpose and requesting information

The Data Sharing Principles (the Principles) describe:

- the relevant data element(s) collected and retained by the System Administrator for the purposes of performing its powers and functions under the *Digital ID Act 2024* (the Act)
- the purpose for which the System Administrator stores and discloses data collected and retained, or requests data with/from:
    - Participating Entities,
    - The Digital ID Regulator as represented by the Australian Competition and Consumer Commission (**ACCC**),
    - The Information Commissioner as represented by the Office of the Australian Information Commissioner (**OAIC**),
    - The Data Standards Chair (DSC) and the Data Standards Body (DSB)
    - Courts or Tribunals
    - Law Enforcement Agencies, and
    - The Minister for Finance (the Minister).

Schedule A describes the sharing of information with Participating Entities for the purposes of ensuring the safe and effective operation of the Australian Government Digital ID System (AGDIS).

Schedule B describes the sharing of information by the System Administrator to the Digital ID Regulator, the Information Commissioner, the Minister and the Digital ID Data Standards Chair for the purpose of effective governance and operation of the AGDIS.

Schedule C describes the sharing of information with law enforcement agencies for the purposes of enforcement related activities conducted in relation to digital ID fraud incidents and cyber security incidents.

Schedule D describes the data required by the System Administrator to effectively fulfill its purpose of effective operation and monitoring performance of the AGDIS under the Act.

The intent of these Principles is not to duplicate the purpose or processes outlined in ways of working documents such as the onboarding process or the compliance, referral and reporting strategy. It is intended to provide transparency in how data is shared.

1.1 Requests for information to the System Administrator

All requests for information to the System Administrator will be assessed to ensure the disclosure of the information aligns with the Act, the *Digital ID Rules 2024* (the Rules), the *Digital ID (Accreditation) Rules 2024* (the Accreditation Rules), the *Privacy Act 1988* (the Privacy Act), and the Australian Privacy Principles (the APPs).

Supporting the safe and effective operation of the AGDIS under the Act, decisions about the disclosure and release of information will include, if applicable, a written note in the ADGIS Administrator Portal (the Portal). Entities that do not have Portal access and are not included in the Data Sharing Schedules, must use the Information Request Form to submit a request.

Note: these Principles are distinct and not intended to replace the notification obligations detailed in Chapter 4 of the *Digital ID Rules 2024.*

How to make requests for information to the System Administrator

Requests for information to the System Administrator should be made in accordance with Schedule A for participating entities, and Schedule B for regulatory agencies.

1.2 Attributes of an individual

As per s 10 of the Act, an attribute of an individual is information that is associated with the individual (and includes information that is derived from another attribute). For example, the individual's email address, biometric information of the individual, the time and date an individual's Digital ID was created, or a restricted attribute. Restricted attributes of an individual are defined in s 11 of the Act.

The System Administrator may collect the attributes of an individual from Participating Entities for the purposes of performing its functions under the Act and as reflected in 4.1 of the Reference Matrix.

The attributes of an individual may be shared with the Digital ID Regulator and the Information Commissioner to perform their duties and functions, or exercise powers, under the Act.

All requests for attributes of an individual should be in writing and will be assessed to ensure the sharing of this information complies with the Privacy Act, the APP's, Rule 4.5 of the Rules and, ss 95(i), 151–152 of the Act.

In instances where the attributes of an individual are disclosed, a written note of the use and disclosure will be created in the Portal (if applicable).

2 Background and operating context

2.1 Background

The AGDIS is a simple, safe and secure way for Australians to create and use their digital ID. The System Administrator is responsible for protecting the integrity and performance of the AGDIS, including identifying and monitoring operational risks and reporting suspected matters of participating entity non-compliance against the relevant Acts or Rules to the Digital ID Regulator, and the Information Commissioner where required.

2.2 Operating context

Effective governance is essential to the efficient operation of, and instilling public trust and confidence in, the AGDIS. The System Administrator is responsible for the safe operation of the AGDIS, and their powers and functions are conferred on the Chief Executive Centrelink (within the meaning of the *Human Services (Centrelink) Act 1997*). Exercising powers may include collecting or requesting information on matters within or relating to the AGDIS, to fulfill the functions detailed in s 95 of the Act.

2.3 Digital ID legislative framework

Underpinning the AGDIS is the Act, the Rules, the *Digital ID (AGDIS) Data Standards 2024* (the Data Standards), *the Digital ID (Accreditation) Rules 2024* (the Accreditation Rules), the *Digital ID* (*Accreditation) Data Standards 2024* (the Accreditation Data Standards), the *Digital ID (Transitional and Consequential Provisions) Act 2024* (the Transitional and Consequential Provisions Act) and the *Digital ID (Transitional and Consequential Provisions) Rules 2024* (the Transitional and Consequential Provisions Rules).

