



Australian Government

Department of the Prime Minister and Cabinet

Office of the National Data Commissioner

# Accreditation Framework

Discussion Paper



## **Accreditation Framework Discussion Paper**

© Commonwealth of Australia 2020

### **Copyright Notice**

With the exception of the Commonwealth Coat of Arms, this work is licensed under a Creative Commons Attribution 4.0 International licence (CC BY 4.0)(<https://creativecommons.org/licenses/by/4.0/>).



### **Third party copyright**

Wherever a third party holds copyright in this material, the copyright remains with that party. Their permission may be required to use the material. Please contact them directly.

### **Attribution**

This publication should be attributed as follows:

© Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Accreditation Framework Discussion Paper*

### **Use of the Coat of Arms**

The terms under which the Coat of Arms can be used are detailed on the following website:

<https://www.pmc.gov.au/government/commonwealth-coat-arms>

### **Other uses**

Enquiries regarding this document are welcome at:

<https://www.datacommissioner.gov.au/form/contact>

# Contents

---

1. Introduction.....	1
1.1. What we heard.....	1
1.2. Review of existing accreditation schemes .....	2
2. Proposed Framework.....	3
2.1. Legal framework .....	4
2.2. Types of accreditation .....	5
2.2.1. Accredited User.....	6
2.2.2. Accredited Data Service Providers.....	7
3. Accreditation Criteria .....	9
3.1. Governance and administrative frameworks.....	9
3.2. Arrangements for security and privacy of data .....	10
3.2.1. Privacy coverage.....	10
3.3. Technical skills and capability.....	11
3.4. Additional requirements for Data Service Providers .....	11
4. Accreditation Process.....	12
4.1. Apply .....	12
4.2. Assess.....	12
4.3. Decide.....	13
4.4. Maintain.....	13
4.4.1. Obligations under the legislation .....	13
4.4.2. Conditions on accreditation.....	13
4.5. Renew.....	14
4.5.1. Discontinuing accreditation .....	14
5. Other matters.....	15
5.1. Regulation.....	15
5.1.1. Suspension or cancellation of accreditation .....	15
5.2. Registers .....	16
5.3. Fees.....	16
6. Transition Arrangements.....	18
6.1. Accredited Integrating Authority.....	18
7. Next steps .....	19
Appendix 1: Key terms .....	20



# 1. Introduction

Accreditation is an important assurance mechanism for the Data Availability and Transparency Bill. It's the entry point for participation in the data sharing scheme and a safeguard to prevent participants from entering the data sharing scheme who have not been or should not be accredited. Only accredited entities will be able to access public sector data under the legislation.

This data sharing scheme is an alternative pathway to share public sector data where it is currently prevented by secrecy provisions or where arrangements are burdensome and complex. It does not replace or impact existing data sharing arrangements which are working successfully.

Accreditation works together with the Data Sharing Purposes, the Data Sharing Principles and Data Sharing Agreements as safeguards to provide a holistic, robust and safe approach for accessing public sector data. Specifically:

- **Accreditation** will control entry into the data sharing scheme and identify participants' data capability
- The **Data Sharing Purposes** will only allow data to be shared for government service delivery, government policy and program development, and research and development.
- **Data Sharing Principles** apply a holistic risk management framework to safely share data, and
- **Data Sharing Agreements** will specify the agreed arrangements necessary for safe data sharing and will be specific to each project and instance of data sharing.

To enforce these safeguards, the legislation will empower the National Data Commissioner to oversee and regulate the system.

This paper discusses the objectives of accreditation, our proposed framework and how it will work in practice.

Throughout the paper, we ask a number of specific questions for you to consider. We would like to hear your responses to these questions, and encourage you to provide your views on any element of the paper.

Our consultation period runs for eight weeks, and is an opportunity for you to provide formal written submissions to the Office of the National Data Commissioner through [our website](#). Submissions will be due by 6 November 2020.

## 1.1. What we heard

Extensive consultation with key stakeholders highlighted the importance of visibility and transparency of participants in the data sharing scheme, as well as understanding their data capability.

Our proposed approach takes into account the views we have heard so far and has been designed to:

- create a robust and streamlined scheme
- provide a consistent national framework that states and territories could also leverage in future
- ensure every entity in the data sharing scheme is aware of their responsibilities
- ensure the National Data Commissioner can have visibility of every entity in the scheme and impose conditions, as appropriate
- incorporate measures to address privacy considerations
- incorporate measures to manage if things go wrong

- make publicly available information about accredited entities, and
- ensure an equitable and merit-based assessment.

## 1.2. Review of existing accreditation schemes

In designing the proposed framework, we reviewed a number of data access processes of national and international organisations.<sup>1</sup> We also looked at how registration and accreditation works in other sectors, including standards development, education and training, data access and IT security. These schemes presented valuable insights which have informed our approach.

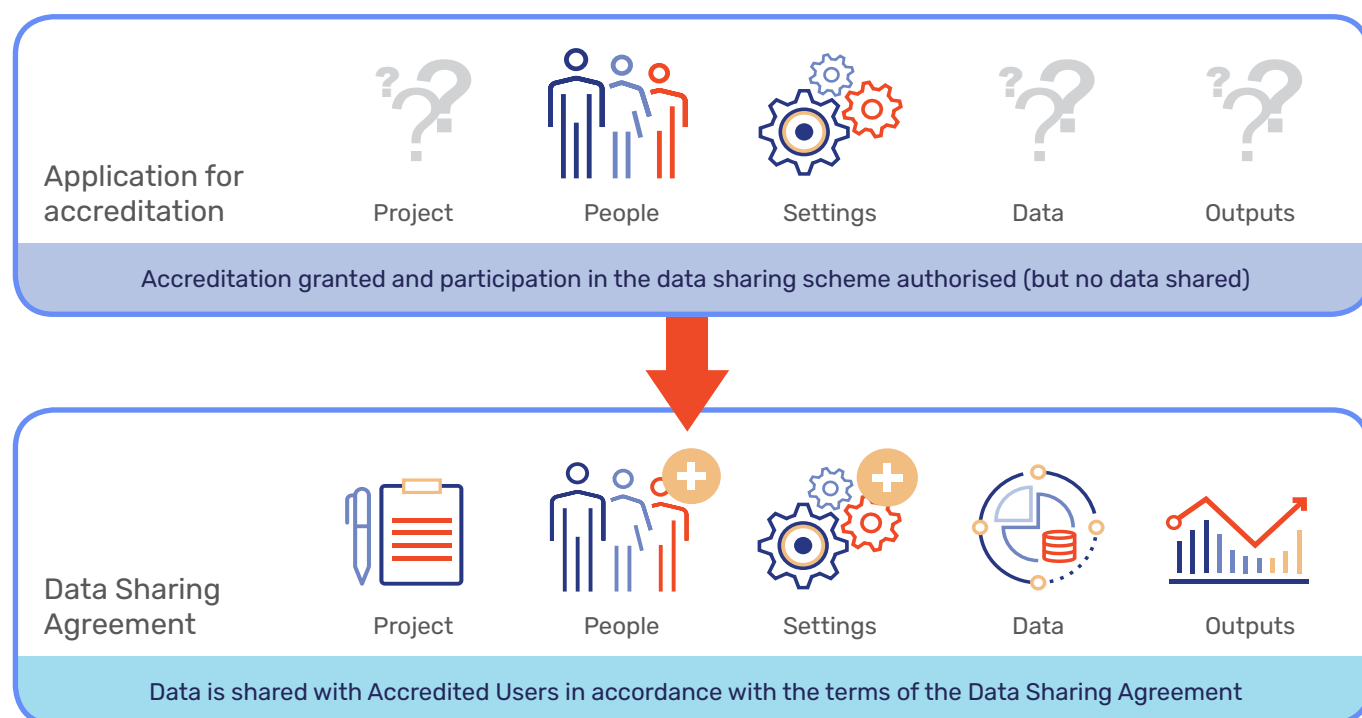
The review also highlighted key differences between models, including ours. Most other schemes accredit users based

