Data Availability and Transparency Code 2022

Consultation paper

August 2022

Contents

1. Setting the scene: legislation and previous consultation

The *Data Availability and Transparency Act 2022* (**the Act**) establishes a new, best practice scheme for sharing Australian Government data – **the DATA Scheme**. The DATA Scheme is underpinned by strong safeguards and consistent, efficient processes. It is focused on increasing the availability and use of Australian Government data helping deliver better government services, policies and programs with people and businesses at the heart, and support world-leading research and development.

The National Data Commissioner (**the Commissioner**) is the regulator of the DATA Scheme and provides advice and guidance about its operation. The Commissioner also delivers education and support for best practice data handling and sharing.

In addition to the Act, the DATA Scheme is comprised of four types of legislative instruments:

- Regulations – The Minister may make regulations that prescribe details of when sharing is barred under the Act. For example, prescribing when a data custodian is prohibited from sharing data under the DATA Scheme.

- Rules – The Minister may make rules about matters necessary, or convenient, for giving effect to the DATA Scheme. For example, rules relating to the accredited user accreditation framework.

- Data codes – The Commissioner may make codes of practice about the DATA Scheme. As set out below, the Commissioner must first make a data code about certain topics, and following from this, can also make data codes about other matters necessary, or convenient, for giving effect to the DATA Scheme.

- Guidelines – The Commissioner may make guidelines to provide the Commissioner's view about DATA Scheme principles and processes.

The data code will be subject to Parliamentary scrutiny and can be disallowed. The data code, once made, will be binding on scheme entities (that is, data custodians, accredited users and accredited data service providers).

Legislative requirement

Under the Act, the Commissioner must make a data code about the following:

- The five data sharing principles set out in section 16 of the Act. These principles provide a statutory risk management framework which apply to how DATA Scheme participants negotiate and enter into data sharing agreements. Entities must ensure a data sharing project is consistent with the project, people, setting, data and output principles and appropriate safeguards required by the principles are in place. The Act sets out high level requirements for each principle. The data code is intended to provide more detail on how each principle is to be applied in practice.

- Privacy protections regarding the collection of consent and the limited circumstances in which it is permissible for a data sharing project to proceed without the collection of consent. These privacy protections include:
    - the requirements for how consent is to be collected from individuals. These requirements would apply to how express consent is collected for the sharing of biometric data, and how consent is collected for projects where the data sharing purpose is delivery of government services, informing government policy and programs, or research and development;
    - the circumstances in which it is permissible for a project to *not* collect individual consent because it is unreasonable and impracticable to seek consent. This is a limited exception and only applies to projects where the data sharing purpose is informing government policy and programs, or research and development;
    - the principles to be applied by a data custodian when determining whether it is necessary to share personal information to properly deliver a government service. This is an important privacy protection and compliments the 'data principle', which requires that only the data reasonably necessary to achieve the data sharing purpose is shared; and
    - additional public interest considerations a data custodian must take into account, where the Act permits a data sharing project to proceed on the basis of *not* collecting individual consent. The data code will set out considerations for custodians to take into account when determining whether the public interest to be served by a project justifies the sharing of personal information without consent.

In addition, the Commissioner can make a data code dealing with other matters about the DATA Scheme. The Commissioner is proposing that the data code require data sharing agreements to clarify which individuals are authorised to access shared data; specify the 31st of July each calendar year as the applicable date by which a data custodian must notify the Commissioner of certain information in relation to the preparation of the annual report; and specify information to be provided to the Commissioner to assist with the registration of data sharing agreements.

Previous consultation

The Office of the National Data Commissioner (**ONDC**) has taken into account feedback from previous consultation processes and submissions to develop the data code, including:

- an Issues Paper on DAT legislation released for public comment in July 2018;
- a series of roundtable forums to discuss the development of DAT legislation from July 2018 – June 2019;
- a Discussion Paper released for public comment in September 2019; and
- consultation on the exposure draft of DAT legislation from September – November 2020.

ONDC has also undertaken and completed three Privacy Impact Assessments on DAT legislation.

From these processes and submissions, scheme participants and others sought clarification on the handling of personal information under the DATA Scheme, the commercial use of data, data security and 'public benefit', including factors that must be considered to determine whether or not a data sharing project serves the public interest.

2. Summary: consultation approach

This consultation focuses on the Exposure Draft of the Data Availability and Transparency Code 2022 (**the draft data code**), particularly the data sharing principles and privacy protections. Ensuring the data code provides proper and pragmatic guidance, so that entities are able to apply and comply with the principles and privacy protections, is critical to fostering safe and trusted data sharing. ONDC invites feedback on these and other aspects of the draft data code to improve it.

This paper intended to be read together with the draft data code. Key sections of the Act are extracted throughout this paper and at Appendix A.

ONDC welcomes responses to all, or some, questions set out in this paper and other feedback. Please provide submissions to: information@datacommissioner.gov.au by 14 September 2022 and include 'Data Code Consultation Submission' in the subject line.

Submissions received from the consultation will be published on the ONDC website. However, organisations or individuals may request to have their submission published anonymously or not published. In these cases, the submission will be handled confidentially, subject to any legal requirements (such as in response to *Freedom of Information Act 1982* requests).

The Commissioner is aiming to make the data code by the end of 2022.

For any queries relating to the consultation paper, please contact: information@datacommissioner.gov.au.

3. Key terms

The following terms have been extracted from the Act (see Appendix A).

- accredited entity;
- accredited user;
- ADSP;
- complex data integration service;
- data custodian;
- DATA Scheme entity;
- data sharing agreement;
- data sharing purpose;
- de-identification data service;
- delivery of government services;
- entity;
- final output;
- output;
- personal information;
- project;
- secure access data service;
- use.

4. Data sharing principles

For data sharing to be authorised under the Act, the entities sharing, collecting or using the data must be satisfied the project is consistent with the five data sharing principles.

The data sharing principles are a statutory risk management framework that sit at the core of the Act. The purpose of the framework is to assess risks of sharing, collecting and using data and identify ways to manage those risks. The data sharing principles provide 'guardrails' for safe sharing, together with the robust privacy protections and accreditation framework under the DATA Scheme.