The Act ensures effective governance and regulation of the AGDIS through the appointment of a Digital ID Regulator, the ACCC.

The Rules set the requirements for the provision of digital ID services. They also make sure all digital ID services meet rules and standards for usability, accessibility, privacy protection, security, risk management, fraud control and more.

These permanent governance arrangements aim to give users confidence that privacy and consumer safeguards enshrined in the legislation are strictly enforced.

3 Types of data attributes collected, stored and disclosed

The reference matrix below identifies entities from which the System Administrator may collect, store, or share data elements, including data attributes, under section 95 of the Act. This is for the purposes of responding to and managing cyber security incidents, digital ID fraud incidents, change enablement, user support and complaints, IT system incidents, and joining the AGDIS.

This matrix links to tables in sections *3.2 Global Data Collection* and *3.3 Activity-specific data collection*, that outline the data elements the System Administrator collects, stores and may disclose to data sharing recipients to enable them to perform their duties and functions, or exercise powers, under the Act.

For details on how and when data elements may be disclosed to data sharing recipients, please refer to Schedules A–C in this document.

3.1 Reference Matrix

Matrix 1 – Data Sharing Recipients of the System Administrator

Data Sharing Recipient Name	Legend
Participating Entities: • Identity Service Providers (ISPs) • Attribute Service Providers (APs) • Participating Relying Parties (PRPs) • Identity Exchange Providers (IXPs)	**A**
Digital ID Regulator	**B**
Information Commissioner	**C**
Data Standards Chair (DSC) and Data Standards Body (DSB)	**D**
Minister	**E**
Law enforcement	**F**

Matrix 2 – Purpose and Digital ID Act 2024 Reference

Functions of the System Administrator	Legislative Authority
Provide assistance to entities participating in the Australian Government Digital ID System, including in relation to connecting to, and dealing with incidents involving, the system	**s 95(a)**
Facilitate and monitor the use of the Australian Government Digital ID System for testing purposes, in accordance with any requirements specified in the Digital ID Rules	**s 95(b)**
Monitor and manage the availability of the Australian Government Digital ID System, including by coordinating system changes and outages and by ensuring that changes made by entities that are participating in the Australian Government Digital ID System do not adversely affect the system as a whole	**s 95(c)**
Identify and manage operational risks relating to the performance and integrity of the Australian Government Digital ID System	**s 95(d)**
Manage digital ID fraud incidents and cyber security incidents involving entities participating in the Australian Government Digital ID System	**s 95(e)**
Advise the following, either on its own initiative or on request, on matters relating to the operation of the Australian Government Digital ID System: **(i).** the Minister; **(ii).** the Digital ID Regulator; **(iii).** the Digital ID Data Standards Chair.	**s 95(f)**
Advise the Information Commissioner, either on its own initiative or on request, on privacy matters that relate to the Australian Government Digital ID System	**s 95(g)**
Report to the Minister, on request, on the performance of the System Administrator's functions, and the exercise of the System Administrator's powers, under this Act	**s 95(h)**
Share information with the following, to assist them to exercise their powers or perform their functions under the Act: **(i).** the Minister; **(ii).** the Digital ID Regulator; **(iii).** the Digital ID Data Standards Chair; **(iv).** the Information Commissioner	**s 95(i)**
Such other functions as are conferred on the System Administrator by this Act or any other law of the Commonwealth	**s 95(j)**

Do anything that is incidental or conducive to the performance of any of the above functions.	**s 95(k)**

3.2 Global Data Elements

The table below identifies global data elements the System Administrator collects, stores and may disclose to data sharing recipients, for the purposes of responding to and managing cyber security incidents, digital ID fraud incidents, change enablement, user support and complaints, IT system incidents and joining the AGDIS.

Global data points are shared data points in the Portal across change enablement, digital ID fraud incidents, cyber security incidents, IT system incidents (ITSI), onboarding configuration and Registration of Interest, Relationship Authorisation Manager RAM) and users.

