Intergovernmental Agreement on data sharing between Commonwealth and State and Territory governments

An Agreement to share data across jurisdictions as a default position, where it can be done securely, safely, lawfully and ethically.

Parties

This Agreement is between

- the Commonwealth of Australia; and
- the States and Territories, being
    - The State of New South Wales
    - The State of Victoria
    - The State of Queensland
    - The State of South Australia
    - The State of Western Australia
    - The State of Tasmania
    - The Australian Capital Territory
    - The Northern Territory of Australia.

Preliminaries

Access to data is critical for policy, service delivery, and government decision making. Data held by one government can be valuable to another government in delivering its activities.

Responsibly, securely and seamlessly sharing data between governments is an efficient use of resources and will help drive economic value, innovation, improve services, and deliver better outcomes for Australians.

All jurisdictions agree to share data across jurisdictions as a default position, where it can be done securely, safely, lawfully and ethically. Data will be shared in accordance with established privacy standards.

Data sharing is occurring effectively in some areas and requires improvement in others. To maximise the benefits for all Australians, all governments will improve data sharing processes and practices between jurisdictions.

This Agreement builds on Data and Digital Ministers' efforts to share data, in support of targeting emergency and recovery measures during the pandemic. Data and Digital Ministers will continue their strategic oversight role in developing data sharing systems to improve outcomes for Australians.

Portfolio Ministers will remain responsible for data sharing activities within their portfolio responsibilities, and will collaborate with Data and Digital Ministers to identify and progress national priority data areas.

This Agreement governs the sharing of public sector data, which is data collected and held by Commonwealth, State and Territory governments.

Operative provisions

The parties agree:

1. Objective and scope of this Agreement

a) The objective of this Agreement is to improve outcomes for Australians by:

   i) committing all governments to use best endeavours to share data between jurisdictions as a default position; where it can be done securely, safely, lawfully and ethically;

   ii) focusing efforts on nationally significant data sharing priorities for the benefit of Australians; and

   iii) reforming data sharing systems from design to delivery.

b) Data will be shared in the public interest, for the purposes of:

   i) informing policy decisions;

   ii) designing, delivering, and evaluating programs;

   iii) tracking implementation; and/or

   iv) improving service delivery outcomes.

c) This Agreement recognises data as a shared national asset. All jurisdictions commit to maximising the value of data to deliver outstanding policies and services for Australians.

2. Interpretation

a) This Agreement establishes national data sharing priorities and also seeks to improve business as usual data sharing.

b) The mechanism for identifying and monitoring national priority data areas is set out at Schedule A to this Agreement.

c) Default data sharing refers to the expectation governments will work collaboratively, be responsive to data requests and share data unless there is a legitimate reason not to (see Schedule B).

d) Data types in scope of this Agreement include the following, where sharing is permitted by or under law:

   i) Routine administrative data (de-identified and aggregated) which informs policy, program and service design, delivery, and other business as usual government functions;

   ii) Statistics and reference data, including metadata;

   iii) De-identified and identifiable data for response and recovery purposes for emergencies, and natural and other disasters and hazards;

   iv) Identifiable data for joined up services shared with customer consent;

   v) De-identified and identifiable data for data integration projects and cohort needs analysis; and

   vi) Data and information which supports existing intergovernmental agreements where needed.

e) This Agreement is not intended to create legal relations between the Parties. Notwithstanding this, the Parties intend to comply with all provisions in this Agreement.

f) This Agreement should be read in conjunction with, and does not override or supersede, all relevant and related legislative obligations, agreements, frameworks and policies.

3. Guiding principles for this Agreement

a) Value – The use and re-use of public sector data will be optimised through sharing by default between jurisdictions, in a way that promotes reciprocity and mutual benefit;

b) Quality – Cooperate to improve data quality and ability to derive insights, with best endeavours to ensure data is reliable, robust, verifiable and fit-for-purpose;

c) Secure – Appropriate standards of privacy and security will be upheld to protect shared data to ensure individual and commercial confidentiality and national security;

d) Trusted – Jurisdictions will build trust with Australians when sharing data by adhering to the Data and Digital Ministers' Trust Principles (Schedule C);

e) Ethical – Appropriate standards of ethics will be applied when sharing data, including that sharing is in the public interest;

