REPLACEMENT EXPLANATORY STATEMENT

Issued by the authority of the National Data Commissioner

Data Availability and Transparency Act 2022

Data Availability and Transparency Code 2022

Purpose and operation

This replacement explanatory statement accompanies the *Data Availability and Transparency Code 2022* (the **Code**).

The *Data Availability and Transparency Act 2022* (the **Act**) commenced on 1 April 2022. The Act established a new data sharing scheme (the **scheme**) for sharing safely Australian Government data with entities accredited under the scheme. The National Data Commissioner (the **Commissioner**) is appointed under the Act as an independent regulator of the scheme. The Commissioner is authorised to make (and in some cases is required to make) codes of practice about the scheme (**data codes**). Data codes may set out how definitions in the Act are to be applied and may impose additional requirements on data scheme participants so long as those requirements are not contrary to, or inconsistent with, the Act. Section 26 of the Act provides that a data scheme entity must comply with a data code.

Section 126 of the Act requires the Commissioner to make a code about the data sharing principles under section 16 of the Act and the privacy protections in sections 16A and 16B of the Act. The Code complies with these requirements. The Code also covers other privacy related matters, matters relating to the registration of data sharing agreements and specifies timing requirements for the notification of certain information to the Commissioner. The Code helps ensure that data scheme entities apply the requirements imposed by the scheme in a consistent manner.

No entities are yet accredited as users under the Act and, accordingly, no data has yet been shared under the scheme.

Authority

The Code is made by the Commissioner under section 126 of the Act.

The Code is a legislative instrument that is subject to disallowance.

Background

The scheme authorises the controlled sharing of Australian Government data in certain circumstances, for one of three data sharing purposes (the delivery of government services; informing government policy and programs; and research and development). Most, but not all, Australian Government departments and agencies that control Australian Government data are 'data custodians', and may share the data they control with accredited users under a registered data sharing agreement, subject to specific limitations and controls in the Act. Data may be shared with accredited users directly, or through Accredited Data Service Providers (**ADSPs**), acting as intermediaries (ADSPs are specialist data service providers). The only entities that may be accredited as users or ADSPs are the Commonwealth and Commonwealth bodies, State and Territory governments and their bodies, and Australian universities. Participants in the scheme, including data custodians, accredited users and ADSPs are collectively known as 'data scheme entities'.

The Act establishes a risk management framework comprising five data sharing principles. Data may only be shared, collected and used under the Act if the parties to a data sharing agreement are satisfied the data sharing project is consistent with the data sharing principles. The Code includes details about how these data sharing principles must be applied.

The Act includes a number of general privacy protections in section 16A. The Act includes further privacy protections in section 16A that vary depending on the data sharing purpose of the data sharing project. The Code includes details about how these privacy protections are to be applied, and where the consent of an individual is required under other provisions of the Act.

The Act promotes transparency by establishing a public register of data sharing agreements covered by the scheme. The Code establishes certain requirements for the information to be provided to the Commissioner when a data custodian gives a data sharing agreement to the Commissioner for registration.

Consultation

Before the Code was made, the Commissioner was satisfied that consultation was undertaken to the extent appropriate and reasonably practicable, in accordance with section 17 of the *Legislation Act 2003*.

Between 17 August and 14 September 2022, the Commissioner consulted publicly on an exposure draft of the Code (the **exposure draft**), which was available on the Office of the National Data Commissioner's website. The Commissioner invited submissions from members of the public including any interested stakeholders.

The Commissioner received 37 submissions during consultation, which provided feedback on a variety of matters, including about the public interest test, ethics processes, conflicts of interest, appropriate protections, appropriate persons and consent. These submissions were considered and informed the drafting of the Code. The submissions were made by a wide range of stakeholders, from Federal and State agencies, departments and data experts, through to concerned organisations and individuals. The Commissioner also consulted with experts on technical issues.

In response to the submissions and consultation process, a number of changes were made to the exposure draft of the Code. These changes included the following:

- The wording of the public interest test in section 6 was amended to clarify and simplify its operation, and it was separated into factors that 'must' and 'may' be considered.
- The interaction between ethics tests outside the Act, and those required by the Act, has been clarified through amendments to section 7.
- The provisions on conflicts of interest were improved to clarify the language.
- The provisions relating to appropriate protections were also improved to clarify its operation and application.
- Additional guidance in the Code is provided about how consent can be determined, especially for sections 20C, 20E and 20F of the Act.
- The provisions on appropriate persons were amended to separate out the factors that enhance and detract from a person being considered appropriate.