The data code will guide how the data sharing principles are to be applied. The principles become most relevant during the data sharing agreement negotiation process. Entities must work through the principles and confirm how the proposed agreement will apply, or comply, with each principle.

Some State and Territory data sharing regimes in Australia use variations of the data sharing principles. The data sharing principles embedded in the DATA Scheme are based on the internationally recognised Five Safes Framework, and have been adopted as a standard by Commonwealth, State and Territory Governments as part of the 2021 Intergovernmental Agreement on Data Sharing.

The data code seeks to establish best practice application of the data sharing principles and foster, over time, greater and consistent sharing between the Commonwealth, States and Territories.

The project principle

Under the DATA Scheme, the project principle is the linchpin to fostering public trust and confidence in the sharing of government data. Application of the project principle requires entities to be satisfied the project can reasonably be expected to serve the public interest, and that relevant ethics processes are observed.

What the Act states, section 16:

> *Project principle*
>
> (1) The project principle is that the project is an appropriate project or program of work.
>
> (2) The project principle includes (but is not limited to) the following elements:
>
> (a) the project can reasonably be expected to serve the public interest;
>
> (b) the parties observe processes relating to ethics, as appropriate in the circumstances.

Draft data code

The draft data code includes two sections on the project principle. The first section focuses on the requirement that a data sharing project is reasonably expected to serve the public interest. The second section focuses on applicable processes relating to ethics.

Project principle: Project reasonably expected to serve the public interest

Ensuring the data code enshrines a proper and pragmatic public interest test is of utmost importance. The draft data code is intended to assist data custodians and accredited users methodically work through public interest considerations.

Consideration of the 'public interest' and the balancing of factors for and against the public interest is standard practice in a number of Commonwealth legislative regimes. To maintain consistency, the Act uses the language of the 'public interest' rather than 'public benefit' (which is the language used in the Five Safes Framework).

Firstly, the draft data code clarifies that if the data sharing purpose is for the delivery of government services (subsection 15(1A) of the Act), the project can reasonably be expected to serve the public interest.

Secondly, the draft data code provides that where the project is for the data sharing purpose of informing government policy and programs, or research and development, the project can reasonably be expected to serve the public interest only if the entities conclude the arguments for the project serving the public interest *outweigh* the arguments against the project doing so. The draft data code provides a non-exhaustive list of considerations entities must take into account as part of the public interest 'weighing up' test. Entities can also take into account other relevant considerations.

Thirdly, the draft data code lists the types of projects that would *not* serve the public interest. For example, if the project does not serve the interests of Australian citizens, or if it exclusively serves the commercial interest of a private entity.

While there is public good in commercial interests, ONDC acknowledges the need to carefully balance what the community would be comfortable with, given some of the data is about individuals.

Consultation questions – Project principle: project reasonably expected to serve the public interest

1. Is the approach to weighing arguments for and against the project serving the public interest appropriate? If not, how else could entities assess whether a project for the purpose of informing government policy and programs, or research and development, serves the public interest?

2. If yes to the above, are the requirements of what entities must do, to weigh up arguments for and against the project serving the public interest, clear and unambiguous, and is this list proper and pragmatic? In your response, please provide reasons.

3. Is the list of projects that do not serve the public interest able to be practically applied? What, if any, further guidance is required to support entities consider when a project does not serve the public interest?

4. Are the notes contained in this section helpful, and would this section benefit from other illustrative examples provided as notes? If yes, what examples and under which subsections?

Project principle: applicable processes relating to ethics

Under the draft data code, entities must have regard to any process of ethics applicable. The draft data code seeks to make clear that entities can agree to apply *one* ethics process in circumstances where more than one ethics process applies to the proposed data sharing project. This pragmatic approach picks up feedback from earlier consultations.

Ethics processes may be applicable based on law or policy. Accordingly, data custodians must be able to identify relevant ethics processes related to the public sector data they manage, and accredited users must be able to identify relevant ethics processes related to the proposed project. A note has been included to assist entities identify what is an ethics process.

Consultation questions – Project principle: applicable processes relating to ethics

5. Under the draft data code, entities must have regard to **any** process of ethics applicable. Do you have any comments about this approach?

6. Is the note provided to assist entities identify ethics processes helpful? Why, or why not?

The people principle

Applying and complying with the people principle is about entities making sure individuals who have access to the data have the appropriate skills, knowledge, and capabilities for the data sharing project. Ensuring fit and proper people work on data sharing projects is an important control for safe data sharing.

What the Act states, section 16:

> *People principle*
>
> (3) The people principle is that data is made available only to appropriate persons.
>
> (4) The people principle includes (but is not limited to) the following elements:
>
> (a) access to data is only provided to individuals who have attributes, qualifications, affiliations or expertise appropriate for the access;
>
> (b) the entity sharing the data considers the following matters in relation to the entity collecting the data (the ***collector***):
>
> (i) the collector's experience with projects involving the sharing of public sector data, under this Act or otherwise;
>
> (ii) the collector's capacity to handle public sector data securely;
>
> (iii) any data breaches, or breaches of the law relating to data, by the collector;
>
> (iv) any other matters specified in a data code.

Draft data code

The draft data code includes two sections on how to apply or comply with the people principle. The first section focuses on conflicts of interest and what entities must do to identify

and manage conflicts of interest. The second section focuses on what is meant by 'appropriate persons' in relation to individuals authorised to access data.

The draft data code seeks to assist entities negotiating a data sharing agreement to consider human resourcing early on. For an accredited user, being able to demonstrate to a data custodian the proposed project will be staffed by appropriate persons could assist the efficiency of the negotiation process.

People principle: conflicts of interest

This element of the people principle includes an ongoing obligation on entities to identify, notify and manage conflicts of interest. Accordingly, an entity should consider conflicts of interest during the data sharing agreement negotiation process, and ensure ongoing compliance with conflict of interest obligations throughout the life of a data sharing project.

In circumstances where an individual's affiliations result in an actual, potential or perceived conflict of interest, that individual is not an appropriate person and should not be involved in the data sharing project unless the conflict is appropriately managed. Affiliations include, for example, sponsorships or scholarships or participation in talent programs.

The draft data code also makes clear that as part of satisfying itself that a project is consistent with this principle, a data custodian and any ADSP is entitled to assume that, if the accredited user is a Commonwealth body, a State or a Territory body, the accredited user has acted consistently with this principle.

