Defining ‘trusted entities’ for the purposes of national data sharing

Appendix 3: Table of trusted entity attributes and guiding questions

Theme	Attribute	Guiding questions	Useful resources
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.	• What audit processes does your agency undertake? • What was the recent outcome of an audit? • What assurance processes does your agency undertake? • How do you ensure compliance to legal and ethical standards? • Does your agency have a strategy or improvement plan for uplifting the data maturity of your agency? How does this align with your recent audit results? • What data environment specific audit processes does your agency undertake? • How frequently does this data environment get audited? • Which aspects of the data environment were audited and at what security level are they operating? For example, only a single instance of a database operates at an Essential 8 level 3.	
Transparency	**Public transparency standards** The agency will have public-facing processes and/or standards for data release and publication.	• Does your agency have a public transparency statement? • What documentation does your agency publish regarding your agency's its data processes and procedures? • What documentation is available to staff to understand standards for data release? • Does your agency have a public register of data sharing projects?	• Guidelines on data matching in Australian Government administration | OAIC

Theme	Attribute	Guiding questions	Useful resources
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.	• What documentation does this project have to detail the project methodology? • Is there a risk register or a similar process in place to identify and mitigate risks within the project? • What output vetting mechanisms are in place to ensure that only approved data is being released?	
Accountability	**Legally supported sharing** Data sharing arrangements will be legally authorised and supported by clear documentation such as agreements and data sharing registers.	• How does your agency manage data sharing agreements? Does it operate a data sharing register? • What support does your agency have to understand the legal requirements of data sharing or the impact of legislation on the data your agency holds and hosts? • How does your agency ensure legal compliance in data sharing? • Has your agency considered the legal basis for requesting data? • Does your agency undertake conformance assessments to ensure the shared data remains aligned with the specified purpose and legal authorisation for data sharing?	• Data Sharing Agreements | ONDC
Accountability	**Ethical consideration** Projects will undergo ethics consideration and where required approval, consent and review processes to ensure alignment with ethical standards.	• What ethics approval processes does your agency have? • How does your agency ensure its ethics processes align with standards? • Does this project/request require an ethics approval?	• APS Data Ethics Framework | Department of Finance • APS Data Ethics Use Cases | Department of Finance • Australia's Artificial Intelligence Ethics Principles | Department of Industry Science and Resources • Interim guidance on government use of public generative AI tools | Digital Transformation Agency

Theme	Attribute	Guiding questions	Useful resources
			• Adoption of Artificial Intelligence in the Public Sector | Digital Transformation Agency • OECD Good Practice Principles for Data Ethics in the Public Sector | OECD
Accountability	**Defined roles and responsibilities** Agencies will have clear data roles and responsibilities to ensure accountability.	• What data roles are evident within your agency? • Does your agency have governance committees with responsibility for data management and issue resolution? • What specific data governance processes within your agency ensure accountability and responsibility for data?	• Data job role personas | Australian Public Service Commission • SES Accountabilities for Data | Department of Finance • Chief Data Officer Information Pack | Department of Finance • Best Practice Guide to Applying Data Sharing Principles | DPM&C • Protective Security Policy Framework - Section 2 | Department of Home Affairs • APS Data Ethics Framework | Department of Finance
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.	• Is there agency specific training provided to data roles? • What training is provided about data breach and risk management reporting? • What training is provided about specific technical aspects of working with the data? • Is training provided about the legal and non-legal consequences of data misuse?	• APS Data Capability Framework | Australian Public Service Commission • Protective Security Policy Framework - Section 16, 18 & 19 | Department of Home Affairs
Data Management and Governance	**Data quality processes** Data quality management plans will be implemented to ensure data integrity and compliance.	• Does your agency have a data quality management plan? How is this governed? • What guidance material is available to support personnel in understanding data quality controls specific to your agencies data?	• Australian Privacy Principle 10: Quality of personal information | OAIC

Theme	Attribute	Guiding questions	Useful resources
		• What data validation protocols are utilised in your agency? • Does your agency track the quality of data over time?	
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.	• Does your agency have a data governance policy? • How does your agency implement the data governance policy? • How does your agency delineate between data governance and platform governance/security? • What decision making bodies exist to manage data governance? • Who in your agency has approval to release data? • Does your agency have a data maturity up-lift plan or data governance forward work plan? • What dispute resolution processes does your agency have regarding data governance and data requests?	• Data Custodians | Data.gov.au • Establishing an information governance framework | National Archives of Australia • Data Integration Projects - Data Custodians | National Statistical Service
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.	• What frameworks inform your agency's metadata management functions? • How does your agency maintain consistency across metadata collection? • Do all data assets within your agency have an accountable officer? • How does your agency capture data lineage information?	• Australian Government Recordkeeping Metadata Standard | National Archives of Australia • Guide on Metadata Attributes | ONDC
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.	• Describe your agency's data release operating model. • What output vetting procedures does your agency implement? • What mechanisms does your agency have in place to ensure custodian release requirements have been met?	

