Defining 'trusted entities' for the purposes of national data sharing

Appendix 2: ONDC alignment with trusted entity attributes

The Office of the National Data Commissioner (ONDC) has established a robust national accreditation framework to ensure that only those who can safely handle public data are able to participate in data sharing. To be accredited as a data users, entities must meet the following criteria:

- the entity has appropriate data management and governance policies and practices and an appropriately qualified individual in a position that has responsibility for data management and data governance for the entity
- the entities are able to minimise the risk of unauthorised access, sharing or loss of data
- the entity has the necessary skills and capability to ensure the privacy, protection and appropriate use of data, including the ability to manage risks in relation to those matters.

In addition to the above, accredited data service providers (ADSP) must also have the necessary policies, practices, skills and capability to perform one or more of the following data services: de-identification of data, secure access data and/or complex data integration.

Findings

Analysis of the trusted entity attributes compared to the ONDC accreditation framework shows that:

- ADSP accreditation aligns with all the attributes.
- User accreditation aligns with nearly all the attributes. Whilst most attributes are covered, there are three attributes which are mostly/partially aligned and two which are not expressly covered in the ONDC framework. The primary reason for non/partial alignment is that the attributes in question relate to data projects, which are generally covered in the ONDC's data sharing agreements and not in the accreditation framework. Information about the two attributes not covered may also be collected throughout the assessment process in adjacent questions, however, they are not expressly part of the original questionnaire set for user accreditation.

More information on the accreditation framework can be found on the ONDC website:

Expected characteristics for user accreditation | Office of the National Data Commissioner; and

Expected characteristics for data service provider accreditation | Office of the National Data Commissioner

Theme	Attribute	User Strong	User Partial	ADSP Strong	ADSP Partial
Transparency	**Verifiable audit and assurance processes:** Where appropriate, internal and external processes will be implemented to verify compliance with legal and ethical standards, including those related to data environments and systems.	✓		✓	
Transparency	**Public transparency standards:** The agency will have public-facing processes and/or standards for data release and publication.	✓		✓	
Transparency	**Transparent and defined project methodology**: Clear and transparent project methodologies, including integration approaches, output vetting and risk management procedures, will be documented and shared with the relevant data custodian.		✓	✓	
Accountability	**Legally supported sharing:** Data sharing arrangements will be legally authorised and supported by clear documentation such as agreements and data sharing registers.	✓		✓	
Accountability	**Ethical consideration:** Projects will undergo ethics consideration and where required approval, consent and review processes to ensure alignment with ethical standards. Agencies will have clear data roles and responsibilities to ensure accountability.	✓		✓	
Accountability	**Defined roles and responsibilities**: Agencies will have clear data roles and responsibilities to ensure accountability.	✓		✓	
Accountability	**Authorised and skilled personnel:** Personnel will have the knowledge, skills, authorisation and training to use data appropriately, including training in data breach and risk management.	✓		✓	
Data Management and Governance	**Data quality processes:** Data quality management plans will be implemented to ensure data integrity and compliance.	✓		✓	
Data Management and Governance	**Data governance authorisations:** Agencies will have established data governance processes which have clear decision-making authorisations. This includes an understanding of the agencies data governance priorities, dispute resolution processes and accountable data custodianship roles.	✓		✓	
Data Management and Governance	**Defined metadata management practices with accountable data custodianship roles**: Agencies will have defined metadata management practices which are accurate, consistent and accessible across the agency. This includes data lineage information.	✓		✓	
Data Management and Governance	**Consistent and controlled data release protocols:** Agencies will have clear operating models for data release, including for review, verification, and approval for release.		✓	✓	
Data Management and Governance	**Established escalation and risk management frameworks**: Agencies will have established escalation pathways for managing risks and incidents. Projects will have comprehensive risk management plans which consider privacy by design and security risk assessments.	✓		✓	
Security	**Secure transfer mechanisms**: Agencies have secure mechanisms for data transfer to prevent breaches.		✓	✓	

Theme	Attribute	User Strong	User Partial	ADSP Strong	ADSP Partial
Security	**Secure access control mechanisms:** Agencies will implement data safeguards, use secure access environments appropriate to the sensitivity of the data, and restrict data access to authorised users with appropriate security clearances.	✓		✓	
Security	**Certified secure environment:** Data will be accessed within certified secure environments appropriate to the classification of the data, e.g. ONDC Accredited Data Service Provider, IRAP-certified or Essential 8.	✓		✓	
Security	**Consistent security labelling and classification:** Agencies will assign appropriate security classifications for data assets and outputs to guide handling and sharing.	✓		✓	
Security	**Established security clearance assessments**: Agencies will consistently use established security clearance/vetting process, e.g. Australian Government Security Vetting Agency.	✓		✓	
Security	**Incident monitoring and response mechanisms:** Mechanisms for incident monitoring, identification, and response are in place.	✓		✓	
Privacy	**Data minimisation protocols:** Agencies will implement the privacy by design principle, including minimising the collection and storage of personal data to what is necessary to achieve the project, and adhering to approved retention and disposal practices.	✓		✓	
Privacy	**De-identification mechanisms**: Agencies will have controls and safeguards to manage re-identification risks, including removing direct identifiers, limiting access to sensitive data, using secure transfer mechanisms or controlled environments, and adhering to the separation principle.	✓		✓	
Privacy	**Privacy incident reporting:** Agencies will have established processes to report privacy incidents and data breaches and fulfil legislative responsibilities.	✓		✓	