The draft data code is not prescriptive on how entities must manage or reduce a conflict. This position appreciates that conflicts are best managed on a case-by-case basis. Where a project is already underway, the draft data code assumes in managing conflicts, entities will be pragmatic and, if appropriate, may suspend a project or exclude the relevant individual while risk mitigation action is being taken.

Consultation questions – People principle: conflicts of interest

7. Are the requirements of this element of the people principle clear and unambiguous? What, if any, further details or guidance could assist?

8. Is the example provided under this section helpful? Why, or why not?

People principle: appropriate persons

The draft data code sets out what types of attributes, qualifications, affiliations and expertise are to be taken into account in assessing if an individual is an appropriate person authorised to access data.

If an individual does *not* satisfy these criterion (for example, because they do not possess a necessary security clearance, or do not have relevant qualifications or expertise required by a data custodian's policy), they would not be an appropriate person and should not be involved in the data sharing project.

Consultation questions – People principle: appropriate persons

9. Are the attributes, qualifications and affiliations listed in this section appropriate and easy to understand?

10. Would this section of the draft data code benefit from other illustrative examples provided as a note? If yes, what examples and under which subsections?

The setting principle

The setting principle focuses on how entities propose to handle shared data. Working through this principle requires 'hands on' and practical consideration about the data handling life cycle (which includes stages such as transfer, transmission, storage, use, or destruction of data).

What the Act states, section 16:

> *Setting principle*
>
> (5) The setting principle is that data is shared, collected and used in an appropriately controlled environment.
>
> (6) The setting principle includes (but is not limited to) the following elements:
>
> (a) the means by which the data is shared, collected and used are appropriate, having regard to the type and sensitivity of the data, to control the risks of unauthorised use;
>
> (b) reasonable security standards are applied when sharing, collecting and using data.

Draft data code

This section is intended to clarify what are reasonable security standards for the purposes of paragraph 16(6)(b) of the Act.

Setting principle: Reasonable security standards

What is a reasonable security standard is best determined on a case-by-case basis, so the draft data code sets out that it is for entities to assess and agree on this standard, by having regard to the sensitivity of the data (for example, if the data includes personal information) and the risks posed by the proposed handling of the data (for example, the physical environment).

The draft data code's approach requires entities to take a holistic view of how the project is proposing to handle data. How data is handled can either increase or decrease risks. For example, if data is only to be accessed through the use of a secure access data service provided by an ADSP, this would be a less risky option than a proposal for an accredited user to store data in their IT system in circumstances where the user is undertaking an update of their IT systems.

This section provides discretion to require accredited entities, who are not Commonwealth bodies, to comply with relevant Commonwealth security standards.

Consultation questions – Setting principle: reasonable security standards

11. Is this section adequate in clarifying what are reasonable security standards?

12. Would this section benefit from an illustrative example provided as a note? If yes, what are some proposed examples?

The data principle

The data principle focuses on the data proposed to be shared under the DATA Scheme. Another way to think about this principle is as the 'Goldilocks principle'. Under a data sharing agreement, the entities should share 'just the right' amount of data. That is, only the data reasonably necessary to achieve the data sharing purpose, or purposes, should be shared.

Applying this principle also requires an entity to carefully consider, 'what else should be done to the data prior to it being shared?' For example, if the data requires any alteration so that only the right type and amount of data is shared.

What the Act states, section 16:

> *Data principle*
>
> (7) The data principle is that appropriate protections are applied to the data.
>
> (8) The data principle includes (but is not limited to) the element that only the data reasonably necessary to achieve the applicable data sharing purpose or purposes is shared, collected and used.

Draft data code

The draft data code sets out considerations for appropriately protecting data before it is shared by a data custodian and collected by an accredited user, and also sets out the test to determine if the data proposed to be shared is reasonably necessary for the project.

Data principle: appropriate protection – whether data should be altered

In practice, this section requires an entity to consider whether, before data is shared, it should be altered (for example, removing some of the data). In circumstances where a dataset contains data irrelevant to the accredited user's proposed project, alteration of data could be an appropriate protection and risk mitigation.

For example, a data custodian may determine only 40% of the data in an existing dataset is reasonably necessary for a project. In this circumstance, to comply with the data principle, the data custodian would need to alter the data to remove irrelevant data.

The note under this section signposts privacy protections in sections 16A and 16B of the Act and the requirements relating to de-identification data service and secure access data service in section 16C of the Act.

Consultation question – Data principle: appropriate protection – whether data should be altered

13. In practice, this element of the data principle, the privacy protections, and three data services set out in the Act, all work together to provide a framework to appropriately protect data. ONDC acknowledges there is a need to strike the right balance between taking a layered approach and not making the DATA Scheme too complex. Could the draft data code be improved to better assist entities apply this element of the data principle?

Data principle: appropriate protection - data sharing must be reasonably necessary

This element of the data principle requires entities to consider whether a reasonable person, who is properly informed, would conclude the data proposed to be shared, collected and used in the project is reasonably necessary to achieve the project's data sharing purpose or purposes. This is an objective test. The inclusion of the phrase, 'a reasonable person who is properly informed,' is intended to clarify the reasonable person test in this context involves a person who has baseline data literacy. That is, the person has the ability to read, understand, create and communicate data as information.

Whether the decision to conclude the data proposed to be shared, collected and used in the project is reasonable will depend on whether there are 'reasonable grounds' to support this decision. The High Court has observed that whether there are 'reasonable grounds' to support a course of action requires the 'existence of facts which are sufficient to persuade a reasonable person,' and involves 'an evaluation of the known facts, circumstances and considerations which may bear rationally upon the issue in question.'

The note under this section signposts privacy protections in sections 16A and 16B of the Act. As discussed above, a general privacy protection set out in subsection 16A(1) is that the sharing of personal information must be minimised as far as possible, without compromising the data sharing purpose of a project.

Consultation question – Data principle: appropriate protection - data sharing must be reasonably necessary

14. Is the 'reasonable person' test adequate in this section? If not, how could this section be improved to allow the entities to test whether the data proposed to be shared, collected and used is reasonably necessary to achieve the data sharing purpose?