Theme	Attribute	Guiding questions	Useful resources
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.	• What are your agency's data incident reporting and escalation procedures? • Who are your agency's accountable officers related to risk management? • Does the project have a risk management plan?	• Commonwealth Risk Management Framework | Department of Finance • Establishing Risk Management Framework | Department of Finance • Risk Management Toolkit | Department of Finance • Five Safes framework | Australian Bureau of Statistics
Security	**Secure transfer mechanisms** Agencies have secure mechanisms for data transfer to prevent breaches.	• What secure transfer mechanisms does your agency operate? • How does your agency determine when to use secure transfer mechanisms? • Does your secure transfer mechanism change depending on the type and/or size of the data being transferred?	
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.	• How does your agency monitor and control data access? • How does your agency maintain up-to-date information about data users authorised to access data? • How does your agency determine what safeguards to implement for a data asset or specific project/data request? Are any of these safeguards automated? • Do access controls differ if a data requester accesses data physically or digitally?	
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.	• Does your agency have a certified secure data environment? • What certification does this environment have? When was it last audited or verified? • How does your agency determine if a certified secure data environment is required for a data asset or data project?	• Protective Security Policy Framework | Department of Home Affairs

Theme	Attribute	Guiding questions	Useful resources
		• Will this data request require a certified secure data environment?	
Security	**Consistent security labelling and classification** Agencies will assign appropriate security classifications for data assets and outputs to guide handling and sharing.	• How consistent is the application of security labelling and classification within your agency? • What security labelling and classification system does your agency use? How does your agency determine when it is appropriate to use this security labelling and classification system, e.g. state, territory or Commonwealth labels?	
Security	**Established security clearance assessments** Agencies will consistently use established security clearance/vetting process, e.g. Australian Government Security Vetting Agency.	• What security and clearance vetting procedures does your agency use?	
Security	**Incident monitoring and response mechanisms** Mechanisms for incident monitoring, identification, and response are in place.	• What incident monitoring procedures does your agency have? • Does your agency implement automated incident monitoring and response controls? • Has your agency responded to a reportable breach in the last 12 months? If not, how has your agency responded to a simulated breach?	
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.	• Does your agency have a data minimisation policy? • Does your agency have formal retention and disposal policies? • How does your agency implement the privacy by design principle? • Is the scope of the data requested appropriate to achieve the specified purpose?	• Australian Privacy Principle 11 Security of personal information | OAIC • Protective Security Policy Framework - Section 11 Information disposal | Department of Home Affairs • Guide to undertaking privacy impact assessments | OAIC • Privacy by design | OAIC

Theme	Attribute	Guiding questions	Useful resources
			• 10 steps to undertaking a privacy impact assessment | OAIC • Privacy impact assessment tool | OAIC • Assessing privacy risks in changed working environments: privacy impact assessments | OAIC
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.	• Does your agency have a data de-identification policy? • How does your agency implement the separation principle? • What processes does your agency implement to adhere with privacy legislation?	• Australian Privacy Principles guidelines | OAIC Australian Privacy Principle 11 Security of personal information | OAIC • De-identification and the Privacy Act | OAIC • De-Identification Decision-Making Framework | OAIC • Data confidentiality guide: Understanding re-identification | ABS • The separation principle | ABS
Privacy	**Privacy incident reporting** Agencies will have established processes to report privacy incidents and data breaches and fulfil legislative responsibilities.	• What data disclosure compliance does your agency implement? • How does your agency ensure outputs are compliant with project agreements and legislation? • How does your agency manage and respond to privacy complaints?	• Notifiable data breaches | OAIC • Preventing, preparing for and responding to data breaches | OAIC • Handling privacy complaints | OAIC • Information privacy officers | Office of the Information Commissioner Queensland