Global Data Elements

Data Element Name	Data Element Description	Data Sharing Recipients	Legislative Authority
Participating Entity Service	Name of the participating entity service	A, B, C, D, E, F	**s 95(a), s 95(c), s 95(e)**
Organisation Name	Legal name of the entity that owns the service	A, B, C, D, E, F	**s 95(c), s 95(e)**
Participating Entity Role	Participant entity's service role in AGDIS e.g. Identity Service Provider/Participating Relying Party	A, B, C, D, E, F	**s 95(c), s 95(e)**
Participating Entity ID	A unique identifier assigned to each participating entity's service record	A, B, C, D, E, F	**s 95(a), s 95(c), s 95(e)**
Participating Entity Record Status	Whether the participating entity's record is active or inactive	A, B, C, D, E, F	**s 95(a), s 95(c), s 95(e)**
Applicable Application	This field identifies the application the service has access to in the Portal. i.e. fraud and cyber or ITSI	A, B	**s 95(a), s 95(c), s 95(e)**
Contact Person Name	Contact for the participating entity	A, B, C, D, E, F	**s 95(a), s 95(b)**
Contact Officer Phone Number	Contact number for participating entity contact person/point	A, B	**s 95(a), s 95(b)**
Identity Service Provider	Identity Service Providers (ISPs) are accredited entities that create, maintain and manage trusted identity information of other entities and offer identity-based services. An ISP carries out identity proofing and/or identity information verification	A, B, C, D, E, F	**s 95(c), s 95(e)**
Relying Party	Relying Party (RP) is not directly connected to the AGDIS. An RP relies on an attribute of an individual that is provided by the AGDIS via a Participating Relying Party (PRP)	A, B, C, D, E, F	**s 95(c), s 95(e)**
Identity Exchange	Identity Exchange acts like a switchboard facilitating all digital ID interactions between AGDIS systems and PRP services	A, B, C, D, E, F	**s 95(c), s 95(e)**
Organisation Details	Participating entity details (role, name, contact details)	A, B, C, D, E, F	**s 95(a), s 95(c), s 95(e)**
Key identifier	Identifier created by the Digital ID Regulator and referred to by the Digital ID Regulator and System Administrator in communications between them	B	**s 95(a), s 95(f), s 95(i)**

3.3 Activity-specific Data Elements

The table below identifies activity-specific data elements the System Administrator collects, stores and may disclose to data attribute recipients, for the purposes of responding to and managing cyber security incidents, digital ID fraud incidents, change enablement, user support and complaints, IT system incidents and joining the AGDIS.

Activity-specific data elements are unique data elements in the Portal.

Change Enablement Data Elements

Data Element Name	Data Element Description	Data Sharing Recipients	Legislative Authority
Change ID	A unique identifier that identifies a change record	A, B	**s 95(e)**
Change Type	Description of the type of change i.e.: standard/normal/major/emergency	A, B	**s 95(e)**
Change Type	Description of the type of change i.e.: standard/normal/major/emergency	A, B	**s 95(e)**
Change Status	The current status in the change itself as opposed to the record workflow	A, B	**s 95(e)**
Date/time Created	Date/time change notification was created in the Portal	A, B	**s 95(e)**
Category	Short non-technical summary of change	A, B	**s 95(e)**
Environment Type	The environment which the proposed change occurs, i.e.: AGDIS/testing (previously known as production/non-production)	A, B	**s 95(e)**
Proposed Release Date/Time (AEST)	The date/time the change is proposed to go ahead	A, B	**s 95(e)**
Change/project Name	Title given to a change	A, B	**s 95(e)**
Does This Change Have the Potential to Cause any System Outage?	Notifying participating entity service assesses potential change impact on system availability	A, B	**s 95(e)**
Does This Change Have the Potential to Cause any System Outage?	Notifying participating entity service assesses potential change impact on system availability	A, B	**s 95(e)**
Change/Project Summary Description	Notifying participating entity service describes the change and the effect on the system from proposed change and intended outcomes	A, B	**s 95(e)**
Planned Outage Start Date/time (AEST)	Start date/time of planned outage	A, B	**s 95(e)**
Planned Outage finish Date/time (AEST)	Finish date/time of planned outage	A, B	**s 95(e)**
File Attachment	Additional data attached as supplementary files to support a proposed change	A, B	**s 95(e)**
Third Party Approvals Required	If third party approvals are required before the change can be implemented	A, B	**s 95(e)**

Change Enablement Data Elements

Data Element Name	Data Element Description	Data Sharing Recipients	Legislative Authority
Third Party Approval Decision	Who made the decision and what the outcome was	A, B	**s 95(e)**
Pre-Release Start Date/Time (AEST)	Start date/time of planned change window	A, B	**s 95(e)**
Pre-Release Finish Date/Time (AEST)	End date/time of planned change window	A, B	**s 95(e)**
Components of the system impacted	Identification of impacted components to the system	A, B	**s 95(e)**
Release Description	Change details and brief description of the changes	A, B	**s 95(e)**
Comm ID	Unique identifier that identifies an external communication	A, B	**s 95(e)**
Is There a Planned Outage Associated with this Release?	This field is for the participating entity to notify the System Administrator If there is an outage that will affect other participating entities	A, B	**s 95(e)**
Outage Start Date/Time (AEST)	Start time of the planned outage	A, B	**s 95(e)**
Outage End Date/Time (AEST)	End time of the planned outage	A, B	**s 95(e)**
Did this change go ahead?	Confirmation if the change proceeded as planned	A, B	**s 95(e)**
Post-Release Start Date/Time (AEST)	Start date/time of when the change occurred	A, B	**s 95(e)**
Post-Release End Date/Time (AEST)	End date/time of when the change was completed	A, B	**s 95(e)**
BVT Start Date/Time (AEST)	Business verification testing start date/time	A, B	**s 95(e)**
BVT End Date/Time (AEST)	Business verification testing end date/time	A, B	**s 95(e)**
Was the change successful?	Change successful: Yes/No	A, B	**s 95(e)**
Were there affected participating entities, digital ID users or systems?	Were there any affected participating entity services, digital ID users or systems	A, B	**s 95(e)**
Was there an outage?	Identifying if an outage occurred because of the change	A, B	**s 95(e)**
Actual Outage Start Date/Time (AEST)	Date/time of when the outage began	A, B	**s 95(e)**
Actual Outage End Date/Time (AEST)	Date/time of when the outage finished	A, B	**s 95(e)**
Is a Post Change Review (PCR) Required?	A PCR is used to evaluate the effectiveness and outcomes of a change after it has been implemented	A, B	**s 95(e)**