f) Lawful – Data sharing has a legal basis, with due diligence undertaken and legal and policy requirements upheld;

g) Pragmatic – Parties adopt a practical approach to data sharing, recognising all jurisdictions retain decision-making rights on sharing data under the Agreement, including on cost, benefit and risk assessments;

h) Discoverable – Parties recognise the benefits of new data sharing and data management systems supporting discoverability, interoperability, data and information accessibility, and cost effective access to data;

i) Enabling – Parties recognise the benefits of shared infrastructure and practices to enable data sharing;

j) Contemporary methods – Where required, and possible, shared data will be made available in real time through automated processes, Application Programming Interfaces (APIs) and secure data access environments; and

k) Accountable – Any decision to decline access to data (non-exhaustive examples are outlined in Schedule B) must be clearly articulated, well substantiated and communicated to the requester as a priority, and as soon as practicable.

4. Governance

a) Data and Digital Ministers will:

   i) oversee implementation of this Agreement;

   ii) seek advice from senior officials and relevant Portfolio Ministers to identify national priority data areas for the National Data Sharing Work Program (Work Program, see Schedule A);

   iii) maintain the Work Program to ensure strong action is taken to address national priority data areas and reform initiatives for data sharing, provide it to National Cabinet on request (in accordance with Schedule A), and assess performance against the Work Program;

   iv) Seek advice from their senior officials on implementation of this Agreement and Work Program and task senior officials as necessary to give effect to this Agreement;

   v) assess the effectiveness of this Agreement and the Work Program; and

   vi) issue guidance to support implementation, including on the Agreement's interactions with other data sharing initiatives as needed.

b) Commonwealth, State and Territory Portfolio Ministers will:

   i) collaborate with Data and Digital Ministers to identify and progress national priority data areas for data sharing; and

   ii) advance and action data sharing activities within their portfolio responsibilities.

c) This Agreement will not override or supersede the data sharing provisions of other formal intergovernmental agreements or memoranda of understanding, which will remain the responsibility of the lead Portfolio Ministers for those agreements.

5. Roles and responsibilities

The Parties to this Agreement have the following roles and responsibilities to:

a) where possible, use this Agreement to facilitate cross-jurisdictional data sharing;

b) share data in accordance with the Data Sharing Principles (see Schedule D);

c) guide data requesters and data custodians to meet the minimum information requirements (see Schedule E);

d) use best endeavours to allocate adequate resources to data sharing priorities identified in the Work Program and business as usual data sharing, acknowledging each jurisdiction will make sovereign decisions on resourcing;

e) identify and remove restrictions unnecessarily impeding lawful data sharing, including potential regulatory and administrative barriers;

f) respond to government requests for data access in a consistent and timely manner;

g) ensure that relevant Commonwealth, state and territory protective security requirements continue to apply to any Commonwealth, state and territory information shared under this Agreement; and

h) ensure any shared identifiable data is handled in accordance with applicable Commonwealth, state and territory privacy laws, including the *Privacy Act 1988* (Cwth).

The Commonwealth has responsibility for:

i) the operation of the Agreement within the Australian Public Service; and

j) the design and oversight of nationally consistent data sharing policy.

The States and Territories have responsibility for:

k) the operation of the Agreement within their jurisdictions; and

l) working with other jurisdictions to identify and align common data requests where appropriate.

6. Commencement

This Agreement will commence as soon as the Agreement is signed by the Commonwealth and one other jurisdiction and will operate for all signatories unless revoked by the Parties.

7. Review of this Agreement

Two years after commencement, Data and Digital Ministers will undertake a review of this Agreement to assess the effectiveness and efficiency of national data sharing activity, performance against objectives in this Agreement, and its value in improving government services delivered to Australians. The review will determine whether amendments to this Agreement are required.

8. Variation/Amendment

This Agreement may be amended at any time by the unanimous decision of Parties. Any amendment must be made in writing and executed by Parties and will include the date on which the amendment will come into force.

9. Delegation

Data and Digital Ministers are authorised to amend Schedules to this Agreement.

10. Withdrawal

A Party may withdraw from this Agreement by sending written notice to all other Parties. The withdrawal will become effective three months after the notice was sent. A Party may revoke its withdrawal at any time prior to it becoming effective. If a Party withdraws from this Agreement, this Agreement will continue in force with respect to the remaining Parties.