The output principle

The output principle is concerned with what happens to data after it is shared by a data custodian. Put another way, the principle shines a spotlight on how the accredited user will use shared data.

To apply the output principle, entities must consider and agree how data will be used by the accredited user. Including, if applicable, if the accredited user will provide third parties access to the data, or any data that is the result or product of the user's use of the shared data. Should provision of access to third parties be proposed, Part 2.7 of the Act sets out what is required to authorise third party access by an accredited user and what a data sharing agreement must include.

What the Act states, section 16:

> *Output principle*
>
> (9) The output principle is that the only output of the project is the final output and output the creation of which is reasonably necessary or incidental to creation of the final output.
>
> (10) The output principle includes (but is not limited to) the following elements:
>
> (a) the data custodian of the data and the accredited user consider:
>
> (i) the nature and intended use of the output of the project; and
>
> (ii) requirements and procedures for use of the output of the project;
>
> (b) the final output contains only the data reasonably necessary to achieve the applicable data sharing purpose or data sharing purposes.

Draft data code

The draft data code includes one section on the output principle. 'Output' has a specific meaning under section 11A of the Act. In summary, output is a copy of the data collected by an accredited user and any data that is the result or product of the user's use of the shared data. Within the DATA Scheme, output has a meaning that relates solely to an accredited user. Where a data custodian shares public sector data with an accredited user, that data becomes 'output' once it is 'in the hands' of the accredited user.

Section 9 of the Act also defines 'final output', which is the agreed final output specified in the data sharing agreement for the project.

Output principle

The output principle brings to the fore the need for entities to negotiate how the shared data will be used. In working through the output principle and Part 2.7 of the Act, entities should identify how shared data will be used (for example, to inform a policy or research paper) and whether output is proposed to be provided by the accredited user to a third party.

This section of the draft data code sets out a non-exhaustive list of intended uses of the shared data (for example, data to be used in a pre-filled form). It also directs entities to Part 2.7 of the Act and sections about allowing access to output. The concept of access in these provisions refers to circumstances in which an accredited user is authorised to provide a third party with access to project output. For example, section 20B states that a data sharing agreement may allow the accredited user to provide another entity (e.g. a business, or an individual) with access to output to validate or correct the output. This mechanism could

arise in circumstances where an accredited user is wanting to confirm, with a business, that the data received from a data custodian about that business is correct.

Section 20E of the Act clarifies when output is taken to exit the DATA Scheme. When output exits the DATA Scheme, it ceases to be output and practically, this means the data is no longer regulated by the DATA Scheme. There are limited circumstances in which this can occur. The exit provisions in the Act set out the limited circumstances in which data shared through the DATA Scheme can exit and cease to be regulated. That said, the primary intention of the output principle in the data code is to focus the entities on working through the accredited user's proposed use of the shared data while it is regulated by the DATA Scheme.

Consultation question - Output principle

15. In practice, the output principle requires entities to agree how the accredited user will use shared data. Overall, how could the draft data code be improved to best assist entities apply the output principle?

5. Privacy protections

The Act complements the *Privacy Act 1988* (**the Privacy Act**). One of the objects of the Act is to enable the sharing of public sector data consistently with the Privacy Act.

The data code explains how the general and purpose specific privacy protections embedded in the Act are to be applied.

The general privacy protections are the protections that apply to all projects, irrespective of the data sharing purpose. Purpose specific privacy protections refer to privacy protections relevant to each of the three data sharing purposes under the DATA Scheme. That is, delivery of government services, informing government policy and programs, and research and development.

Where the data sharing project involves the sharing of biometric data, express consent is required.

Draft data code

Under section 126 of the Act, amongst other things, the Commissioner must make a data code about the general privacy protections and the purpose specific privacy protections, including when it could be unreasonable or impractical to seek an individual's consent.

The purposes of this part of the data code are to:

- set out requirements for consent under both sections 16A and 16B of the Act; and
- set out relevant principles in determining:
    - where the purpose of a project is the delivery of government services – whether sharing personal information is necessary to properly deliver a service; or
    - the public interest to be served by a project justifies the sharing of personal information without consent.

Privacy protections: Consent to sharing personal information

Section 16A and 16B of the Act sets out the circumstances when consent may support the sharing of personal information. Where consent is to be relied on, this section of the draft data code sets out requirements and what compliance involves.

The draft data code builds on the foundation provided by the Office of the Australian Information Commissioner and current privacy law guidelines on what constitutes consent. Namely, the draft data code requires that:

- the individual providing consent be adequately informed;
- consent be voluntary;
- the consent relate specifically to the sharing of data under the DATA Scheme;
- the consent is current at the time of sharing the data; and
- the consent is given by an individual who has capacity to consent, or otherwise given by a responsible person for the individual.

Under the draft data code, consent can be express or implied. However, withdrawal of consent must be express. Where the Act specifically requires consent to be express (for example, for the sharing of biometric data), express consent must be collected.

The draft data code clarifies that where consent is withdrawn, the effect of the withdrawal is to prevent sharing of data after, but not before, the withdrawal. The timing of an individual's withdrawal is a fact that determines whether consent is effective or ineffective. For example, if an individual withdraws their consent prior to a data custodian sharing their personal information, that withdrawal would be effective.

Privacy protections: Informing government policy and programs, and research and development - Unreasonable or impracticable to seek consent

This section of the draft data code applies to projects where the data sharing purpose is informing government policy and programs, or research and development.

Subsections 16B(4) and (7) of the Act set out limited circumstances in which a data custodian can share personal information without consent. One of these limited circumstances is that the project purpose cannot be achieved with the use of de-identified information and it is unreasonable or impracticable to seek the individual's consent.

This section of the draft data code sets out the considerations a decision-maker must take into account when deliberating whether it is unreasonable or impracticable to seek consent. Amongst other factors, one of the considerations is whether the data sharing relates to a serious threat or urgent situation.

This section makes clear it may be unreasonable or impracticable to seek consent if seeking consent would be excessively burdensome in all the circumstances, but that this exception does not apply merely because it would be inconvenient, time-consuming, incur-costs or because the consent of a very large number of individuals needs to be sought.