on the context of a specific project or proposal.<sup>2</sup> In contrast, our framework will accredit users as part of a general accreditation process, with the ability to apply further controls for specific projects once they have been accredited and are able to access data shared under the scheme (i.e. at the Data Sharing Agreement stage). Figure 1 illustrates this in the context of the Data Sharing Principles.

The benefit of our accreditation approach is that entities only have to seek accreditation once, and then they can use that accreditation to support any number of data requests.

It also supports the legislation's coverage across a broad spectrum of public sector data, ranging from summary tables of statistics to sensitive individual records, and acknowledges the skills and capability of individuals to handle data safely will vary depending on the project.

Figure 1. Limits of accreditation under the Data Availability and Transparency Bill



1 Organisations included the Australian Bureau of Statistics, the Sax Institute, the Office for National Statistics (United Kingdom), Statistics New Zealand, Statistics Canada, Statistics Netherlands, the United States Census Bureau and Eurostat.

2 Ritchie, F and Tava, F 2020, 'Five Safes' or 'One Plus Four Safes'? Musing on project purpose: <https://blogs.uwe.ac.uk/economics-finance/five-safes-or-one-plus-four-safes-musing-on-project-purpose/>

## 2. Proposed Framework

The proposed framework will facilitate participation by data users and data service providers from different sectors (e.g. government, business, academia, think tanks, not-for-profit, etc.) and across a range of data sharing scenarios (e.g. data integration, microdata access, aggregate statistics, etc.).

Accreditation will promote consistency by enabling a streamlined process for entities wanting to access public sector data, specifically, to be accredited once to access data many times. Our approach should also enable the re-use of accreditation information in the data request and Data Sharing Agreement processes that follow. That is, Data Custodians will have access to information about accredited entities and their data capability, before deciding whether and how to share data.

Accreditation has been designed to manage scheme risks and minimise barriers to safe data sharing. The framework will work to prevent:

- **Unauthorised activity**

Accreditation will control entry into the data sharing scheme by verifying the identity of applicants and identifying their data capability. The National Data Commissioner will decide who is accredited, monitor who is participating in the data sharing scheme and regulate their actions, including suspending or cancelling their accreditation.

Accredited entities will be accountable for their data activities under the legislation and must continue to meet the conditions of accreditation to stay accredited.

The National Data Commissioner will also publish information about accredited entities on public registers to promote transparency of the scheme. See *Registers* for further details.

- **Data sharing benefits are not realised**

Accreditation will work to prevent inappropriate participation in the scheme, without being so onerous that genuine users cannot become accredited and actively participate. The accreditation process must be clear and translatable across different sectors and objectively assessable. This will ensure organisations and individuals have a consistent pathway into the data sharing scheme and only need to provide their credentials and capabilities once.<sup>3</sup>

Accreditation should also build trust between Data Custodians and accredited entities. Through the accreditation process, Data Custodians can be assured that accredited entities are who they say they are and have data handling capability. Data Custodians should be able to use the information collected through the accreditation process to support their decision-making about sharing their data.

- **Gaps in regulatory oversight**

Ensuring the National Data Commissioner can identify, monitor and regulate accredited entities is critical for minimising disruptions to the systems that support the operation of the data sharing scheme. Accreditation will apply at the organisation and individual levels to ensure shared accountability

---

<sup>3</sup> Accredited entities are responsible for maintaining their accreditation. This includes providing information to the National Data Commissioner about events and changes in circumstances affecting their accreditation. Failure to do this will be considered a breach of their obligations under the legislation.

for data activities. It will also provide the National Data Commissioner with information on the organisation’s data environment and an individual’s ability to handle data. A scheme-wide view of participants, including sub-units and individuals, will reduce gaps in regulatory oversight that might otherwise exist.

By managing these risks, accreditation strengthens and supports consistency in how the Australian Public Service approaches public sector data sharing and help build public trust.