Data Element Name	Data Element Description	Data Sharing Recipients	Legislative Authority
Is An Emergency Change Required?	An emergency change is a change that needs to be implemented immediately (such as resolving a Major Incident)	A, B	**s 95(e)**
Close Reason	Reason why a change was closed	A, B	**s 95(e)**
Service Level Commitment (SLC) Met	If the SLC was met: Yes/No	A, B	**s 95(e)**

Digital ID Fraud and Cyber Security Incident Response Data Elements

Data Element Name	Data Element Description	Data Sharing Recipients	Legislative Authority
Incident ID	System generated unique identifier for an incident	A, B, C, D, E, F	**s 95(c), s 95(e)**
Date/Time Incident Created (AEST)	Date/time a participating entity created the incident in the Portal	B	**s 95(e)**
Date/Time Incident Submitted (AEST)	Date/time a participating entity submitted the incident in the Portal	A, B, C, D, E, F	**s 95(c), s 95(e)**
SLC Met?	Were the service levels met by the notifying participating entity: Yes or No	A, B	**s 95(e)**
Incident Status	Current stage of incident	B	**s 95(e)**
Participant Service	Identifies the notifying participating entity	A, B, C, D, E, F	**s 95(c), s 95(e)**
Incident Summary	High-level incident summary of what occurred	A, B, C, D, E, F	**s 95(c), s 95(e)**
Date/Time of Incident (AEST)	Date/time when a specific incident occurred	A, B, C, E, F	**s 95(c), s 95(e)**
Date/Time of Detection (AEST)	Date/time the incident was detected by the notifying participating entity	A, B, C, E, F	**s 95(c), s 95(e)**
Time taken to respond to the Incident	Total time taken to respond to a specific incident once identified	B, C	**s 95(e)**
Incident Severity Level	Self-assessed by the notifying participating entity, level of impact to the victimised individual and organisation	B	**s 95(e)**
Incident Category	Fraud or cyber event	A, B, C, D, E, F	**s 95(e)**
Method/Source of Detection	Method of identification of a fraud or cyber security incident	A, B, C, D, E, F	**s 95(e)**
Incident Type	The type of fraud or cyber incident e.g. unauthorised assumed identity, phishing campaign	A, B, C, D, E, F	**s 95(e)**
Actions/measures taken in response to the incident and when were these taken	What actions were undertaken by the notifying participating entity in response to the incident	A, B, C, D, E, F	**s 95(e)**
Has the incident been referred to the AFP or the relevant authority?	Referral to the Australian Federal Police or other relevant authority	A, B, C, E, F	**s 95(e)**