11. Dispute resolution

Any Party may give notice to other Parties of a dispute under this Agreement. Officials of relevant Parties will take action to resolve any dispute in the first instance.

If a dispute related to a national priority data area (as agreed in the Work Program) cannot be resolved by officials, it may be escalated to Data and Digital Ministers. Data and Digital Ministers may seek external expertise to inform their advice.

12. Definitions

a) Application Programming Interfaces (APIs)

A tool that allows developers and product teams to re-use parts of existing systems when designing and building new products.

Used to build services across government that talk to each other and provide access to data or functionality in ways that are secure, and efficient.

b) Best endeavours

The mutual obligation of all jurisdictions to work together in good faith to meet the intent and spirit of the Agreement, whilst acknowledging the right of each jurisdiction to make decisions in their best interests.

c) Data de-identification

Personal information is de-identified if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.

d) Data and Digital Ministers Meeting (DDMM)

The regular, ongoing meeting of Commonwealth and state and territory Ministers with responsibility for data and digital matters under Australian federal relations architecture.

e) DDMM National Data Sharing Work Program

The Work Program which supports this Agreement by documenting national data sharing priorities.

f) Identifiable data

Data consisting of personal information, where an individual is identified or reasonably identifiable.

g) Metadata

Information about how data is defined, structured and represented.

h) National priority data areas

A data sharing proposal or topic which meets the eligibility criteria at Schedule A.

i) Public interest

Activities that have a consideration of the potential benefits and risks to the economy, public health, the environment, and overall social wellbeing. The evaluation also has to pay attention to the risks and benefits for individuals and businesses as well as population groups, including vulnerable communities.

j) Public sector data

Data that is collected, created or held by a Commonwealth, State or Territory Government, or on its behalf.

k) Social licence

Broad public acceptance and/or ongoing approval of an activity.

Schedules:

A. Mechanism to develop the National Data Sharing Work Program

B. Examples of legitimate reasons to decline a data request

C. Data and Digital Ministers' Trust Principles

D. Data Sharing Principles

E. Data request minimum information requirements

Schedule A – Mechanism to develop the National Data Sharing Work Program

1. Purpose

The purpose of this Schedule is to identify how specific time-limited national priority data areas will be agreed for focused national effort.

2. Eligibility criteria

A national priority data area may be added to the Work Program if it meets each of the following criteria:

a) It is a national strategic priority, including for example consideration by National Cabinet or a Ministers' Meeting;

b) Public benefit (or a public cost to be reduced or removed) outweighs the costs and risks of sharing;

c) There are current barriers preventing or limiting effective data sharing which requires a cross-jurisdictional response; and

d) The nomination is endorsed by a minimum of one Commonwealth portfolio Minister and a relevant portfolio Minister from at least two States and/or Territories.

3. Prioritisation process

a) Data and Digital Ministers will seek advice from responsible Portfolio Ministers from all jurisdictions to seek the nomination of national priority data areas for the Work Program.

b) Data and Digital Ministers will apply the eligibility criteria to determine the forward Work Program.

c) Data and Digital Ministers reserve the right to decide not to add a nominated national priority data area to the Work Program and may apply additional eligibility criteria to national priority data area nominations as required.

d) Deliverables and timeframes for each national priority data area will be identified in the Work Program.

4. Progress and review

a) Where multiple Portfolio Ministers are responsible for a national priority data area, multiple data sharing agreements may be used to initiate and progress data sharing.

b) Portfolio Ministers, with support from Data and Digital Ministers as needed, will identify key projects under each priority data area.

c) Data and Digital Ministers will review Work Program progress every six months in consultation with Portfolio Ministers.

d) Resolved priorities will be removed from the Work Program.

5. Opt-out process

a) Any jurisdiction may decide to opt-out of, or withdraw, their participation in any individual national priority data area in the Work Program.