The provisions in the exposure draft of the Code addressing issues associated with foreign nationals accessing shared data have been included in a separate code, the *Data Availability and Transparency (National Security Measures) Code 2022*.

Statement of Compatibility with Human Rights

A Statement of Compatibility with Human Rights for the purposes of Part 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011* is set out at the end of this document.

Impact Analysis

The Productivity Commission's *Inquiry Report into Data Availability and Use* (2017) has been certified as being informed by a process and analysis equivalent to an impact analysis for the purposes of the Government decision to implement this legislative instrument. The Productivity Commission's report can be found at this link: www.pc.gov.au/inquiries/completed/data-access/report (OIA reference **OIA22-02632**).

Explanation of provisions

Part 1—Preliminary

Section 1 - Name

1. Section 1 provides that the name of the instrument is the *Data Availability and Transparency Code 2022*.

Section 2 - Commencement

2. Section 2 provides that the Code commences the day after it is registered on the Federal Register of Legislation.

Section 3 - Authority

3. Section 3 provides that the Code is made under section 126 of the *Data Availability and Transparency Act 2022*.

Section 4 - Definitions

4. Section 4 provides for definitions of **Act** which means the *Data Availability and Transparency Act 2022*, and **permanent resident** which has the same meaning as in the *AusCheck Act 2007*. In addition, section 4 includes a definition for **data accessor**. **Data accessor** is defined to mean either a designated individual for the entity who is permitted to access data under the data sharing agreement; or a body corporate who is permitted to access data under a data sharing agreement as a result of an approved contract. This definition is used in sections 8 to 10, to ensure those provisions also apply to individuals who are parties to a data sharing agreement as a result of an approved contract.

5. Section 4 also explains that some terms used in the Code are defined in the Act. Important terms used in the Code that are defined in the Act are *accredited entity, accredited user, ADSP, approved contract, ADSP-enhanced data, data custodian, data scheme entity, data sharing agreement, data sharing purpose, delivery of government services, designated individual, entity, output; personal information, project, and use*. These terms have the same meaning in the Code as in the Act.

Part 2—Data sharing principles

Section 5 - Purpose of Part

6. Section 5 of the Code provides the purpose of Part 2 of the Code, which is to set out matters to be taken into account, and requirements to be complied with, by a data scheme entity in satisfying itself that a project is consistent with the data sharing principles. The section explains that the Act requires data scheme entities sharing, collecting or using the data as part of a data sharing project to be satisfied (among other things) that the project is consistent with the data sharing principles.

Project Principle

7. Sections 6 and 7 of the Code set out requirements in relation to the **project principle**. Subsection 16(1) of the Act provides that the project must be an appropriate project or program of work. Subsection 16(2) of the Act provides that the project principle includes, but is not limited to, whether the project can reasonably be expected to serve the public interest, and whether the parties observe processes relating to ethics. This principle helps Scheme participants to understand when a project is an appropriate project or program of work for the purposes of the Act.

Section 6 - Project principle—project reasonably expected to serve the public interest

8. Section 6 of the Code sets out matters that may be considered and matters that must be considered when determining whether a project is reasonably expected to serve the public interest. This helps clarify how to determine if a project is in the public interest for the purposes of paragraph 16(2)(a) of the Act.

9. Subsection 6(1) of the Code provides that an entity must take into account the matters, and comply with the requirements, set out in this section when satisfying itself that a project is consistent with the project principle set out in subsection 16(1) of the Act, including the element set out in paragraph 16(2)(a) of the Act.

10. The note at the end of subsection 6(1) of the Code provides that, in accordance with subsection 16(11) of the Act, a data scheme entity must be satisfied that it has applied each of the data sharing principles to the sharing, collection or use of data in such a way that, when viewed as a whole, the associated risks are appropriately mitigated. This refers to subsection 16(11) of the Act, which provides that the data sharing principles can be considered in a holistic way. For instance, if a project has a high level of controls under the setting principle, then it may not be necessary to have the same level of controls when considering the people principle.

