Accredited Data Service Provider (ADSP) Application Form

To lodge an application for ADSP accreditation under the Data Availability and Transparency Act (DATA) Scheme, go to [Dataplace](http://www.dataplace.gov.au).

Responses to the questions in the *ADSP Application Form* are designed to obtain evidence relevant to the Data Availability and Transparency Act 2022 (the Act).

This form is to be used in conjunction with the:

* [Evidence Guidance for ADSP applications](https://www.dataplace.gov.au/assets/Evidence%20Guidance%20for%20ADSP%20applications.pdf); and
* [Instructions for making an ADSP application](https://www.dataplace.gov.au/assets/Instructions%20for%20making%20an%20ADSP%20application.pdf).

## About your Organisation and Data Services

1. Organisation name and email/s for general enquiries.

*1.1 Response:*

Organisation Name:

Type of entity:

ABN /ACN:

Legal name of the organisation:

Email address/es for general enquiries:

1. Authorised officer: the application must be submitted by an authorised officer.

*1.2 Response:*

First Name:

Last Name:

Preferred name:

Email:

Phone:

Position title:

1. ADSP application co-ordinator (contact officer).

*1.3 Response:*

First Name:

Last Name:

Preferred name:

Email:

Phone:

Position title:

1. Does your organisation intend to provide all data services under the DATA Scheme (de-identification data services, secure access data services, complex data integration data services)
OR
Is the application being made for accreditation with a condition to exclude one or more data services under the DATA Scheme?

*1.4 Response:*

My organisation is intending to provide:

[ ]  ALL data services (de-identification data services, secure access data services, AND complex data integration data service)

OR

My organisation is NOT intending to provide:

[ ]  de-identification data services

[ ]  secure access data services

[ ]  complex data integration data services

1. Provide a detailed description of your organisation’s data services under the DATA Scheme.
	1. *Response:*
2. Tell us about your organisation’s legal structure, including details relevant to your data services. For example:
* whether your organisation constitutes a separate legal entity (e.g. a state government department)
* whether your data services will be provided by unit within the legal entity, e.g. a research institute within a university
	+ if a government body, identify the Group or Division providing the services.
	1. *Response:*
1. Outline any conflicts of interest (perceived, real or potential) your organisation has, related to providing data services under the DATA Scheme, including contractual commitments.
	1. *Response:*
2. Does your organisation have any obligations or affiliations that could impact or conflict with obligations under the Act should your organisation become accredited? Outline these obligations or affiliations and how you will manage these matters.
	1. *Response:*
3. Are there any legislated functions or restrictions or protections that are specific to how your organisation will undertake data activities?
	1. *Response:*

## Data Management and Governance

* 1. What data governance policies, and practices does your organisation have in place, including any data governance bodies or groups?
	How do these policies align to the data services your organisation would provide under the DATA Scheme?

*2.1 Response:*

* 1. Tell us about the corporate roles in your organisation that have responsibility of data governance and the implementing data policies and practices.

Who is the person chiefly responsible for data management and data governance?

For the area that providing data services, include details of the person chiefly responsible for data governance in that unit.

*2.2 Response:*

* 1. What is your organisation’s approach to risk management, and how are data issues monitored and managed under that approach?

*2.3 Response:*

* 1. What audit and review processes does your organisation have in place (internal and external) relating to current and on-going management of data?

*2.4 Response:*

* 1. Tell us how your organisation will demonstrate public transparency of your data activities and operations, including transparency of processes for data access, confidentialisation, publication or release of data.

*2.5 Response:*

* 1. What are the communication channels your organisation has in place, for the lodgement of complaints or stakeholder contact?

What arrangements does your organisation have, or will put in place, for responding to enquiries from the National Data Commissioner?

*2.6 Response:*

## Privacy and Data Protection

* 1. Tell us about the privacy obligations that apply to your organisation.

How will your organisation apply these privacy obligations under the DATA Scheme, including but not limited to any of the following that may apply:

* + the Commonwealth *Privacy Act 1988;*
	+ State or Territory privacy laws; and
	+ circumstances where you may have the Australian Privacy Principles (APP)-equivalence term in a data sharing agreement.