Data Element Name	Data Element Description	Data Sharing Recipients	Legislative Authority
Description	Description of a specific digital ID incident Note: This data field may contain PII and will only be disclosed in accordance with the Act and APPs.	A, B, F	**s 95(e)**
Impacted Identity ID	Portal generated identifier number	B	**s 95(e)**
Link Value	Unique RP or ISP pairwise identifier	A	**s 95(e)**
Lift Double Blind Decision	The System Administrator's decision to lift/not lift the double blind.	A, B, C, E, F	**s 95(e)**
Search Start Date	Start date requested to search for transactions	A	**s 95(e)**
File Attachment	Additional data attached as supplementary files to support the incident or event	A, B, C, E, F	**s 95(e)**
Date Identity Created	Date digital ID created	A, B, C, E, F	**s 95(e)**
Identity Proofing Level	The Digital ID (Accreditation) Rules 2024identity proofing level applicable to a specific digital ID	A, B, C, D, E, F	**s 95(e)**
Linked Email Address	Email address used to create the digital ID	A, B, C	**s 95(e)**
Credential Level	The Digital ID (Accreditation) Rules 2024 credential level applicable to a specific digital ID	A, B, C	**s 95(e)**
Date Suspended	Date the digital ID was suspended	A, B, C	**s 95(e)**
Date re-proofed	Date a specific digital ID is reproofed to the same or higher proofing level	A, B, C	**s 95(e)**
Date re-verified	Date a specific digital ID credential (CL) is re-verified and reset	A, B, C	**s 95(e)**
Victim Name	Name of the individual who has been victimised/compromised	A, B, C, F	**s 95(e)**
Victim primary contact number	Trusted contact telephone number of an individual victimised digital ID user	A, B, C, F	**s 95(e)**
Victim secondary contact number	Trusted secondary contact telephone number of an individual victimised digital ID user	A, B, C, F	**s 95(e)**
Date victim contacted	Date participating entity contacted an individual victimised digital ID user after the discovery of the incident	A, B, C, F	**s 95(e)**
Date support services provided to victim	Date support provided to an individual victimised digital ID user	A, B, C, F	**s 95(e)**
Type of support services a victim receives	Type of support provided to an individual victimised digital ID user e.g. IDCARE	A, B, C, F	**s 95(e)**
Date/time stamp of digital ID verification and transaction identifiers	Date/time of the initial and subsequent digital ID verification, provided to the Identity Exchange by the relevant Identity Service Provider	A, B, C	**s 95(e)**
Relying Party/s receiving information user has consented to share	Participating Relying Parties who consumed the digital ID	A, B, C, D	**s 95(e)**

Data Element Name	Data Element Description	Data Sharing Recipients	Legislative Authority
Identity Service Provider pairwise identifier	A unique identifier for every interaction between an Identity Service Provider and an identity exchange	A, B, C	**s 95(e)**
Relying Party pairwise identifier	A unique identifier that identifies a specific participating relying party account linked to a digital ID	A, B, C	**s 95(e)**

IT System Incidents (ITSI) Data Elements

Data Element Name	Data Element Description	Data Sharing Recipients	Legislative Authority
Date/Time of Incident AEST	This is the date and time the incident first occurred	A, B, D	**s 95(c)**
System Incident ID	A unique identifier used to track and manage ITSI related incidents	A, B, D	**s 95(c)**
System Incident Title	A brief title for the issue: e.g. Digital Identity unavailable	A, B, D	**s 95(c)**
Incident Owner(s)	The best-placed entity to diagnose and resolve the issue	A, B, D	**s 95(c)**
Priority	Incident priority level (P-1, P-2, P3, P-4)	A, B, D	**s 95(c)**
Incident Manager	A responsible officer within the System Administrator for overseeing and managing incidents	A, B, D	**s 95(c)**
System Incident Status	The status of an incident (e.g. In-progress, closed, open)	A, B, D	**s 95(c)**
Notification SLA Met	Whether the initial reporting of an incident was within service level timeframes **Note**: Notification SLA currently refers to Operational Standards established by the System Administrator.	A, B	**s 95(c)**
Recovery Time Objective (RTO) Met	Service level showing whether the timeframe to restore business process, after an incident or outage, has been met	A, B	**s 95(c)**

Onboarding Configuration Data Elements

Data Element Name	Data Element Description	Data Sharing Recipients	Legislative Authority
Identity proofing level(s)	Minimum identity level required by the participating entity's service	A, B	**s 95(a)**
Business attributes	Requires RAM to allow users to act on behalf of a participating entity's service	A, B	**s 95(a)**
Restricted attributes	Minimum attributes required for access to a participating entity's service i.e. DOB	A, B	**s 95(a)**
Alternative access pathways	Other methods of accessing a participating entity's service in accordance with s 74 of the Act, i.e. by phone, person	A, B	**s 95(a)**
Minimum identify proofing level required for accessing service	Minimum identity proofing (IP) level an individual user needs to access a participating entity's service, i.e. IP1, IP2, IP3	A, B	**s 95(a)**

Data Element Name	Data Element Description	Data Sharing Recipients	Legislative Authority
Monthly user base growth	Statistics and growth figures of potential users	A, B	**s 95(a), s 95(c)**
Daily authentications	Number of people accessing Service on Start up	A, B	**s 95(a), s 95(c)**
Daily authorisations	Number of daily RAM Authorisations at launch	A, B	**s 95(a), s 95(c)**
Daily registrations	Number of new users daily setting up DI for first time	A, B	**s 95(a), s 95(c)**
Peak periods	Dates/Times of most usage predicted	A, B	**s 95(a), s 95(c)**
Testing Commencement Date	Start date of technical integration of a participating entity's service	A, B	**s 95(a), s 95(b)**
AGDIS Participation Commencement	Start date within the AGDIS for user base (Go Live)	A, B	**s 95(a)**
Connection type	What type of connection Is required, i.e. Service or Enterprise (Brokerage)	A, B	**s 95(a)**
For enterprise connections only	Type of connection required to connect to the Identity Exchange i.e. Open ID Service Provider	A, B	**s 95(a)**
OpenID Connect details	URI'S and URL	A, B	**s 95(a)**