11. Subsection 6(2) of the Code provides that a project can reasonably be expected to serve the public interest if delivery of government services is the only data sharing purpose of the project. The term 'delivery of government services' is defined in subsection 15(1A) of the Act to mean the delivery of services by the Australian Government, or by a government of a State or a Territory, including providing information and services, and determining eligibility and payment of an entitlement or benefit. As a project delivering government services has already been assessed and approved through usual processes by the relevant government, it is reasonable to expect they would serve the public interest and it is not necessary for them to be reassessed against the public interest test under section 6 of the Code if this is their only purpose.

12. Subsection 6(3) of the Code applies to projects where the data sharing purpose includes informing government policy and programs, or research and development (including if delivery of government services is a joint data sharing purpose).

13. Paragraph 6(3)(a) of the Code provides that projects for these data sharing purposes can reasonably be expected to serve the public interest under the Act if the data custodian is sharing the data in the course of medical research within the meaning of the *Privacy Act 1988* (**Privacy Act**) and in accordance with guidelines made under section 95 of the Privacy Act. This recognises that Human Research Ethics Committees already apply a rigorous public interest test for medical research projects, as set out in *Guidelines approved under section 95A of the Privacy Act 1988*.

14. Subsection 6(3)(b) of the Code provides that a project under subsection 6(3) must also meet the following conditions:
    - the user must be an organisation within the meaning of the Privacy Act;
    - the data to be shared must be health information within the meaning of that Act; and

- a permitted health situation within the meaning of that Act must exist or will exist in relation to the user's use of the data.

These criteria mean these projects, which have already met a rigorous public interest assessment, do not need to also undergo a further consideration against the public interest test under section 6 of the Code.

15. Subsection 6(4) of the Code applies to projects where one of the data sharing purposes is informing government policy and programs, or research and development (including if delivery of government services is also a data sharing purpose). It provides that if subsection (3) does not apply, the project can reasonably be expected to serve the public interest only if the entity concludes that the arguments for the project serving the public interest outweigh the arguments against, clarifying for Scheme participants how to apply the public interest test. The matters that must be considered and which may be considered on a discretionary basis in balancing the arguments are set out in subsection 6(5) of the Code.

16. Paragraph 6(5)(a) of the Code prescribes a list of matters which must be considered when determining whether or not the project serves the public interest test outlined in subsection 6(4). The matters that must be considered include whether the project promotes better availability of public sector data; any benefits or adverse impact to individuals or groups of people; and any benefits to Australian citizens, permanent residents and other people in Australia. If the data sharing purpose of the project includes informing government policy and programs, it must also be considered how desirable it is for the policy and program to be informed by the result of the project. If the data sharing purpose of the project includes research and development, the potential release of the output must also be considered. This provides a list of criteria that are relatively straightforward to assess, and will be relevant to most projects, so the public interest test in subsection 6(4) of the Code is practical to apply and fit for purpose.

17. Subsection 6(5)(b) of the Code sets out matters the entity may think are relevant when determining whether or not the project serves the public interest. These factors are optional to consider because the information required to fully inform these considerations is not readily available to all data scheme entities and they will only be relevant to certain projects. The matters that may be considered include any issues relevant to Australia's national interests, as set out in policies of the Australian government, and the social, economic, environmental, cultural benefit or costs that can reasonably be expected to result from the project being (or not being) undertaken. This helps ensure the public interest test in subsection 6(4) of the Code is not too burdensome to apply for simple projects, but can address more complex situations where appropriate.

18. Note 1 at the end of subsection 6(5) of the Code clarifies that a project having commercial benefit does not preclude it from being in the public interest, particularly if the research contributes to knowledge or understanding of an issue. Note 2 clarifies that projects that adversely impact people or groups may still be in the public interest so long as the benefit justifies and outweighs the adverse impact.

19. Subsection 6(6) of the Code sets out prescribed matters which do not serve the public interest when considered for a project where the data sharing purpose includes informing government policy and programs, or research and development. These matters include the project exclusively serving the interests of another nation or people of another nation, or exclusively providing a commercial benefit to an entity that is not an Australian entity (as defined in the Act).

Section 7 - Project principle—applicable processes relating to ethics

20. Section 7 of the Code sets out how ethics process interact with the Act, and how data scheme entities satisfy themselves that a project is consistent with the project principle in subsection 16(1)

of the Act, including the element set out in paragraph 16(2)(b) of the Act. Paragraph 16(2)(b) of the Act provides that the project principle includes the element of parties observing processes relating to ethics, as appropriate in the circumstances.