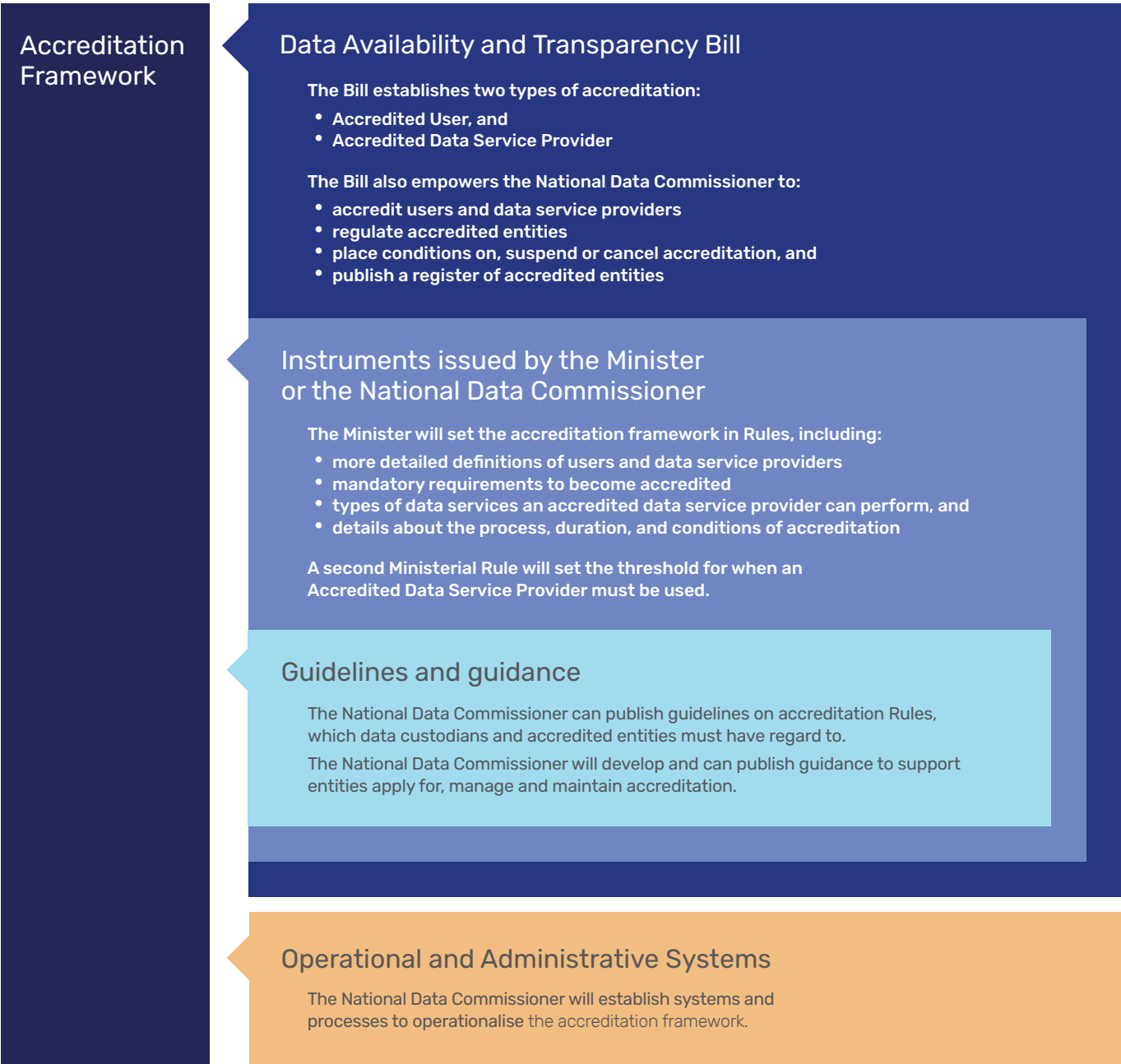
## 2.1. Legal framework

Accreditation will be established through multiple legal mechanisms. Figure 2 lays out how accreditation will operate under each mechanism.

The Data Availability and Transparency Bill establishes two types of accreditation and empowers the National Data Commissioner to accredit entities, regulate their activities and place conditions on, suspend or cancel their accreditation.

The accreditation framework, including detailed definitions of accreditation entities, eligibility criteria and details about

Figure 2. Legal framework for Accreditation





process, duration and conditions of accreditation, will be established in Rules by the responsible Minister and be legally binding.<sup>4</sup> This approach enables the creation of a self-contained system in Rules, which is better suited to contain detailed technical requirements rather than primary legislation, and are subject to Parliamentary oversight. Establishing the framework in Rules will also enable flexibility to respond to technological and environmental changes in the future.

Broadly, the criteria will require applicants to demonstrate they have appropriate data governance and administration frameworks, appropriate arrangements for data security and privacy, and skills and capability to handle data safely. The Rules will also define types of data services an Accredited Data Service Provider can perform. Accreditation will ensure entities are identifiable and capable of handling data in accordance with the legislation's requirements.

The Rules for the accreditation framework will be tabled with Parliament once the legislation has received Royal Assent from the Governor-General, and are subject to disallowance (for a period of 15 sittings days).

To support the accreditation process, the National Data Commissioner will develop and can publish guidance including on:

- how to apply for and maintain accreditation
- how an accreditation application is assessed

- what it means to be accredited, and
- how Data Custodians can use accreditation when considering a data sharing request and/or agreement.

Layering the legal framework for accreditation ensures it is adaptable to future changes while still maintaining enforceable safeguards and penalties.

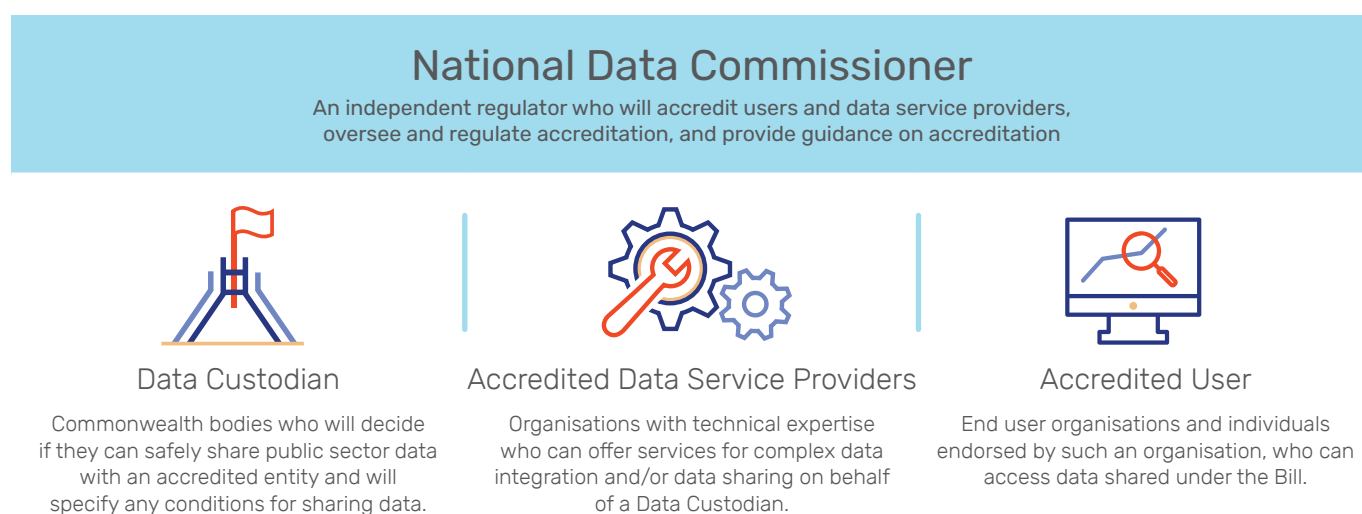
## 2.2. Types of accreditation

The Data Availability and Transparency Bill provides for two types of accreditation – Accredited User and Accredited Data Service Provider.

Figure 3 shows the different roles in the data sharing scheme in the context of accreditation. It is important to note entities can have multiple roles. For example, Data Custodians can apply to be accredited for one or both accreditation roles.