A data custodian has to be satisfied the conclusion it is unreasonable or impracticable to seek individual consent is defensible having regard to the considerations set out in this section of the draft data code. The relevant data sharing agreement needs to capture this decision.

Privacy protections: Delivering a government service – whether it is necessary to share personal information

This section of the draft data code is intended to provide further clarification for whether it is necessary to share personal information depending on the specific service that is being delivered. This guidance is intended to assist Commonwealth government service delivery agencies.

For example, if the government service is to provide information (paragraph 15(1A)(a) of the Act), then the information necessary to properly deliver the service is contact information for the individual and information relevant to the timing and/or content of the information to be provided to the individual. In another example, if the service is a service mentioned in paragraph 15(1A)(c) or 15(1A)(d) (determining eligibility for payment, entitlement, or benefit, or paying a payment entitlement, or benefit), and the service is provided under legislation, the information necessary to properly deliver the service is contact information for the individual and any information about the individual that could be lawfully taken into consideration under that legislation, and the accredited user proposes to take into account when delivering the service.

Privacy protections: Informing government policy and programs, and research and development – whether public interest justifies sharing of personal information without consent

This section of the draft data code applies to projects where the data sharing project involves the sharing of personal information for the purposes of informing government policy and programs, or research and development, and the individual has not provided consent for their personal information to be shared.

Subparagraph 126(2C)(b)(ii) of the Act requires that the data code list principles that should be applied by data custodians when determining the circumstances, or categories of circumstances, where the public interest to be served by a project justifies the sharing of personal information without consent.

This section requires that the data custodian weigh the benefits of the project to the public against any adverse impact to an individual caused by the sharing of the personal information, and only determine the sharing is justified if the benefit or benefits outweigh the adverse impact or impacts.

When making this assessment, the data custodian should have regard to all the relevant factors listed in this section, including whether the project relates to the prevention of, or response to, a serious threat to life, or to the health, safety, or welfare of the public, whether the project includes any safeguards to minimise the impact to the individual, and the social, economic, environmental, cultural, or other costs to sharing, collecting and using the data.

Consultation questions - Privacy protections

16. One of the objects of the Act is to enable the sharing of data consistently with the Privacy Act and appropriate safeguards. Does this part of the draft data code strike the right balance between holding data custodians accountable to seek consent, and providing data custodians with an exception to collect consent in circumstances where it is genuinely unreasonable or impracticable to seek consent? How could the draft data code be improved to achieve the right balance? For example, could the National Health and Medical Research Council waiver of consent guidelines be used here?

17. Is this part of the draft data code adequate in providing further clarification for what considerations should be taken into account when determining whether it is necessary to share personal information to properly deliver a government service? How could this section be improved?

18. Does this part of the draft data code provide an adequate list of factors for data custodians to consider when determining whether the public interest justifies the sharing of personal information without consent? Would this section benefit from an example provided in a note, and if so, can you suggest one?

6. Data sharing agreements

Under section 19(16) of the Act, a data sharing agreement must meet any other requirements prescribed by a data code.

Draft data code – designated individuals

The draft data code states that a data sharing agreement must require an accredited user to ensure shared data is only accessed by 'designated individuals' for the accredited user and that these individuals either:

- are Australian citizens or permanent residents, or
- where an individual is not an Australian citizen or permanent resident, the individual's full name, nationality, relationship to the accredited user (for example, employee) and a description of their role in the project, is set out in the data sharing agreement.

Who is a 'designated individual' is set out in section 123 of the Act. A designated individual is a person who has a legal relationship ('designation') to an accredited user. For example, an employee, a contractor or an agent.

This additional data sharing requirement is intended to complement the people principle.

Draft data code – non-Australian designated individuals for Australian universities

This section also sets out further requirements if the designated individual is a foreign employee, contactor, or agent of an Australian university.

One of the recommendations from the Senate Finance and Public Administration Legislation Committee Report on the DAT Bill package was that findings of the *Inquiry into National Security Risks Affecting the Higher Education and Search Sector* (the Inquiry) be taken into account when developing data codes and guidance material under the DATA Scheme. On 25 March 2022, the Parliamentary Joint Committee on Intelligence and Security released their report containing 27 recommendations, which cover greater transparency, accountability, training, reporting to government, and enhanced due diligence on international research partnerships and grants.

This section of the draft data code reflects a number of recommendations arising from the Inquiry.

Consultation question - Data sharing agreements

19. Should the data sharing agreement include any additional details about the designated individual who is a foreign national?

7. Miscellaneous

The following additions to the draft data code deal with matters the Commissioner considers necessary or convenient to deal with for carrying out, or giving effect to the DATA Scheme.

Draft data code – information to be provided upon registration

Subsection 33(1) of the Act provides that a data custodian must give the Commissioner an electronic copy of the data sharing agreement within 30 days after the agreement is made. Subsection 33(2) provides that the data custodian must also give the Commissioner any other information or documents required by a data code. These steps are intended to assist the Commissioner to register the agreement.

This section of the draft data code is informed by the list prescribed under section 130 of the Act, which deals with information that must be included in the public register of data sharing agreements. This will assist the Commissioner to have all the required information on hand, rather than having to request further information from the data custodian once the data sharing agreement is ready to be registered.

Draft data code – applicable period for notifying Commissioner of certain information

Subsection 34(2) of the Act provides that a data custodian must give the Commissioner any other information and assistance reasonably required in relation to the preparation of the annual report mentioned in section 138. Subsection 34(4) provides that the period for notifying the Commissioner is the period applicable under a data code.

The effect of this section in the draft data code is that accredited entities must provide this information by 31 July each year. The information to be provided to the Commissioner is information about the previous financial year, that is, 1 July to 30 June.

Consultation questions - Miscellaneous

20. This part of the draft data code is informed by the list prescribed in section 130 of the Act. Is this an appropriate approach, and are there any additional details that should be provided to the Commissioner outside of that list?

21. Is 31 July an appropriate deadline for data custodians to provide information and assistance to the Commissioner to prepare for the annual report?

8. Potential additions to the data code

In accordance with section 126 of the Act, set out below are other topics that could be included in the data code:

- how provisions in Chapter 2 (Authorisations) and Chapter 3 (Responsibilities of DATA Scheme entities) of the Act are to be applied, or complied with;
- any additional requirements, other than those imposed by Chapters 2 and 3 of the Act; and
- the handling and management of complaints.