*3.1 Response:*

* 1. Outline your organisation’s privacy policy, privacy risk management plan and supporting policies and practices, including:
	+ privacy governance processes;
	+ breach and complaints processes; and
	+ how privacy risks are mitigated.

How will these policies and practices apply to the data services you intend to provide?

*3.2 Response:*

* 1. Tell us about the roles within your organisation that have responsibility over privacy obligations and practices.
	Who is the organisation corporate/enterprise level person chiefly responsible?

Who is the person chiefly responsible in the area providing data services?

*3.3 Response:*

* 1. What policies and practices does your organisation use to ensure its data activities are ethical? Please provide details where your organisation uses ethics committees.

*3.4 Response:*

* 1. Tell us about how your organisation ensures that personnel are aware of their privacy and data protection responsibilities and consequences of non-compliance.

*3.5 Response:*

* 1. Tell us about how your organisation ensures personnel involved in providing data services are made aware of their responsibilities handling sensitive information, including personal information.
	How are these responsibilities reflected in the culture of your organisation?

*3.6 Response:*

* 1. Tell us about how your organisation manages customer use of de-identified information and ensures all customers of data services are:
		+ aware of their responsibilities when accessing or handling information; and
		+ managed and monitored when accessing information.

Include your policy, procedures and/or examples of information for customer use.

*3.7 Response:*

## Security Settings

1. Tell us about the security framework/s your organisation has been assessed against, and indicate:
	* + - * when the last assessment was undertaken; and
				* the scope of the assessment, for example a secure access unit or systems used for complex data integration.

*4.1 Response:*

1. Tell us where your organisation’s personnel are located and provide evidence that your DATA Scheme services will be performed or operated only within Australia.
If any part of your data services will be hosted by another organisation or another unit in your organisation, including a cloud service provider, tell us about your hosting arrangement/s.

*4.2 Response:*

1. Tell us about the security roles in your organisation, including corporate role/s such as Chief Information Security Officer, and how these roles provide leadership and oversight of security including cyber in providing data services.

*4.3 Response:*

1. Outline your organisation’s network management policies and activities that ensure:
* secure network design and configuration;
* secure wireless networks; and
* service continuity for online services.

*4.4 Response:*

1. Outline your organisation’s data storage system management policies and processes that apply to delivering data services and that ensure secure management of:
* database servers;
* database management system software; and
* databases and other storage or file systems.

*4.5 Response:*

1. Tell us about your organisation’s security plan, manual, policy or similar documents, including information on:
* risks, threats and vulnerabilities that impact the protection of people;
* information and assets, security goals and strategic objectives;
* tolerance to security risks, assessment of maturity to manage security risks; and
* strategies to implement security risk management and maintain a positive risk culture.

*4.6 Response:*

1. Tell us about your organisation’s software development policies and guidelines on a secure and consistent approach to application development including web application development.

*4.7 Response:*

1. Tell us about your organisation’s ICT equipment and media management policies and practices to ensure their controlled and secure usage.

*4.8 Response:*

1. Outline your organisation’s controls to ensure mobile devices are securely managed and used appropriately.

*4.9 Response:*

1. Tell us about your organisation’s vetting processes or assessment when/if outsourcing information technology services.

*4.10 Response:*

1. Tell us about your organisation’s policies and practices for system hardening, including operating systems, application and authentication processes.

*4.11 Response:*

1. Outline your organisation’s system management policies and guidelines around:
* secure system administration;
* system patching; and
* change management.

*4.12 Response:*

1. Tell us about your organisation’s data transfer policies and procedures.

*4.13 Response:*

1. Outline your organisation’s data encryption policies and procedures and their application in mitigating threats during the ingress and egress of data.

*4.14 Response:*

1. Outline how your organisation achieves gateway monitoring for data movement into and out of your systems.

*4.15 Response:*

1. Outline your organisation’s system management policies and guidelines for data backup and restoration.

*4.16 Response:*

1. Outline your organisation’s personnel security controls including:
* ensuring individuals understand their security responsibilities and receive security awareness training including cyber security;
* individuals have access to only what is required to do their job; and
* methods to identify and authenticate personnel.