Accredited entities will have ongoing responsibilities when participating in the data sharing scheme. This includes advising the National Data Commissioner of any changes to their circumstances relating to accreditation and meeting any new criteria as the scheme evolves. Failure to do this will be considered a breach of their obligations under the legislation. See *Obligations under the legislation* for further details.

Figure 3. Roles established by the legislation



<sup>4</sup> Ministerial Rules are legislative instruments established to support the parent Act. A Rule is tabled in both the House of Representatives and the Senate and is subject to disallowance. Ministerial Rules will follow the standard disallowance regime, in which a senator or member of the House of Representatives can put forward a motion to disallow (in whole or in part) within 15 sitting days after tabling in Parliament.

### 2.2.1. Accredited User

An **Accredited User** is an organisation, or individual endorsed by such an organisation, who has been accredited to access public sector data under the legislation.

Including both organisations and individuals as Accredited Users promotes shared accountability. Organisations will be accountable for ensuring the right settings are in place to protect, manage and use data accessed under the legislation, including who they endorse for accreditation. Individuals will be accountable for handling the data in accordance with the requirements of the legislation and are liable for their actions if they do not act within the bounds of their professional duties.

This approach provides the National Data Commissioner with the ability to:

- collect information on organisation's governance processes, data handling procedures and technical environment to protect, manage and use data, and
- ensure an individual, acting on behalf an organisation, is aware of their responsibilities when handling data accessed under the legislation.

The National Data Commissioner will have whole-of-scheme visibility, minimising blind spots in the data sharing scheme and strengthening accountability for data activities.

### Organisations

Australian organisations can apply to be an Accredited User. They can be of any size, structure, industry or type<sup>5</sup> but must demonstrate an appropriate level of Australian ownership to be eligible.<sup>6</sup> The application will require supporting information about the organisation's data environment and capabilities. See *Accreditation Criteria* for further details.

For larger organisations, accreditation will recognise sub-units of organisations. For example, schools and departments of universities. The organisation will need to provide information relevant to each sub-unit as part of their application. This approach accounts for variations in

each sub-unit's access to secure data environments, data governance and management practices and privacy and security coverage.

The organisation must nominate a Responsible Officer who has legal authority to act on behalf of the organisation for accreditation purposes to:

- nominate any sub-units within the organisation to be recognised as part of their accreditation coverage
  - endorse individuals for accreditation
  - apply for accreditation, including managing and maintaining their organisation's accreditation status, and
- approve Data Sharing Agreements and be accountable for their organisation's data activities under the legislation.

The Responsible Officer can delegate the authority to endorse individuals, apply for accreditation, and approve Data Sharing Agreements. They cannot delegate authority to nominate sub-units to be recognised as part of their accreditation coverage.

The Responsible Officer will need to declare their understanding of obligations under the legislation as a representative of the organisation (see *Accreditation Process* for more information on obligations).

Typically, the role of a Responsible Officer may be, but is not limited to:

- For government departments: Statutory Head, Secretary of department, Head of Agency or equivalent, as agreed with the Office of the National Data Commissioner.
- For all other organisations: a person who has the same legal responsibility for the actions of the entity as a departmental Secretary does for a government department.

---

5 The legislation outlines how partnerships, unincorporated associations and trusts are handled (Part 6.4 of the Data Availability and Transparency Bill).

6 Classification of what is an appropriate level of ownership is still under development. We will be consulting on this with various agencies to define this concept and will consider the *Foreign Acquisitions and Takeovers Act 1975*.

## Individuals

Individuals must be endorsed by an accredited organisation. An individual may only be endorsed if they are employed by, or acting on behalf of, the accredited organisation and are bound by that organisation's policies and procedures.<sup>7</sup>

In many instances, an individual is dependent on an organisation's data infrastructure and environment to undertake data activities. By linking an individual's accreditation to an organisation, the National Data Commissioner will have a holistic view of an individual's data skills and capabilities as well as the settings they will operate in.

For endorsing organisations, this approach ensures they have oversight of data activities occurring within their environment and balances accountability for such activities appropriately.

The National Data Commissioner will verify an individual's identity, test their understanding of their responsibilities under the legislation and collect other information relevant to their ability to manage, use and protect data appropriately (see *Accreditation Criteria* for more detail).

Individuals can be endorsed by a number of accredited organisations. For example, an independent researcher who is working on multiple projects for an accredited university and an accredited think tank can be endorsed by one or both organisations for accreditation.

## Foreign nationals

Foreign nationals are non-Australian citizens and non-permanent residents and are eligible for accreditation.

Accrediting foreign nationals can encourage the best and brightest minds to solve Australia's policy and research challenges and foster international cooperation. This is particularly beneficial for the Australian research and development sector. Understandably, these benefits must be balanced against risks to Australia's national interests,

including national security. We will be guided by advice from appropriate Commonwealth agencies to ensure any risks are managed appropriately.

Foreign nationals will be assessed as individuals and need to meet the same criteria, including endorsement by an accredited organisation. The National Data Commissioner may request further documentation or seek advice from other regulators or government agencies as part of the assessment process.

If accredited, individuals are liable for their actions if they do not act within the bounds of their professional duties. The endorsing organisation will also be held responsible for the accredited foreign national's activities in the scheme as they would for any other accredited individual.

Through accreditation, the National Data Commissioner will have regulatory oversight of these individuals within Australia and overseas.

### 2.2.2. Accredited Data Service Providers

An **Accredited Data Service Provider** is an organisation that has been accredited as having relevant technical expertise and can offer complex data integration and/or share data on behalf of a Data Custodian.

The [\*Productivity Commission's Data Availability and Use Inquiry\*](#) found there was a gap in data capability across the public sector and that a number of agencies did not have the necessary skills, resources or infrastructure to integrate and share data safely. Organisations with appropriate data capability can be accredited under the scheme to address this capability gap and ensure this type of work is done by those with the right skills.

## Organisations

Australian organisations<sup>8</sup> with technical expertise to undertake complex data integration and/or support secure data sharing, can apply to be an Accredited Data Service Provider.<sup>9</sup>

---

7 In the context of this paper, 'acting on behalf of' refers to an individual, such as a contractor or consultant, who is authorised to perform certain activities or make decisions on behalf of an organisation through the terms of their employment, appointment, or engagement.

8 Classification of what is an appropriate level of ownership is still under development. We will be consulting on this with various agencies to define this concept and will consider the *Foreign Acquisitions and Takeovers Act 1975*.

9 Eligible organisations can be of any size, structure, industry or type. The legislation will outline how partnerships, unincorporated associations and trusts are handled (Part 6.4 of the Data Availability and Transparency Bill).