The Commissioner may also make a code about other matters necessary, or convenient, for giving effect to the DATA Scheme.

Consultation question - Potential additions to the data code

22. What additional topics could the data code include to assist the establishment or integrity of the DATA Scheme?

9. Summary of consultation paper questions

Consultation questions – Project principle: project reasonably expected to serve the public interest

1. Is the approach to weigh arguments for and against the project serving the public interest appropriate? If not, how else could entities assess whether a project for the purpose of informing government policy and programs, or research and development, serves the public interest?

2. If yes to the above are the requirements of what entities must do, to weigh up arguments for and against the project serving the public interest, clear and unambiguous, and is this list proper and pragmatic? In your response, please provide reasons.

3. Is the list of projects that do not serve the public interest able to be practically applied? What, if any, further guidance is required to support entities consider when a project does not serve the public interest?

4. Are the notes contained in this section helpful, and would this section benefit from other illustrative examples provided as notes? If yes, what examples and under which subsections?

Consultation questions – Project principle: applicable processes relating to ethics

5. Under the draft data code, entities must have regard to **any** process of ethics applicable. Do you have any comments about this approach?

6. Is the note provided to assist entities identify ethics processes helpful? Why, or why not?

Consultation questions – People principle: conflicts of interest

7. Are the requirements of this element of the people principle clear and unambiguous? What, if any, further details or guidance could assist?

8. Is the example provided under this section helpful? Why, or why not?

Consultation questions – People principle: appropriate persons

9. Are the attributes, qualifications and affiliations listed in this section appropriate and easy to understand?

10. Would this section of the draft data code benefit from other illustrative examples provided as a note? If yes, what examples and under which subsections?

Consultation questions – Setting principle: reasonable security standards

11. Is this section adequate in clarifying what are reasonable standards?

12. Would this section benefit from an illustrative example provided as a note? If yes, what are some proposed examples?

Consultation question – Data principle: appropriate protection – whether data should be altered

13. In practice, this element of the data principle, the privacy protections, and three data services set out in the Act, all work together to provide a framework to appropriately protect data. ONDC acknowledges there is a need to strike the right balance between taking a layered approach and not making the DATA Scheme too complex. Could the draft data code be improved to better assist entities apply this element of the data principle?

Consultation question – Data principle: appropriate protection - data sharing must be reasonably necessary

14. Is the 'reasonable person' test adequate in this section? If not, how could this section be improved to allow the entities to test whether the data proposed to be shared, collected and used is reasonably necessary to achieve the data sharing purpose?

Consultation question – Output principle

15. In practice, the output principle requires entities to agree how the accredited user will use shared data. Overall, how could the draft data code be improved to best assist entities apply the output principle?

Consultation questions - Privacy protections

16. One of the objects of the Act is to enable the sharing of data consistently with the Privacy Act and appropriate safeguards. Does this part of the draft data code strike the right balance between holding data custodians accountable to seek consent, and providing data custodians with an exception to collect consent in circumstances where it is genuinely unreasonable or impracticable to seek consent? How could the draft data code be improved to achieve the right balance? For example, could the National Health and Medical Research Council waiver of consent guidelines be used here?

17. Is this part of the draft data code adequate in providing further clarification for what considerations should be taken into account when determining whether it is necessary to share personal information to properly deliver a government service? How could this section be improved?

18. Does this part of the draft data code provide an adequate list of factors for data custodians to consider when determining whether the public interest justifies the sharing of personal information without consent? Would this section benefit from an example provided in a note, and if so, can you suggest one?

Consultation questions - Data sharing agreements

19. Should the data sharing agreement include any additional details about the designated individual who is a foreign national?

Consultation questions - Miscellaneous

20. This part of the draft data code is informed by the list prescribed in section 130 of the Act. Is this an appropriate approach, and are there any additional details that should be provided to the Commissioner outside of that list?

21. Is the 31 July an appropriate deadline for data custodians to provide information and assistance to the Commissioner to prepare for the annual report?

Consultation question - Potential additions to the data code

22. What additional topics could the data code include to assist the establishment or integrity of the DATA Scheme?

10. Appendix A – Key terms

Accredited entity / accredited user / ADSP

11 Entity definitions

(4) An entity accredited under section 74 as an:

(a) accredited user (an ***accredited user***); or

(b) ADSP (short for accredited data service provider) (an ***ADSP***);

is an ***accredited entity***.

Note 1: Accredited users are able to collect and use shared data (including by creating output they can provide other entities with access to, or release) in accordance with an applicable data sharing agreement. ADSPs are expert intermediaries who can assist data custodians to prepare and share data appropriately.

Note 2: Excluded entities cannot be accredited (see subsection 74(1)).

Complex integration data service

16D Project involving complex data integration services

(3)A service to integrate data is a ***complex data integration service*** if:

(a) 2 or more entities control the data being integrated; and

(b) the data is at the unit or micro level; and

(c) any of the following subparagraphs applies to any of the data to be integrated, or to the integrated data:

(i) the data includes personal information;

(ii) the data includes commercially sensitive information (including trade secrets) about the business, commercial, or financial affairs of an organisation;

(iii) the data includes information that is not publicly available about an industry or sector that forms part of the Australian economy;

(iv) the data includes information about one or more persons or things the data custodian of the data considers to be vulnerable or sensitive;

(v) the data is to be used for more than one project;

(vi) the data meets conditions prescribed by the rules; and

(d) the data to be integrated, or the integrated data, has any of the characteristics prescribed by the rules (if any).

Data custodian

11 Entity definitions

(2) An entity is a ***data custodian*** if the entity:

(a) is a Commonwealth body; and

(b) is not an excluded entity; and

(c) either:

(i) controls public sector data (whether alone or jointly with another entity), including by having the right to deal with that data; or

(ii) has become the data custodian of output of a project in accordance with section 20F.

(2A) If a data custodian of public sector data shares the data with an intermediary under section 13 as part of a project, the data custodian is taken also to be the data custodian of any ADSPenhanced- data of the project.