21. Subsection 7(1) of the Code provides that an entity must observe any ethics processes applicable (on the basis of law or policy) to all (or part if only applicable to a part) of the project. This promotes the use of applicable ethics processes and clarifies for Scheme participants how to use ethics processes to meet the project principle under subsection 16(1) of the Act.

22. Note 1 at the end of subsection 7(1) of the Code provides more detail on what is meant by ethics processes and projects where they would or would not apply. Ethics processes are often required through frameworks (legal or policy) and are developed by specialist bodies, such the National Health and Medical Research Council or the Australian Institute of Aboriginal and Torres Strait Islander Studies. Note 2 refers to subsection 19(7) of the Act which requires the data sharing agreement to specify actions the entity will take to observe an ethics process if paragraph 16(2)(b) applies to the project.

23. Subsection 7(2) of the Code provides that the requirement to observe a mandatory process for the purpose of paragraph 7(1)(b) is satisfied if at least one applicable process is observed, and the choice of which process to use is made by the accredited user and the data custodian. The note under subsection 7(2) clarifies that while data scheme entities need not observe more than one applicable ethics process for the purpose of the Act, an entity still has a duty to observe other mandatory ethics processes based on legal and policy frameworks external to the Act.

24. Subsection 7(3) of the Code clarifies that the project principle does not impose additional ethics processes, where no mandatory ethics processes exist. Subsection 7(3) further clarifies that the project principle allows data scheme entities to observe additional ethics processes if they wish to do so. This allows data custodians and accredited users to agree to go beyond the requirements of the Act and observe more than one ethics process if they consider it is appropriate in the circumstances.

People Principle

25. Sections 8-12 of the Code set out how entities can meet the requirements of the people principle in the Act. This principle is that data is only made available to an appropriate person. This is considered at the accredited entity level (that is, for the accredited user and the ADSP, if any) and at the level of designated individuals of the accredited entity or entities. It is also applies to a body corporate who may be contracted with an accredited entity to access data. As the people principle helps establish safeguards, to ensure that data is only accessed by appropriate persons who can be trusted and have the right skills for the project, it is important to clarify for entities how to satisfy this principle.

Section 8 - People principle—existence of conflicts of interest

26. Section 8 of the Code establishes conflicts of interest as a consideration for whether an entity is an 'appropriate person' as part of the people principle set out in subsection 16(3) of the Act.

27. Subsection 8(1) provides that an entity, or any of its data accessors, who have an actual, potential or perceived conflict of interest in relation to collection or use of the data are not appropriate persons to make the data available to unless the conflict is appropriately managed. Subsection 8(2) provides there may also be other circumstances in which a person is not an appropriate person to whom the data is made available.

Section 9 - People principle—projects for the data sharing purpose of delivery of government service

28. Section 9 of the Code discusses assumptions that data scheme entities may make about conflicts of interest and how they may be managed in circumstances where the sole data sharing purpose of the project is the delivery of government services. These assumptions help clarify for data scheme entities how to treat conflicts of interest in an appropriate way where the only purpose of the project is the delivery of government services, noting the context of frameworks and other requirements which apply to such projects.

29. Subsection 9(1) limits the operation of the section to projects where the sole data sharing purpose is the delivery of government services.

30. Section 9 provides that the following assumptions may be made about other data scheme entities when considering a conflict of interest for projects that have the sole data sharing purpose of delivery of government services:
    - Subsection 9(2) provides that a data custodian, or an ADSP, may assume any conflicts of interest are appropriately managed in relation to the collection or use of data by the accredited user or its data accessors.
    - Subsection 9(3) provides that a data custodian, or an accredited user, may assume any conflicts of interest are appropriately managed in relation to the collection or use of data by an ADSP or its data accessors.