Initially, we propose to accredit two types of data services:

- **Complex data integration services** involves combining data from two or more sources to create an enriched data asset that may be more sensitive than the individual source data.<sup>10</sup>
- **Data sharing services** involves facilitating secure data sharing or access consistent with terms agreed with the Data Custodian.

This does not impact on current data service provider arrangements (e.g. cloud infrastructure to host data assets). Other data services can continue to be contracted through standard procurement processes.

Data integration can range in complexity and technical difficulty. For complex data integration, it will be mandatory for a Data Custodian to engage an Accredited Data Service Provider to be part of the project. This ensures that projects with elevated risk can be managed by an organisation with qualified technical expertise in handling, analysing and releasing information. For instance, if the risk posed from a data breach would be reasonably likely to result in serious harm to a person, entity (or group of entities), or a thing to which the data relates. Further work is needed to define when it is mandatory to use an Accredited Data Service Provider, and we would welcome your thoughts on this issue.

To be accredited, data service providers must demonstrate they have appropriate governance arrangements, data policies and processes, privacy coverage, technical environment, hiring and vetting practices and sophisticated access logging arrangements (for monitoring and logging of individual access to data). They will also need to nominate a Responsible Officer who has legal authority to act on behalf of the organisation for accreditation purposes.

## Individuals

Individuals employed by or acting on behalf of<sup>11</sup> an Accredited Data Service Provider are likely to routinely undertake more complex data activities such as data integration. These individuals will need specialist data skills to handle data and be subject to stringent hiring, vetting and training practices.

To be accredited, Accredited Data Service Providers will need to demonstrate that their employees, or individuals contracted to act on their behalf to handle data, are highly skilled and appropriately vetted. Responsibility and accountability for ensuring training and vetting processes will rest with the Accredited Data Service Provider.

We welcome views on ways to maintain a robust assurance process while further streamlining the accreditation process.

## Questions:

1. **What is considered to be an appropriate level of Australian ownership for an organisation to be eligible for accreditation?**
2. **Should individuals acting on behalf of an Accredited Data Service Provider be accredited individually? If so, what might be appropriate arrangements?**
3. **Are there circumstances when it should be mandatory to use an Accredited Data Service Provider for a data sharing project?**
4. **What would those circumstances be?**



<sup>10</sup> The Australian Bureau of Statistics 2019, ABS Data Integration: <https://www.abs.gov.au/websitedbs/D3310114.nsf/home/Statistical+Data+Integration>

<sup>11</sup> In the context of this paper, 'acting on behalf of' refers to an individual, such as a contractor or consultant, who is authorised to perform certain activities or make decisions on behalf of an organisation through the terms of their employment, appointment, or engagement.

# 3. Accreditation Criteria

The accreditation criteria will be established in Ministerial Rules and will be based on three categories:

- appropriate governance and administrative arrangements to protect, manage and use data
- arrangements for security and privacy of data to ensure appropriate handling, and technical skills and capabilities to protect, manage and use data.

The responsible Minister can add additional criteria, as appropriate.

The accreditation criteria and the types of considerations that could be taken into account are discussed below. Collection of this information will help determine an organisation or individual's data capabilities, in particular, abilities to keep data safe.

In forming this approach, we recognise that other frameworks, standards and processes may already consider or have assessed elements of these data capabilities. We want to be able to deliver an accreditation process that is robust yet still streamlined. Being able to acknowledge other standards or processes as evidence of a particular area of data capability is one way to do this.

For example, an organisation who has been certified by the Australian Signals Directorate to be a Gateway or Cloud provider, or uses such a certified provider, could use this to demonstrate their ability to safely and securely host data. It means applicants wouldn't have to re-supply evidence and would streamline the accreditation process for all users.

We would like to hear your views on leveraging the use of existing standards or processes to streamline our accreditation framework and which ones might be appropriate to recognise.

Once accredited, entities will have ongoing obligations to maintain their accreditation. This includes providing information to the National Data Commissioner about events and changes in circumstances affecting their accreditation. See *Obligations under the legislation* for more details.

One of the defining characteristics of the Data Availability and Transparency Bill is the creation of a new regulator to oversee data sharing activities under the legislation. The National Data Commissioner will have the power to regularly monitor and investigate accredited entities and can apply civil and criminal penalties for breaches of the legislation. The Commissioner's oversight of accredited entities and their activities will be supported through public registers and Data Sharing Agreements.

## 3.1. Governance and administrative frameworks

Organisations will need to demonstrate they have effective governance and administrative controls in place to support the protection, management and use of data. Key considerations to meet this criteria may include:

- organisational structure, delegations and conflicts of interest
- data management policies and procedures (including privacy policy, roles and training)

- disclosure risk management processes and framework, and
- data governance arrangements including reporting, audit and review, transparency and feedback mechanisms.

Examples of the information an organisation may provide could include, but is not limited to, annual reporting on data activities, ethics approval processes, publication of data policies, adoption of the Data Sharing Principles or Five Safes Framework, work program advisory boards, data user and provider engagement forums, details of employees sanctions or penalties for non-compliance, and complaints and investigations mechanisms.

Individuals will need to provide evidence of endorsement by an accredited organisation and meet the identity requirements. Endorsement can be evidenced through a nomination form submitted by the organisation, which will confirm the individual:

- can act on behalf of the organisation for the purposes of the legislation
- was subject to appropriate pre-employment checks
- has undertaken training related to the organisation's policies and procedures, and
- understands their individual responsibilities as part of the organisation.

## 3.2. Arrangements for security and privacy of data

Organisations will need to demonstrate they have effective security and privacy controls to keep data safe and secure.

Organisations could demonstrate their security arrangements by providing information, for example on:

- Recent assessments or audits against recognised Australian Government (such as the Protective Security Policy Framework) or international standards
- Security policy, roles and incident management processes and frameworks

- Fraud control plans and risk assessments
- Physical security protocols
- Personnel security protocols and training
- ICT equipment and media management practices and frameworks
- Software development controls
- Database and email management practices and frameworks
- System, network and gateway management processes, and
- Data transfer protocols and use of cryptography.

Individuals will need to confirm they have no history of data misconduct and provide details of, relevant qualifications, experience and training. They must also complete and pass the Office of the National Data Commissioner's training to demonstrate they understand their obligations under the legislation.

### 3.2.1. Privacy coverage

The legislation mandates privacy coverage for organisations and individuals who want to access public sector data that involves personal information.

Privacy coverage<sup>12</sup> is demonstrated if an organisation is covered under the Commonwealth *Privacy Act 1988* (the Privacy Act) or a state or territory equivalent that provides:

- a) protection of personal information that is comparable to the Australian Privacy Principles
- b) monitoring of compliance with the law, and
- c) a means of recourse for individuals if their information is handled in a way that is contrary to the law.