RAM Data Elements

Data Element Name	Data Element Description	Data Sharing Recipients	Legislative Authority
RAM website	Services published on RAM Website	A, B, RAM	**s 95(a)**
myID website	Service published on myID website	A, B	**s 95(a)**
ID / URL	Service provider ID/Entity ID URL	A, B	**s 95(a)**
RAM Service provider ID	Required for service name change	A, B	**s 95(a)**
Previous Service Name	Service name change	A, B	**s 95(a)**
Previous organisation ABN	Other ABN that services has held	A, B	**s 95(a)**
New Service Name	New name of service	A, B	**s 95(a)**
New organisation name (agency legal name)	Legal name of organisation	A, B	**s 95(a)**
New organisation ABN	New ABN for service	A, B	**s 95(a)**

Users Data Elements

Data Element Name	Data Element Description	Data Sharing Recipients	Legislative Authority
Contacts of Service	Contact details of persons responsible for service portfolios that impacts users of the AGDIS	A, B	**s 95(a)**

Onboarding ROI Data Elements

Data Element Name	Data Element Description	Data Sharing Recipients	Legislative Authority
Entity name (legal name)	Name of entity that owns the service as per the Australian Business register	A, B	**s 95(a)**
Entity ABN	Australian Business Number registered to entity	A, B	**s 95(a)**
Existing AGDIS entity	Current type of entity participating in the AGDIS, i.e. PRP, ISP	A, B	**s 95(a)**
Participation type	The type of entity role being requested, i.e. Participating Relying Party, Attribute Service Provider, etc.	A, B	**s 95(a)**
Type of testing required	Testing required under s81 of the Digital ID Act 2024	A, B	**s 95(a), s 95(b)**
Guidance material read and understood	Acknowledgement of Digital ID website, prerequisite reading and understanding of AGDIS	A, B	**s 95(a)**
Service Name	Name that the service will be known as	A, B	**s 95(a)**
Service Description	Overview of what the service will provide	A, B	**s 95(a)**

4 Data Sharing Schedules

4.1 Schedule A – Data sharing with participating entities

Schedule A describes the disclosure of information by the System Administrator to participating entities for the purposes of ensuring the safe and effective operation of the AGDIS. These entities are listed in Matrix 1.

Triggering events

A triggering event is a specific occurrence or condition that initiates a particular action or response. For example, a digital ID triggering event may include the creation of a digital ID using stolen or manipulated identity documents, a digital ID being compromised by a third party, or the creation of multiple digital IDs for dishonest purposes.

Entities must notify the System Administrator of a triggering event through the Portal, where relevant information can also be requested, before the System Administrator can disclose any information. Identified information will be assessed by the System Administrator to ensure it complies with the Act, the Privacy Act and the APP's before disclosing it to the entity through

the Portal. The System Administrator will also ensure the information being disclosed does not exceed the parameters of the original request.

Lifting the double blind

Where entities identify an event that requires information or data relevant to these Principles, the System Administrator will assess the event, as reported by the entity, and lift the double blind where one of the following applies:

1. Information is needed from entities to investigate suspected fraud or assist with enforcement.
2. Information regarding known fraud needs to be shared with other entities.
3. The AGDIS (or a component) is subject to a cyber security incident that cannot be managed without lifting the double blind.

4.2 Schedule B – Data sharing for exercising powers and functions

The System Administrator collects information to manage system-wide matters affecting stability, reliability, and integrity of the AGDIS as well as overarching reporting and audit requirements.

As per Matrix 1 in Section 3.1, the System Administrator can share information with the Minister, the Regulator, the Data Standards Chair, the Data Standards Body and the Information Commissioner. This includes reporting, accreditation of entities, notifiable data breaches, compliance and enforcement related activity, as well as joining the ADGIS.

The System Administrator will share information as required which will provide oversight on the operation and performance of the AGDIS.

Requests for information to the System Administrator

Any request for information required by regulatory agencies, that is not covered by existing reports or falls outside of the regular cadence, must be made using the Information Request Form included at the end of this document.

A request for information will be acknowledged within 2 business days and a response provided, including a nil response, within 10 business days.

4.3 Schedule C – Data sharing with law enforcement

Where an enforcement body, as defined by Section 6 of the *Privacy Act 1988,* requires personal information under these Principles for a permitted enforcement related activity, they may request that information from the System Administrator. Enforcement bodies may contact the System Administrator at AGDIS.Administrator@servicesaustralia.gov.au for advice.

The System Administrator will disclose personal information to an enforcement body in limited circumstances. The System Administrator will generally redirect the enforcement body to the relevant accredited entity.

