Australian Government
Office of the National Data Commissioner

ONDC

DATA Scheme Accreditation

Establishing entity credentials and the ONDC assessment process

July 2025

Accreditation in the DATA Scheme

The Data Availability and Transparency Act (DATA) Scheme is underpinned by four key safeguards to ensure safe sharing of data under the Scheme.

Accreditation	Authorisations	Privacy Protections	National Data Commissioner
Only accredited entities can access Scheme data	Only authorised people can agree to data sharing	Supplements Privacy Act	Independent regulator

DATA Scheme Requirements

All accredited entities

All accredited entities must:

Have appropriate data management and governance:

- ✓ Policies
- ✓ Practices
- ✓ Responsible individual

Minimise risk of unauthorised:

- ✓ Access
- ✓ Sharing
- ✓ Loss

Have necessary skills and capabilities for:

- ✓ Privacy
- ✓ Protection
- ✓ Appropriate use

DATA Scheme Requirements

Accredited Data Service Providers

In addition, ADSPs must have:

The necessary:

- ✓ **Policies**
- ✓ **Practices**
- ✓ **Skills**
- ✓ **Capabilities**

To perform any, or all, of the data service:

- ★ De-identification services
- ★ Secure access data services
- ★ Complex data integration

Design of the Accreditation Framework

The ONDC:

Reviewed other accreditation, registration and user/researcher schemes.

Referenced the Commonwealth Accredited Integrating Authority program.

Obtained expert technical advice – Australian Bureau of Statistics, Australian Institute of Health and Welfare, Australian Cyber Security Centre, Digital Transformation Agency, Dept of Finance, IT industry adviser.

Set up the National Data Advisory Committee (including the Australian Statistician, the Information Commissioner, Australia's Chief Scientist and at least 5 other members) to advise the National Data Commissioner.

Consulted with data custodian and user organisations.

Reviewed the accreditation framework twice, through an internal audit and an external IT / Cyber security expert to ensure it has appropriate controls and safeguards in place and complies with the requirement of the Act.

Expected Characteristics

Accredited User

In undertaking an assessment, the ONDC looks at:

Data management and governance policies and practices, and a qualified individual

- Identified roles responsible for data; ICT including security; and personal information.
- Governance bodies responsible for data management, governance and use; data risks; and audit.
- Policies and practices, roles, responsibilities and processes for managing and governing data.
- An indication of how the organisation will manage and govern the entity's DATA Scheme responsibilities and obligations.

Minimise the risk of unauthorised access, sharing or loss of data

- Identified roles responsible for the organisation's security.
- Governance bodies responsible for physical, ICT and data security governance.
- Policies and practices, roles, responsibilities and processes for managing and governing physical, ICT and data security.
- Controls for Scheme data.
- Workforce governance addresses personnel risks to data.

Skills and capability to ensure the privacy, protection and appropriate use of data, including risks

- Identified data specialist roles, including data analyst and data manager or data policy/governance.
- Policies and practices that support data skills and capability, including mandatory training on data responsibility, security awareness and privacy.
- Training for staff about the DATA Scheme.

Expected Characteristics

Accredited Data Service Provider

In undertaking an assessment, the ONDC looks at:

The same expected characteristics as for users, but with greater focus on the safeguards associated with complex data services.

Plus:

- Policies and practices for the provision of services.
- Skills and capabilities for the provision of services.
- Documentation, processes, and guidance to support the services.