Currently, Commonwealth agencies and organisations (including the Australian National University), medium-to-large businesses with an annual turnover of more than \$3 million are covered under the Privacy Act. This coverage extends to individuals who are acting on behalf of the organisation.

<sup>12</sup> Privacy coverage encompasses the three conditions listed as well as a notifiable data breaches scheme. The mechanism to ensure notification for data breaches is covered separately in Part 3.3 of the Data Availability and Transparency Bill.



Additionally, state or territory public sector agencies<sup>13</sup> in New South Wales, Victoria, Queensland, Tasmania, the Australian Capital Territory, and the Northern Territory are covered by equivalent privacy laws. Government agencies in Western Australia and South Australia would need to be prescribed in Regulations of the Privacy Act, to gain an appropriate privacy coverage.

Small businesses, universities, public schools, media organisations and registered political parties are not generally covered by the Privacy Act. However, they can choose to opt-in by completing an opt-in application form and returning it to the Office of the Australian Information Commissioner (OAIC) by mail, email or fax.

Organisations can demonstrate privacy coverage by providing evidence of their legal coverage (as an organisation defined in the Privacy Act or state and territory privacy law or listed on the OAIC register). This may also include providing information about their privacy policy and internal protocols.

### 3.3. Technical skills and capability

Organisations will need to demonstrate they have capability to handle and work with data. This may include providing information on, but is not limited to:

- Data roles and expertise, and recruitment processes, and
- Existing data access arrangements and previous project experience

Individuals can provide evidence of qualifications, experience or training related to data analysis, analytical techniques, or software/languages as well as professional references, awards, published works or association membership.

### 3.4. Additional requirements for Data Service Providers

Data service providers will also need to demonstrate skills in data integration and/or data sharing to be accredited for one or both types of services.

Examples of data integration capability include, but are not limited to, the recruitment of data specialists, details of previous data integration projects, application of the separation principle<sup>14</sup>, data minimisation processes and data integration specific audit and governance processes.

Examples of data sharing capability include, but are not limited to, experience providing safe and secure access to data, processes for vetting users and projects, experience creating microdata files, experience with appropriate de-identification methods, experience providing data laboratory access arrangements (on-site, mobile or remote), user support availability and formal data request processes.

To meet the criteria for an Accredited Data Service Provider, a provider must demonstrate they have effective controls and processes in place to keep data safe and secure (as it is relevant to the service they are performing).

#### Questions:

- .....
- 5. Are there elements of data capability that should be given more or less weight in the accreditation process, i.e. making elements mandatory or optional?**
  - 6. What elements would be most useful to Data Custodians to support their decision-making process when considering sharing and access to data?**
  - 7. Should the accreditation process recognise other frameworks, standards or processes that have assessed an element of data capability? If so what standards/processes might be appropriate to recognise?**
  - 8. Are there any elements of data capability that should be captured in order to understand an accredited entity's ability to keep data safe?**

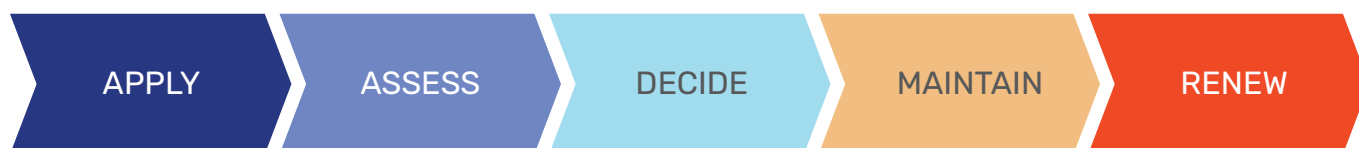
<sup>13</sup> New South Wales, Victoria, Tasmania and Australian Capital Territory privacy legislation also specifies coverage for statutory bodies, local councils, and universities.

<sup>14</sup> National Statistical Service 2020, the Separation Principle: <https://statistical-data-integration.govspace.gov.au/topics/applying-the-separation-principle>

# 4. Accreditation Process

There are five main steps in the accreditation process with further information on each provided below.

Figure 4. Accreditation Process



## 4.1. Apply

To apply for accreditation, an organisation or individual will complete an application form, attach relevant supporting documentation, and submit it to the National Data Commissioner for assessment. Once the application has been received, the applicant will be sent a confirmation notification and provided with details on next steps.

For individuals, this will include completing a training course and passing a test before the National Data Commissioner can finalise their decision. The training course will cover an individual's obligations under the legislation as well as other information regarding its operation and intent.

There are no limits to application attempts. Organisations that can resolve identified issues or uplift in their data capability to meet the criteria, can reapply for accreditation.

## 4.2. Assess

The National Data Commissioner will assess the applicant's claims against the criteria and review the supporting documents.

The National Data Commissioner can seek further information to support the decision-making process. This may occur where there are higher risks, such as foreign interference. Information sought may include, but is not limited to:

- affiliations with other organisations or individuals, particularly international ties
- additional identity documents
- security clearance validations, and
- advice from other government agencies or regulators.



The National Data Commissioner will be supported by staff from their office to assess applications. Any staff working to the National Data Commissioner from the Department of the Prime Minister and Cabinet will not be able to assess applications relating to the Department of the Prime Minister and Cabinet.

## Question:

### 9. What is a reasonable period of time to assess an application?

## 4.3. Decide

Based on the outcome of the application assessment, the National Data Commissioner will make a decision to grant or reject the application. The applicant will be notified in writing about the decision, with reasons and information about review rights.

If the applicant is unsuccessful, they will be able to request a review of the decision or, in some cases, may be able to resubmit a new application (if the application was rejected due to insufficient evidence provided, but can now be provided in a new application process).

If the applicant is successful, information about their accreditation, including the accredited entity's name and contact details will be published on a public register. See *Registers* for further information.

## 4.4. Maintain

To maintain accreditation, accredited entities must:

- continue to meet the criteria
- comply with obligations set in the legislation, and
- comply with conditions set by the National Data Commissioner.

Failure to comply with one or more of the criteria or any additional conditions may lead to a suspension or cancellation of accreditation.

The National Data Commissioner will have oversight of all accredited entities and will monitor and regulate their activities to ensure compliance. See *Regulation* for further details.

## 4.4.1. Obligations under the legislation

Accredited entities have ongoing obligations under the legislation to:

- comply with the mandatory terms of a Data Sharing Agreement
- not use or share data for any purpose that is not outlined in the Data Sharing Agreement
- comply with Data Codes and Rules
- have regard to guidelines operating under the legislation
- maintain coverage under Australian privacy laws (the Privacy Act or a state/territory equivalent)
- not provide false or misleading information
- comply with ongoing conditions of accreditation
- report events and changes in circumstances affecting accreditation to the National Data Commissioner
- provide information to the National Data Commissioner when requested, and
- comply with regulatory measures.