For the purposes of the Act, law enforcement agency has the same meaning as in the *Australian Crime Commission Act 2002.*

Circumstances where the use or disclosure of personal information that is not biometric information for enforcement purposes is permitted:

- Personal information (that is not biometric information)

- A warrant issued under a law of the Commonwealth, State or Territory; or
- Reporting a digital ID fraud or cyber security incident (suspected or actual); or
- Express consent for verifying identity or investigating/prosecuting an offence; or
- Complying with the Digital ID Act 2024; or
- Proceedings started against a person (for an offence or certain breaches).

4.4 Schedule D – Data sharing with the System Administrator by other regulatory bodies

All communication between the System Administrator, the Digital ID Regulator (noted as 'B' in the table below) and the Information Commissioner (noted as 'C' in the table below) will be conducted via email. An Application Program Interface (API) between the Digital ID Regulator and the System Administrator will be implemented in the future and will reduce the need for email. The System Administrator's Business Continuity Plan will include email post-implementation of the API.

The following table outlines information required from the Digital ID Regulator and/or the Information Commissioner for the System Administrator to perform its functions. The triggering events that require this information to be shared include but are not limited to:

- Approval of entities/services
- Accreditation of entities, including annual reviews
- Decisions to vary, suspend or revoke approval or conditions, including initial notification and final decision, whether that be Regulator, Minister or participating entity initiated
- Changes to entity information including Machinery of Government changes
- Show cause notices where consultation or validation from the System Administrator is required
- An accredited entity is making a system change as part of an accreditation review process (not already notified to the System Administrator)
- Requests for information from other regulatory agencies
- Compliance and enforcement related activity
- Notifiable data breaches.

Data shared with the System Administrator by other regulatory agencies

Data Collected	Description of Data Collected	Who	Legislative Authority
Date of decision	Specific date a formal decision is made and documented.	B	**s 95(a), (d), (f), (i)**
Date of effect (e.g. participation start/variation date)	Specific date when a particular action, decision or measure becomes operational or enforceable.	B	**s 95(a), (b), (d), (f), (i)**
Organisation name	Participating entity's service name e.g. Digital ID exchange, myGov	B, C	**s 95(a), (b), (d), (f), (g), (i)**
Trading service name	Customer-facing name	B, C	**s 95(a), (b), (d), (f), (g), (i)**
Provider type	If they are an Identity Service Provider, Identity Exchange Provider or Attribute Service Provider	B	**s 95(a), (b), (d), (f), (i)**
Reference number	Internal ACCC reference number	B	**s 95(a), (b), (d), (f), (i)**
Key identifier	Identifier created by the Digital ID Regulator and referred to by the Digital ID Regulator and System Administrator in communications between them	B	**s 95(a), (b), (d), (f), (i)**

Data Collected	Description of Data Collected	Who	Legislative Authority
Connection type	Whether this is a service connection (individual service) or enterprise connection (through an enterprise authentication solution)	B	**s 95(a), (b), (d), (f), (i)**
Conditions / exemptions imposed	High-level description of conditions and/or exemptions that may be imposed on the participating entity	B	**s 95(a), (b), (d), (f), (i)**
High-level reasons an entity has failed requirements of application, or withdrawn application, and application can't proceed, or application has been denied.	Reason why the application cannot proceed because the entity has either failed to meet the requirements or has withdrawn the application, resulting in its denial	B	**s 95(a), (b), (d), (f), (i)**
High-level reason of variation / suspension / revocation	Reason why a variation, suspension or revocation has been imposed on a participating entity	B	**s 95(a), (b), (d), (f), (i)**
High-level reason/description of action required for show cause notice	Reason or description of action required to be taken by a participating entity because of the show cause notice	B	**s 95(a), (b), (d), (f), (i)**
Reason for request	Brief summary of why the Digital ID Regulator is requesting action be taken in relation to the show cause notice	B	**s 95(a), (b), (d), (f), (i)**
Date of change (includes IT change or change to participating entity's information)	The date/time the change is proposed to go ahead (if change is in the future) or the date/time the change occurred	B	**s 95(a) - (f), (i)**
Summary of change (includes IT change or change to participating entity's information)	Summary of what the change activity entails	B	**s 95(a) - (f), (i)**
Type of change (IT change)	Description of the type of change i.e. standard / normal / major / emergency	B	**s 95(a) - (f), (i)**
Description of data breach	Summary of how the data breach occurred, who was impacted and when it occurred	C	**s 95(a) - (g)**
Information involved in data breach	Information at risk because of the data breach	C	**s 95(a) - (g)**
Recommended actions to be taken in response to data breach	Summary of actions to be taken by a participating entity in response to a data breach **Note**: This is limited to relevant information that the OAIC may provide, if appropriate, on a case by case basis in accordance with s33A of the Privacy Act/relevant legislative information sharing provisions	C	**s 95(a) - (g)**

5 Document information

Change history

The System Administrator maintains this document in electronic form. It is the responsibility of the user to verify that this copy is the latest revision.