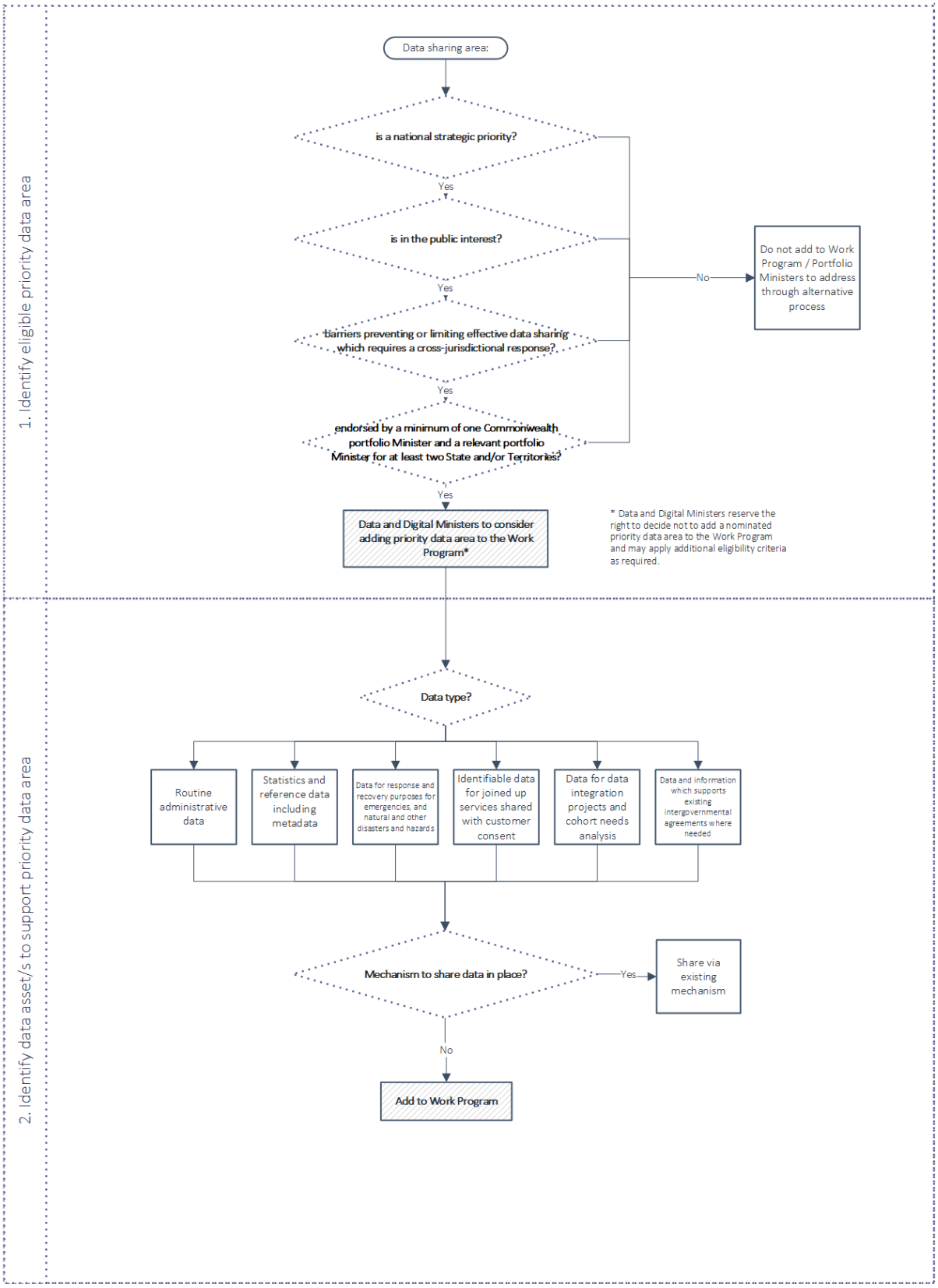
b) The relevant Portfolio Minister should notify Data and Digital Ministers of the decision and outline the reasons for it in writing.

c) Participating jurisdictions for each national priority data area will be noted in the Work Program.

6. System reforms

Based on lessons learnt through the COVID-19 period, the Commonwealth and States and Territories have identified foundational reform activities required to support better data sharing and continued improvements in data maturity. These reform activities will be built into the Work Program.