Accredited Data Service Providers will have additional obligations to:

- ensure data sharing activity is authorised by the legislation, where sharing data is on behalf of the Data Custodian
- ensure delivery of data services as agreed with the Data Custodian
- maintain infrastructure, capability, governance and policy, consistent with any conditions associated with accreditation or Data Sharing Agreements, and
- ensure individuals are also compliant with ongoing conditions of accreditation.

## 4.4.2. Conditions on accreditation

The National Data Commissioner can set conditions on any accredited organisation or individual to manage risks and maintain the integrity of the data sharing scheme. For example, where there is a serious or deliberate breach of the legislation by an individual, the National Data

Commissioner can apply conditions on both the individual and the organisation to mitigate or prevent further breaches and/or as a penalty. Failure to comply with conditions can lead to a suspension or cancellation of accreditation.

Conditions can relate to limiting access to data under the legislation or imposing additional criteria to maintain accreditation. Conditions may reflect new standards or processes that come into play over time. For example, the National Data Commissioner may require an organisation to handle data in accordance with a particular encryption standard, if introduced.

The National Data Commissioner can also place limits on the types or scope of data an individual is authorised to access under the scheme, particularly for those not covered by the Privacy Act or equivalent.

## 4.5. Renew

Accredited entities will be required to renew their accreditation after a period of time as a way to refresh their understanding of their obligations and to reflect any changes that may have been implemented to the data sharing scheme.

Accredited organisations will need to confirm, and Accredited Data Service Providers will need to demonstrate, that they continue to have the appropriate controls and systems in place before accreditation can be renewed. For accredited individuals, their organisation must confirm their endorsement of the individuals, and individuals will need to confirm their understanding of their obligations.

It is proposed that Accredited Data Service Providers would renew their accreditation every five years. Accredited Users would renew their accreditation every three years. In some circumstances, the National Data Commissioner could also request an accredited entity to undergo the renewal process earlier. For example, if a new or significant technological development emerges in the data sharing scheme which requires an entity to meet updated or additional criteria.

Three months from the expiry date, accredited entities will receive a notice to remind them to renew their accreditation but they can choose to start this process at any time.

Accredited entities will also receive directions from the National Data Commissioner on what they will need to do with any scheme data<sup>15</sup> they still hold before their accreditation expires. This could include destroying or returning the scheme data as instructed.

If their accreditation expires and they continue to hold or maintain access to scheme data, they will be suspended from the data sharing scheme until they have appropriately dealt with the data. The National Data Commissioner maintains regulatory oversight and enforcement powers over the suspended entity until they have complied with directions. Failure to comply is considered a breach of the legislation.

Accreditation will be cancelled once they have completed the directions in the notice.

### 4.5.1. Discontinuing accreditation

Accredited entities can apply to cancel their accreditation, if they no longer want to participate in the data sharing scheme or do not require access to data under the legislation.

If an accredited entity does not intend to renew their accreditation, they must finalise any Data Sharing Agreements they are a party to and ensure scheme data is appropriately managed as per the Data Sharing Agreement or as directed by the National Data Commissioner.

Questions:

.....

10. Are there further ways we can streamline the accreditation process?

11. Do the timeframes to renew accreditation, every 5 years for Accredited Data Service Providers and every 3 years for Accredited Users, seem reasonable?

15 Scheme data is data shared under the legislation, including outputs of such data unless it has exited the data sharing scheme.

# 5. Other matters

## 5.1. Regulation

The National Data Commissioner has a range of regulatory and enforcement powers to ensure all participants in the data sharing scheme remain compliant with the requirements of the legislation.

To regulate accreditation, the National Data Commissioner will maintain oversight of all accredited entities and can conduct assessments or initiate investigations about an accredited entity in response to a complaint or a suspected breach of the legislation or commence their own investigation.

The National Data Commissioner will also have the power to suspend or cancel accreditation (see *Suspension or cancellation of accreditation*). Where accreditation has been cancelled, the National Data Commissioner may also give a direction to the organisation or individual on how to handle the scheme data. The Commissioner will provide a notice of the suspension to and consult with Data Custodians of active Data Sharing Agreements to determine what the appropriate action is for dealing with scheme data.

Until the organisation or individual has complied with the direction and dealt with the scheme data appropriately, they will remain a part of the scheme with a suspended accreditation status. This will ensure the National Data Commissioner continues to have regulatory and enforcement powers over the accredited entity and can apply penalties for any breach of the legislation. Suspended entities cannot enter into new Data Sharing Agreements.

The National Data Commissioner must notify an organisation or individual as soon as practicable after a decision is made to suspend or cancel their accreditation. We are also proposing

that, as an extra level of assurance, the National Data Commissioner may also notify parties to Data Sharing Agreements of the changed status of accredited entities.

### 5.1.1. Suspension or cancellation of accreditation

Accreditation may be suspended if there is suspected:

- unauthorised data sharing
- failure to comply with the mandatory terms of a Data Sharing Agreement
- provision of false or misleading information as part of their application for accreditation
- breach of a requirement of the legislation or the Rules and/or
- activity against the national interest.

Depending on the outcome of an investigation, including the culpability of the accredited entity, the National Data Commissioner may:

- find there is no case to answer and remove suspension or
- require action to redress the issue and remove suspension or
- require action to redress the issue/breach and apply conditions before removing suspension or
- cancel accreditation.

## Question:

.....

**12. Is it appropriate to notify parties to Data Sharing Agreements of an accredited entity's suspension?**

## Questions:

.....

**13. Is there any information that must, or must not, be made publicly available through the registers of accredited entities?**

**14. Is there any information that should be made available to Data Custodians through the registers of accredited entities?**

## 5.2. Registers

The legislation specifies that the National Data Commissioner must maintain public registers of accredited entities, which contain the accredited entity's name and contact details. For Accredited Data Service Providers, the register will also include the type(s) of data services they are accredited to perform.

Under these parameters, we are proposing to publish:

- names of accredited organisations, the Responsible Officer and their position
- the date of accreditation and duration
- the number of accredited individuals within the accredited organisation
- contact details of the organisation
- list of data services the organisation is accredited to perform (Accredited Data Service Providers only), and
- other information the National Data Commissioner deems appropriate.

The Ministerial Rules will specify what information will be publicly available, circumstances where information should be omitted, what may be shared with specific organisations, such as Data Custodians, and what will only be visible to the Commissioner and their office.

Specific details related to an accredited individual may be published in association with a Data Sharing Agreement.

Maintaining these registers will provide transparency of the schemes operation, particularly the users wanting to access public sector data.