Accreditation and Australian Privacy Principles

In undertaking an assessment, the ONDC looks at information related to the Australian Privacy Principles (APPs) such as:

Accreditation assesses whether entities have public privacy policies, and procedures to request personal information and make privacy complaints.	APP 1: Open and transparent management of personal information APP 12: Access to personal information APP 13: Correction of personal information
Accreditation assesses whether an entity is capable of appropriately using personal information. DATA Scheme information cannot be used for enforcement.	APP 6: Use or disclosure of personal information
DAT Act requires personal information to be stored in Australia.	APP 8: Cross-border disclosure of personal information
Accreditation assesses security, access controls, data breach response.	APP 11: Security of personal information

Cyber and IT Security

Security frameworks

- Protective Security Policy Framework
- Information Security Manual / Essential Eight
- International Standards Organisation 27001
- National Institute of Standards and Technology

Prefer Infosec Registered Assessors Program (IRAP), or other external IT audit

Secure storage

- Prefer provider in Home Affairs Hosting Certification Framework
- Otherwise assess on premises or other hosting provider

Responsibility and oversight

- Chief Information Officer, Chief Information Security Officer / IT Security Advisor
- IT security committee
- Governance, skilled people, and policies are in place to ensure accountability, responsibility and oversight

Environmental and Gateway Controls

- Access control for users and administrators
- Activity monitoring and auditability
- Secure data transfer
- Encryption of data in transit and at rest
- Separation of identifying and content data
- Output vetting controls and capability
- Disclosure risk management
- Personnel checks
- Data responsibility training

Accreditation Framework and Alignment with the National Data Principles

Project principle	• governance bodies and roles that oversight data use in general and the use of Scheme data • policies and procedures for managing data and associated risks • plans to manage data, privacy and cyber security incidents
People principle	• policies and practices that ensure staff have the right data skills • workforce vetting practices e.g. police and reference checks • training in data responsibilities including privacy and cyber security

Setting principle	• IT and cyber security policies and strategies
	• IT governance roles and bodies
	• application of IT security frameworks and reviews/audits against these
	• status of environments that host Scheme data
	  ○ protected or
	  ○ equivalent to managing 'official sensitive' public sector data
	• access controls to identify and limit access to individuals

Data principle	• identifying specialist data roles • skills and capabilities to use data appropriately
Output principle	• skills and capabilities that prevent misuse of Scheme data • training in data responsibilities including privacy • ability to apply Scheme requirements in using data

ONDC Assessment Process

The team

A small but experienced ONDC Accreditation team is supported by a range of experts, internal and external, including:

- Senior Data advisors
- Cyber Security Advisors
- Information Technology Security Advisors
- The Office of the Australian Information Commissioner

Assessment process

1. Pre-assessment check application is valid
2. Assessment against expected characteristics
3. Identification of any gaps in information or clarifications required
4. Requests for further information
5. Site visit for ADSP assessments
6. Internal and legal review
7. Final assessment against legislative criteria and recommendation to the National Data Commissioner, including any recommendations to impose conditions on accreditation.

Assessment considerations

- Assessors discuss any issues with applicants.
- The approaches that entities take in data management and governance, protections and skills and capabilities may differ depending on functions, size and other characteristics of the organisation.
- ONDC assessment takes all information into account to determine whether it is appropriate in all the circumstances to accredit the entity.

Accredited Entity Accreditation Profiles

Entity profiles for ADSPs are in development and will be published on Dataplace.

These profiles will provide information from the ADSPs on:

- the services they provide,
- their data management, governance and personnel,
- adherence to data sharing principles and industry recognised IT standards,
- data security; and
- the key policies, practices, skills, IT systems and capabilities the entity has against each specific data service they are accredited to provide.

More Information

Accreditation Information

More information about accreditation, including the benefits and how to get accredited.

https://www.datacommissioner.gov.au/request-data

User Accreditation Expected Characteristics

https://www.datacommissioner.gov.au/node/186

User Accreditation Application Checklist

https://www.datacommissioner.gov.au/node/271

Sample User Accreditation Form

https://www.datacommissioner.gov.au/node/273

DATA Scheme Guidance and Info Sessions

Public resources and registration links to our monthly webinars.

www.datacommissioner.gov.au/resources

Contact the ONDC

information@datacommissioner.gov.au

https://www.datacommissioner.gov.au/contact-us

Follow us on LinkedIn for data news

@Office of the National Data Commissioner