7. Work Program prioritisation flowchart



Schedule B – Examples of Legitimate Reasons to Decline a Data Request

A legitimate reason to decline a data request includes where the sharing would, or could reasonably be expected to:

- contravene a law (such as a privacy or data protection obligation or a secrecy provision), contractual obligation or right (such as intellectual property rights), legal professional privilege or equitable obligation of confidence, an order of a court or tribunal;
- prejudice an investigation, inquiry or legal proceeding; or
- be likely to endanger an individual's health, safety or wellbeing.

A request may also be refused if:

- the requested data is readily available through other sources (e.g. is published)
- the requested data is not collected or does not exist in a sharable form;
- the proposed sharing arrangement does not satisfy the Data Sharing Principles (under Schedule D); or
- sharing is inappropriate from a data ethics and social licence perspective, despite the proposed public interest.

These reasons are not exhaustive and Parties may consider other sensitivities or obligations that prevent from data being shared.

Where resourcing is a genuine constraint, Parties agree to use best endeavours to determine how resourcing should be dealt with in light of the proposed public interest.

The 'responsibility to share' is also found in the National Best Practice Guide to Applying Data Sharing Principles published by the Office of the National Data Commissioner.

Schedule C – Data and Digital Ministers Meeting's Trust Principles

To make sure citizens' needs are front of mind and governments earn the trust of Australians when sharing data, jurisdictions will observe the Data and Digital Ministers' agreed Trust Principles. There are four principles, containing eight commitments.

These principles and their associated commitments will govern data sharing under this intergovernmental agreement and the Work Program.

Baseline request and response requirements will describe how Trust Principles and Commitments will be met (see Schedule E).

Schedule D – Data Sharing Principles

The Parties agree to apply the Office of the National Data Commissioner (ONDC) Best Practice Guide to Applying Data Sharing Principles, as updated from time to time.

The Data Sharing Principles are based on the Five Safes Framework, which is an internationally recognised approach to disclosure risk management.

The five Data Sharing Principles are:

a) Project – data is shared for an appropriate purpose that delivers a public benefit.

b) People – the user has the appropriate authority to access the data.

c) Settings – the environment in which the data is shared minimises the risk of unauthorised use or disclosure.

d) Data – Appropriate and proportionate protections are applied to the data.

e) Outputs – the output from the data sharing arrangement is appropriately safeguarded before further sharing or release.

Different levels of controls should be applied under each of the principles depending on the context of the data sharing and its sensitivity.

Schedule E – Data request minimum information requirements

The following minimum information requirements will assist data requesters and custodians to make and action data requests, and identify appropriate controls using the Data Sharing Principles in Schedule D.

A data sharing agreement can be used to ensure the arrangement is appropriately authorised and governed. A data sharing agreement should always be used where identified data or de-identified data is proposed to be shared.

Data type	Requester information requirements	Custodian information provision
Routine administrative data (de-identified and aggregated) Statistics and reference data Emergency data (de-identified and identifiable) Identifiable data for joined up services Data and information to support existing IGAs	Baseline request requirements • Confirmation requested data is not readily available from other sources • Contact information of parties to the data request • Purpose(s) for use of data, with use case examples • Intended public interest from purported use • Data breakdown (e.g. variables needed by geography, cohort), where known • Timing information - dataset time periods, duration of need, critical delivery date • Advice on intended outputs • Advice on how DDMM Trust Principles (Schedule C) will be met under the data request • Proposed data transfer mechanism and security • Proposed data storage and access arrangements • Anticipated internal and external users, and on-sharing requirements • Data archiving and disposal plan	Baseline response requirements • Contact information for data custodian and data request approval processes • Advice on any legislative requirements relevant to the data request • Advice on the need for a Privacy Impact Assessment and/or a Security Impact Assessment • Advice on the need for formal ethics approval • Advice on dataset characteristics, including variables collected and any available metadata and definitions • Advice on how DDMM Trust Principles (Schedule C) will be observed in meeting the data request • Timeframe for approval and access • Advice on permissible and non-permissible uses of shared data • *(If the data request is rejected)* Reasoning for decision
Data for integration projects and cohort needs analysis (de-identified and identifiable)	Baseline request requirements <u>plus</u>: + Endorsement from an accredited integration authority/accredited data service provider + Evidence of engagement with affected communities (optional)	Baseline response requirements