## 5.3. Fees

Charging fees for accreditation will be determined through a Cost Recovery Impact Statement, in line with the Australian Government Charging Framework.

Generally, fees could be introduced to meet increasing demand for accreditation as the data sharing scheme matures or support improvements to the accreditation process through better technological solutions or additional resources.

If the outcome of the impact statement supported charging fees, it would likely be applied to accreditation applications, renewals, undertaking regulatory functions related to accreditation or maintaining public registers on accredited entities. How fees are applied would then be specified in the Ministerial Rules, including amount and timeframes for payment. This information would be made publicly available.

We recognise that fees could be a barrier for some organisations or individuals to apply for accreditation. Should a decision be made to charge fees, we will seek to ensure the National Data Commissioner has the discretion to provide an exemption.

More broadly, Data Custodians can consider cost recovery measures for additional expenses incurred through enabling data sharing, such as preparing data or providing additional training to Accredited Users.

Accredited Users may also incur separate costs as part of receiving access to data. For example, undertaking additional training specified in the Data Sharing Agreement or fees sought by the Data Custodian for data access.

**Question:**  
.....

**15. Is charging a fee for accreditation, such as a renewal fee, reasonable?**



# 6. Transition Arrangements

## 6.1. Accredited Integrating Authority

Under the current Commonwealth framework for statistical data integration, organisations accredited as Integrating Authorities are responsible for data integration using Commonwealth Data for statistical and research projects. To avoid duplicating current arrangements, we are proposing to transition the Accredited Integrating Authority model to the Accredited Data Service Providers model.

To enable a smooth transition and minimise any gaps in existing arrangements, we will engage with existing Accredited Integrating Authorities to discuss viable transition approaches. This discussion will include how to ensure there are no policy gaps, that is, that the integration and sharing services of Accredited Data Service Providers are recognised and have policy authority, even if the Accredited Data Service Provider is not being engaged to share or integrate data under the auspices of the legislation.

Our starting point is for Accredited Integrating Authorities to notify the National Data Commissioner they are seeking accreditation for the provision of data integration services, using their Accredited Integrating Authority application and with the following conditions:

- Accredited Integrating Authorities who were accredited five or more years ago will need to reapply within 12 months of the accreditation framework coming into effect, using the new Accredited Data Service Provider accreditation process.

- Other Accredited Integrating Authorities will need to reapply five years from their original Accredited Integrating Authority's accreditation date, using the new accreditation process.

Data sharing on behalf of a Data Custodian is a new data service and is not part of the assessment criteria for existing Accredited Integrating Authorities. The National Data Commissioner will separately assess Accredited Integrating Authorities that wish to be accredited for data sharing services under the new accreditation process.

Once all Accredited Integrating Authorities are transitioned to the Accredited Data Service Provider model, the Commonwealth framework for statistical data integration would effectively cease operation. The transition to the new model does not impact existing data integration activities and will not limit Accredited Data Service Providers from performing data integration on data shared under other legislative authority.

## 7. Next steps

We want to hear your views on our proposed framework, especially responses to the questions we have posed. Our consultation period runs for eight weeks, and is an opportunity for you to provide formal written submissions to the Office of the National Data Commissioner through [our website](#). Submissions will be due by 6 November 2020.

We will also host a webinar about accreditation to discuss the proposed framework and answer any questions. More information about when this is happening will also be available on [our website](#).

In addition to this consultation process, we are planning:

- bilateral and multilateral meetings with stakeholders, including the Australian Public Service, potential data service providers and users as well as the current Accredited Integrating Authorities
- drafting instructions to inform the Ministerial Rules
- to undertake a Privacy Impact Assessment on the accreditation framework, and
- co-design workshops to help design the implementation of the framework.

In the coming months, we look forward to engaging with you to listen, learn and improve the framework.



# Appendix 1: Key terms

**Accreditation** is the process by which the National Data Commissioner approves an entity for entry into the data sharing scheme.

**Accredited Integrating Authorities** is an organisation assessed as having the infrastructure and capability to undertake high risk data integration projects involving Commonwealth Government data for statistical or research purposes. They are also responsible for providing researchers with safe and secure access to the integrated data in line with the requirements of Data Custodians.

**Accredited Data Service Provider** is an organisation or individual with technical expertise who can offer complex data integration services and/or data sharing on behalf of a Data Custodian.

**Accredited Entity** is an Accredited User organisation, individual or Accredited Data Service Provider.

**Accredited User** is an organisation or individual who wants to access public sector data under the legislation.

**Cancellation** means the accreditation of a user or data service provider ceases. The user or data service provider is no longer a data scheme entity and cannot hold scheme data or participate in the data sharing scheme.

**Complex data integration** is combining information from different data sources to produce new datasets and which has a level of difficulty or risk associated with it.

**Condition** is any limitation or requirement placed on the accreditation of a user or data service provider.

**Data** is any information in a form capable of being communicated, analysed or processed (whether by an individual or by computer or other automated means).

**Data Custodians** are Commonwealth bodies that control and have the right to deal with particular public sector data.

**Data Scheme Entities** are Data Custodians of public sector data and accredited entities.

**Data sharing** means providing controlled access to public sector data to the right people for the right reasons with safeguards in place.

**Data Sharing Principles** are risk management safeguards applied prior to sharing public sector data under the Data Sharing legislation. The five principles are Project, People, Setting, Data and Outputs.

**Data Sharing Purposes** provides the scope for sharing public sector data under this legislation.

**Data sharing scheme** is the legislative framework established by the Data Availability and Transparency Bill and subordinate legislative instruments (regulations, rules, and data codes), as well as guidelines.

**Entity** covers all types of Australian and foreign nationals capable of participating in the data sharing scheme. This includes individuals, government bodies, body corporate and body politics, organisations and non-legal entities.

**Output** is data that is the result or product of the use, by an Accredited User, of public sector data shared with the Accredited User.

**Personal information** is defined by the *Privacy Act 1988* to mean information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.



**Public sector data** is data that is collected, created, or held by the Commonwealth Government, or on its behalf. Data created or enhanced by an Accredited Data Service Provider on behalf of a Data Custodian in the data sharing scheme falls within this definition.

**Responsible Officer** is an individual who has the legal authority to act on behalf of the organisation for accreditation purposes. This includes applying, managing and maintaining the organisation's accreditation, oversight of data activities accessed under the legislation, and endorsement of individuals for accreditation.

**Scheme data** is data shared under the legislation, including outputs of such data unless it has exited the data sharing scheme.

**Suspension** means the accreditation of a user or data service provider is temporarily revoked and they cannot participate in the data sharing scheme while the suspension remains in effect. The user or data service provider continues to be a data scheme entity who can hold scheme data and is subject to regulatory oversight.