*4.17 Response:*

1. Outline your organisation’s physical controls to ensure the security of:
* ICT equipment;
* wireless devices; and
* facilities containing systems, servers, communications, security containers, network infrastructure and devices, and work spaces.

*4.18 Response:*

1. Outline your organisation’s system monitoring policies and analysis procedures and reporting for:
* ongoing event logging;
* incident analysis; and
* auditing and review of logs.

*4.19 Response:*

1. Outline your organisation’s protocols, policies and practices to:
* detect, manage, recover and report from security events/ incidents including cyber; and
* respond and action security events/incidents including cyber in a timely manner.

*4.20 Response:*

## Skills and Capabilities

* 1. Tell us about the experience the area providing the data service has had with access to government data or provided data services to government in Australia or internationally.

*5.1 Response:*

* 1. Outline your organisation’s data management policies and practices for the data services your organisation could provide.

*5.2 Response:*

* 1. Outline the key operational data roles, responsibilities and accountabilities, specific to each data service your organisation could provide.

*5.3 Response:*

* 1. Tell us about your organisation’s capability requirements, performance expectations and recruitment processes for data staff.

*5.4 Response:*

* 1. Tell us about how your organisation will implement learning, development or training about the DATA Scheme for:
	+ staff; and
	+ customers.

*5.5 Response:*

* 1. Outline your organisation’s metadata standards, classifications and/or interoperability policies and practices.

*5.6 Response:*

* 1. Tell us about your organisation’s data quality assessment policies and practices, including how these mitigate risk of misuse of data.

*5.7 Response:*

* 1. Tell us about the policies, practices and roles your organisation has that support your technical skills and capabilities to meet the requirements of Data Sharing Agreements (DSAs) that relate to the role of an ADSP.

*5.8 Response:*

* 1. Tell us about your experience adjusting settings, controls and constraints that will be relevant to meeting future requirements of Data Sharing Agreements.

*5.9 Response:*

* 1. Outline your organisation’s capability to provide data integration services, including:
* previous experience; and
* personnel skills and capability.

*5.10 Response:*

* 1. Outline your organisation’s data integration policies and practices.

*5.11 Response:*

* 1. How is the separation principle applied in your organisation’s data integration structures and operations?

*5.12 Response:*

* 1. Tell us about your organisation’s experience providing secure access data services.

*5.13 Response:*

* 1. Tell us about your organisation’s arrangements in providing secure access data service user support and training, including how users/researchers will interact with the data in your environment.

*5.14 Response:*

* 1. Tell us about your organisation’s data minimisation practices demonstrating your ability to apply this capability in data sharing projects.

*5.15 Response:*

* 1. Tell us about your organisation’s policies, practices and experience treating data to manage disclosure risk.

*5.16 Response:*

## Consent and declaration

This section is mandatory before the application can be submitted.

Only the authorised officer may submit this application.

I consent to the Commissioner and, if the Minister is the accreditation authority for this application, the Minister, and any person assisting with assessing this application, including any person acting as a delegate of the Commissioner or the Minister:

* obtaining information relevant to this application from third parties, and
* verifying information with third parties in support of this application.

I declare that:

* I am an authorised officer of the Applicant and have authority to make this application on behalf of the Applicant, in accordance with section 76 and 137 of the *Data Availability and Transparency Act 2022*.
* Information provided in this application, including any attachments, is correct.
* Individuals have consented for their personal information to be included in this application.
* I understand that the Applicant will be required to comply with the obligations of an accredited data service provider and any conditions of accreditation that may be imposed by the accreditation authority, if accredited under the *Data Availability and Transparency Act 2022*.

NOTE

It is a serious criminal offence under the Commonwealth *Criminal Code* to knowingly provide false or misleading information to a person exercising a function under any law of the Commonwealth, including the *Data Availability and Transparency Act 2022*. Providing false or misleading information in an application (including any omission of a matter without which the information is misleading) may also be grounds to suspend or cancel any accreditation granted on the basis of that information.

## Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Date: \_\_\_\_/\_\_\_\_/\_\_\_\_\_\_\_