(3) Each of the following is an ***excluded entity***:

(aa) the National Data Commissioner and any APS employee made available to the National Data Commissioner under section 47;

(a) the Australian Commission for Law Enforcement Integrity;

(b) the agency known as the Australian Criminal Intelligence Commission established by the *Australian Crime Commission Act 2002*;

(ba) the Australian Federal Police;

(c) that part of the Defence Department known as the Australian GeospatialIntelligence- Organisation;

(d) the Australian National Audit Office;

(e) the Australian Secret Intelligence Service;

(f) the Australian Security Intelligence Organisation;

(g) the Australian Signals Directorate;

(h) that part of the Defence Department known as the Defence Intelligence Organisation;

(i) the InspectorGeneral- of Intelligence and Security;

(j) the Office of the Commonwealth Ombudsman;

(k) the Office of National Intelligence.

DATA Scheme entities

11 Entity definitions

(1) The following are ***DATA Scheme entities***:

(a) data custodians of public sector data;

(b) accredited entities.

Data sharing agreement

18 Data sharing agreement

(1) An agreement is a ***data sharing agreement*** if:

(a) the agreement relates to the sharing of public sector data; and

(b) the parties to the agreement include a data custodian of public sector data and an accredited user; and

(c) the agreement is in the approved form (if any) or in writing (if there is no approved form); and

(d) any requirements specified in a data code are met in relation to the agreement.

Note 1: All data sharing agreements must also meet the requirements in section 19. Other provisions also impose requirements in certain circumstances (see for example sections 16B and 16C).

Note 2: DATA Scheme entities must also have regard to the guidelines (see section 27) in entering a data sharing agreement.

Note 3: Copies of data sharing agreements, including variations, must be given to the Commissioner (see section 33) for inclusion on the register of data sharing agreements under section 130. Certain details of the agreements must be made publicly available.

(2) A data sharing agreement must not be entered into by an individual on behalf of a data scheme entity unless the individual is an authorised officer of the entity or authorised under subsection 137(4) for the entity.

(3) A variation of a data sharing agreement must not be entered into by an individual on behalf of a data scheme entity unless the individual is an authorised officer of the entity or authorised under subsection 137(3) or (4) for the entity.

(4) A data sharing agreement has no effect until the agreement is registered.

(5) A variation of a data sharing agreement has no effect (and the agreement as in effect before the variation continues in effect) until the variation, or the agreement as varied, is registered.

(6) A data sharing agreement may deal with matters not required to be dealt with by this Act, but must not do so in a way that is inconsistent with the data sharing scheme.

19 Requirements to be met by all data sharing agreements

(1A) The requirements in this section must be met by all data sharing agreements.

Note: There are other requirements that, depending on the nature of the project, must be met by some data sharing agreements. See sections 16A and 16B.

(1) The parties to the agreement must be identified in the agreement.

(2) The agreement must describe the project and specify that this Act applies to the project.

(3) The agreement must specify:

(a) the public sector data that the data custodian is to share (including any ADSPenhanced- data an ADSP is to share on behalf of the data custodian) (the ***source data***); and

(b) the output of the project that the data custodian and accredited user agree is to be the final output.

(4) The agreement must:

(a) specify the data custodian of the source data; and

(b) if the agreement appoints a Commonwealth body as data custodian of output of the project in accordance with section 20F—specify the output and explain why the appointment has been made.

Note: If the accredited user is a Commonwealth body, the agreement may appoint the accredited user as the Commonwealth body that is to be data custodian of the output.

(5) The agreement must specify the title of any law that the sharing would contravene but for section 23 (authorisation to share overrides other laws).

(6) The agreement must:

(a) specify:

(i) the data sharing purpose, or data sharing purposes, of the project; and

(ii) if, under the agreement, the accredited user is to be allowed to use output of the project for any purpose incidental to that purpose or those purposes—any such incidental purpose; and

(b) except in relation to any use of the output allowed in accordance with section 20D—prohibit the accredited user from collecting and using output of the project for any of the following:

(i) any purpose not specified;

(ii) any precluded purpose.

(6A) The agreement must prohibit the accredited user from creating output of the project, other than:

(a) the final output; and

(b) output the creation of which is reasonably necessary or incidental to creation of the final output.

(7) The agreement must specify how the project will be consistent with the data sharing principles, including by:

(a) describing how the public interest is served by the project; and

(b) specifying the actions the party will take to give effect to the principles.

(8) If the sharing is being done through an ADSP, the agreement must:

(a) specify any data services the ADSP is to perform in relation to public sector data shared with the ADSP by the data custodian; and

(b) specify the circumstances in which the ADSP is to share, with the accredited user on behalf of the data custodian, ADSP-enhanced data of the project; and

(c) prohibit the ADSP from providing access to, or releasing, the ADSP-enhanced data in any other circumstances (if any) specified in the agreement.

(8) For the purposes of paragraph (8)(c), the only other circumstances that may be specified in the agreement are those allowed by section 20A.

(9) The agreement must:

(a) describe in general terms the use to be made by the accredited user of the output of the project; and

(b) prohibit the accredited user from using the output in a way that is inconsistent with the description; and

(c) prohibit the accredited user from providing access to, or releasing, the output in any circumstances other than circumstances (if any) specified in the agreement.

(10) For the purposes of paragraph (9)(c), the only circumstances that may be specified in the agreement are those allowed by section 20A, 20B, 20C or 20D.

(11) The agreement must prohibit the accredited entities that are party to the agreement from doing anything inconsistent with the conditions of accreditation imposed on or applicable to the entity from time to time.

(12) If section 37 applies in relation to sharing under the agreement and the agreement does not provide that subsections 37(2) and (3) are not to apply, the agreement must specify that those subsections apply.

(12A) If the parties agree to responsibilities in relation to data breaches additional to those under Part 3.3, the agreement must set out those responsibilities.

(13) The agreement must specify the circumstances in which it may be varied or terminated and how a variation or termination is to be done.

(14) The agreement must specify either or both of the following:
(a) its duration;
(b) the intervals at which the parties must review it.

(15) The agreement must provide for how scheme data covered by the agreement is to be dealt with when the agreement ends.

(16) The agreement must meet any other requirements prescribed by a data code for the purposes of this subsection.

(17) The agreement must require the data custodian of the source data to give the Commissioner written notice of the cessation of the agreement, as soon as practicable after the agreement ceases be in effect.