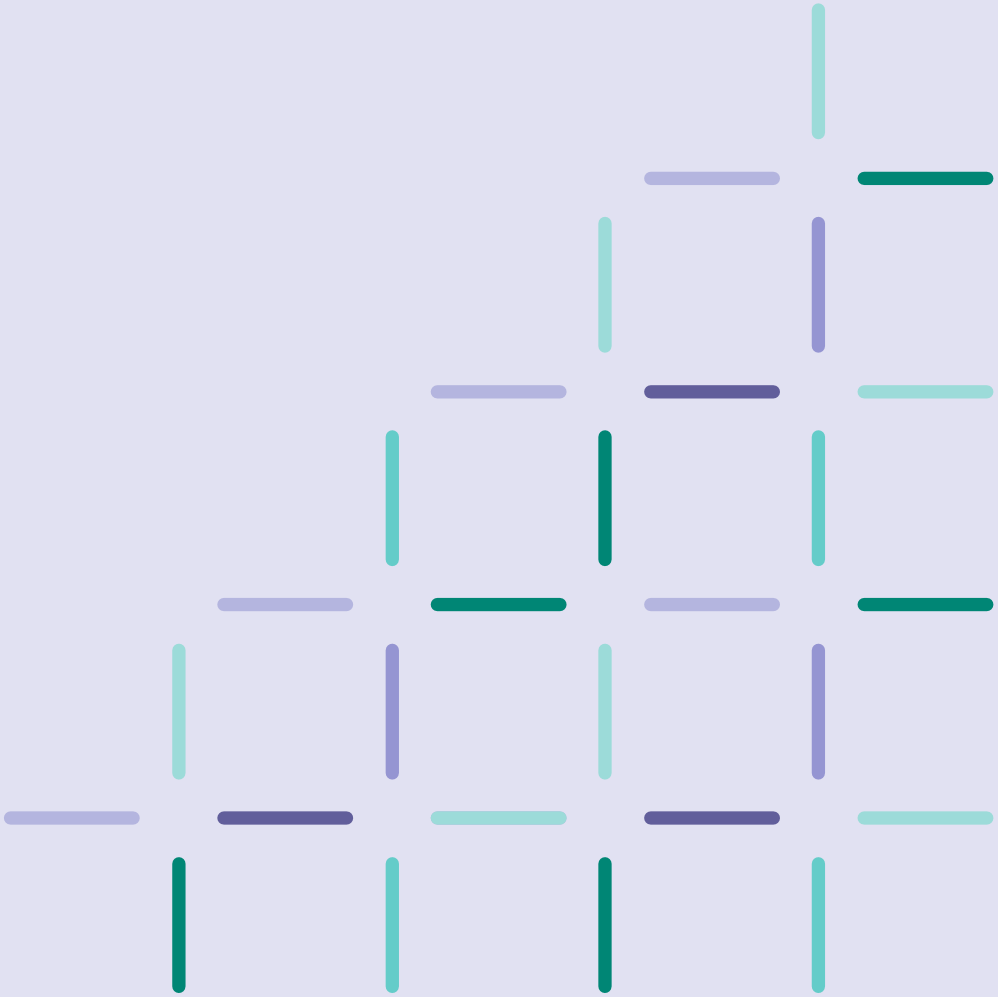
Version	Date Last Revised	Author	Change Description
1	19 November 2024	JO	Final version approved for publishing
2	25 July 2025	JO	Minor updates including formatting

Endorsement

Version	Date	Approved by (name, position)
1	19 November 2024	JH, Director, Office of the System Administrator
2	31 July 2025	JH, Director, Office of the System Administrator

Australian Government

Australia's Digital ID System



Information Request Form

System Administrator
Australian Government Digital ID System (AGDIS)

digitalidsystem.gov.au

Information Request Form

Please complete all fields below and email the completed form to AGDIS.Administrator@servicesaustralia.gov.au[1].

Entity details

Department/agency name:	
Requesting officer name:	
Contact email address:	
Contact phone number:	

Information request details

Does this information request require the System Administrator to disclose any personal attributes of an individual as defined in sections 10 and 11 of the Digital ID Act 2024 (see the following page for the relevant sections of the Act)[2]?	**Yes** ☐ **No** ☐

Clearly describe the information you are requesting. Explain why you need it, how you will use it, and provide the legislative authority that supports your request:

[1] The System Administrator will aim to acknowledge the request within 2 business days of receipt and provide a response, including a nil response, within 10 business days of receipt.
[2] If yes, the System Administrator will assess this request to ensure the disclosure of information complies with the Digital ID Act 2024, the Digital ID Rules 2024, the Privacy Act 1988 and the Australian Privacy Principles.