Data sharing purpose / delivery of government services

15 Data sharing purposes

Data sharing purposes

(1) The following are ***data sharing purposes***:
(a) delivery of government services;
(b) informing government policy and programs;
(c) research and development.

Note: Data sharing agreements must specify the agreed data sharing purpose or purposes and agreed incidental purposes (if any), and prohibit collection or use of data for any other purpose, including any precluded purpose.

Delivery of government services

(1A) For the purposes of paragraph (1)(a), ***delivery of government services*** means the delivery of any of the following services by the Commonwealth or a State or Territory:
(a) providing information;
(b) providing services, other than services relating to a payment, entitlement or benefit;

(c) determining eligibility for a payment, entitlement or benefit;
(d) paying a payment, entitlement or benefit.

Note: Making a decision under legislation about whether an individual is eligible to receive a payment, before any payment is made, is an example of delivery of government services. The purpose of making such a decision is not a precluded purpose.

Precluded purposes

(2) The following are ***precluded purposes***:
(a) an enforcement related purpose;
(b) a purpose that relates to, or prejudices, national security within the meaning of the *National Security Information (Criminal and Civil Proceedings) Act 2004*;
(c) a purpose prescribed by the rules for the purposes of this paragraph.

(3) An ***enforcement related purpose*** means any of the following purposes:
(a) detecting, investigating, prosecuting or punishing:
(i) an offence; or
(ii) a contravention of a law punishable by a pecuniary penalty;
(b) detecting, investigating or addressing acts or practices detrimental to public revenue;
(c) detecting, investigating or remedying serious misconduct;
(d) conducting surveillance or monitoring, or intelligencegathering- activities;
(e) conducting protective or custodial activities;
(f) enforcing a law relating to the confiscation of proceeds of crime;
(g) preparing for, or conducting, proceedings before a court or tribunal or implementing a court/tribunal order.

Note: The purpose of verifying that a government payment previously made to a person was correctly made is an example of an enforcement related purpose. Other examples include the purpose of recovering overpayments, identifying individuals for compliance activity and identifying individuals for the purposes of exercising statutory investigation powers.

(4) A purpose is not a ***precluded purpose*** within the meaning of paragraph (2)(a) or (b) if the purpose is both:
(a) a data sharing purpose; and
(b) a purpose that:
(i) is with respect to matters that relate only in a general way to a purpose mentioned in paragraph (2)(a) or (b); and
(ii) does not involve any person undertaking an activity mentioned in a paragraph of subsection (3).

Preparing data for a later project

(5) A project that involves sharing, collecting and using data in order to prepare (including to create) data for sharing under section 13 as part of a later project that will be for one or more of the data sharing purposes is itself taken to be a project for that or those data sharing purposes.

(6) Subsection (5) applies regardless of whether the entities sharing, collecting and using the data have a particular later project in mind and whether the data is actually shared under section 13 as part of any later project.

De-identification data service

16C Project involving use of de-identification or secure access data services

(3) A ***de-identification data service*** is a service to treat data that includes personal information so that the data is de-identified, using techniques that restrict the data being used in a way that would have the result that the data ceases to be de-identified.

Entity

entity means any of the following:

(a) a Commonwealth body, a State body or a Territory body;
(b) a body politic;
(c) an Australian university;
(d) a body corporate;
(e) an individual.

Final output

final output of a project means the output specified as the agreed final output in the data sharing agreement for the project (see paragraph 19(3)(b)).

Output / Project

11A The data sharing project

Project, and output and ADSPenhanced- data of project

(1) A ***project*** involves at least both of the following elements:
(a) an entity (the ***sharer***) shares data with another entity (the ***user***), either directly or through another entity (the ***intermediary***);
(b) the user collects the data and uses the ***output*** of the project, which is:
(i) the copy of the data collected by the user; and
(ii) any data that is the result or product of the user's use of the shared data.

Note 1: The sharer's authorisation to share data is in section 13. The user's authorisation to collect and use data is in section 13A.

Note 2: A project may involve sharing of data by multiple sharers, if multiple entities are data custodians of the data.

(2) If, for the purposes of sharing data under section 13, data services are performed in relation to data, or data is created, by or on behalf of the sharer, the ***project*** also involves performing the services or creating the data.

(3) If the sharer shares data with the user through an intermediary, the ***project*** also involves both of the following elements:
(a) the sharer shares the data with the intermediary;
(b) the intermediary collects the data and uses the ***ADSPenhanced- data*** of the project, which is:
(i) the copy of the data collected by the intermediary; and

(ii) any data that is the result or product of the intermediary's use of the shared data.

Note: The sharer's authorisation to share data with the intermediary, and the intermediary's authorisation to share data with the user on behalf of the sharer, are in section 13. The intermediary's authorisation to collect data from the sharer and use it is in section 13B.

(4) If the sharer is provided with access to output or ADSPenhanced- data of the project, the ***project*** also involves the sharer's collection and use of the output or ADSPenhanced- data.

Note: The sharer's authorisation to collect and use the output or ADSPenhanced- data of the project is in section 13C.

Combining projects

(5) A data sharing agreement may treat multiple projects as a single project, as long as they all have the same data sharing purpose or purposes and the same sharer and user and (if applicable) intermediary.

Successive projects

(6) If the user in a project shares data that is output of the project as part of a later project:

(a) the copy retained by the user continues to be output of the earlier project; and

(b) the copy collected by the user in the later project is output of the later project in accordance with paragraph (1)(b); and

(c) if the sharing in the later project is done through an intermediary—the copy collected by the intermediary in the later project is ADSPenhanced- data of the later project in accordance with paragraph (3)(b).

Note: A data sharing agreement may allow the user to share output under section 13 as part of a later project (see section 20D).

Personal information

personal information has the same meaning as in the *Privacy Act 1988*.

Note: Information that has been de-identified is no longer personal information.

Secure access data service

16C Project involving use of de-identification or secure access data services

(4) A ***secure access data service*** is:

(a) the service of providing ADSP-controlled access; or

(b) any other service that enables an entity to access data under the control of another entity and that includes controls to prevent or minimise the risk of the data being misused.

Use

use includes handle, store and provide access.

Note: Examples of use of data by an accredited user include developing and modifying output.