31. These assumptions are subject to the accredited user, or ADSP, representing in the data sharing agreement that they have an effective system in place to identify and manage conflicts of interest, and that the system operates effectively. It is preferable to rely on the written representations of the accredited user, or ADSP, as it would be impractical in many cases for a Commonwealth data custodian to assess the operation of the internal conflict of interest processes of another Commonwealth agency or a State or Territory government agency. Subsection 9(4) of the Code provides that an accredited entity, meaning an accredited user or ADSP, is taken to have appropriately managed any conflicts of interest in relation to the collection or use of data by the accredited entity, or its data accessors, if they have an effective system in place to identify and manage such conflicts. The term 'effectively' is intended to have its ordinary dictionary meaning. Section 32 of the Act provides that Scheme entities must not provide information that is false or misleading to another Scheme entity for the purposes of entering into, or giving effect to, a data sharing agreement.

32. In addition, when deciding to accredit an entity under the Scheme, the Commissioner or Minister must consider whether the entity has appropriate data governance and management practices, including arrangements for identifying and managing conflicts of interest in relation to the collection or use of data.

Section 10 - People principle—projects for the data sharing purpose of informing government policy and programs and research and development

33. Section 10 of the Code discusses assumptions that data scheme entities may make about conflicts of interest and how they may be managed in circumstances where the data sharing purpose includes informing government policy or research and development. These assumptions help provide practical guidance and clarify for data scheme entities how to treat conflicts of interest under the data scheme in the context of these types of projects.

34. Subsection 10(1) of the Code limits the operation of the section to projects where the data sharing purpose includes informing government policy or research and development, including if delivery of government services is also a data sharing purpose.

35. Section 10 of the Code provides that the following assumptions may be made about other data scheme entities when considering conflicts of interest for projects where the data sharing purpose includes informing government policy and programs or research and development (including if delivery of government services is also a data sharing purpose):
    - Subsection 10(2) provides that a data custodian, or an ADSP, may assume any conflict of interest is appropriately managed in relation to the collection or use of data by the accredited user or its data accessors.
    - Subsection 10(3) provides that a data custodian, or an accredited user, may assume any conflict of interest is appropriately managed in relation to the collection or use of data by an ADSP or its data accessors.

36. These assumptions are subject to the following:
    - The data custodian, accredited entity, or ADSP, having made reasonable inquiries, must not be aware of any such conflicts that are not appropriately managed; and
    - The accredited entity or ADSP must have identified any such conflicts, and managed them appropriately in a data sharing agreement under the direction of the data custodian.

37. Subsection 10(4) of the Code provides that an accredited entity (meaning an accredited user or ADSP), when satisfying itself that its own data accessors are appropriate persons to collect and use data, must do the following:
    - Identify any actual, potential or perceived conflicts of interest that any of its data accessors, who are permitted to collect or use output or ADSP enhanced data for a project, have in relation to the collection or use; and
    - If any such conflicts are identified, they must manage the conflicts appropriately, notify any other parties to the data sharing agreement of the conflict, and how the conflict is being managed.

38. The note under subsection 10(4) provides that an accredited entity, meaning an accredited user or ADSP, may manage a data accessor's conflict of interest by ensuring the designated individual manages that conflict of interest.

39. The example under subsection 10(4) sets out how a conflict of interest could be resolved using the example of a researcher conducting environmental research at an Australian university, and using shared data. If the researcher is also a member of an environmental group that interacts with the sharer, this would be a relevant conflict for the university. If the university identifies a conflict, the researcher is still able to conduct the research using the shared data provided that the university notifies the sharer of the conflict and the measures it intends to implement to manage the conflict. This can resolve the conflict, if the sharer is comfortable with the proposed measures, which are managed in accordance with the data sharing agreement.

Section 11 - People principle—attributes, qualifications, affiliations, expertise

40. Section 11 of the Code discusses attributes, qualifications, affiliations and expertise of an 'appropriate person' as part of the people principle in projects. The section helps ensure that data is handled by persons with the appropriate attributes, qualifications, affiliations and expertise by setting out the matters that should be considered by entities when applying the people principle, and how to assess them. This promotes safeguards around who data is shared with under the data scheme.

41. Subsection 11(1) of the Code limits the operation of the section to projects where the data sharing purpose includes informing government policy or research and development, including if delivery of government services is also a data sharing purpose.

42. Subsection 11(2) of the Code provides that a data scheme entity must take into account certain matters in relation to any individuals who are designated individuals for an accredited entity that is a party to the data sharing agreement and who can access data under a data sharing agreement, when considering whether they are appropriate people to handle data under subsections 16(3) and (4) of the Act.

43. Subsection 11(3) of the Code provides that entities may take the matters referred to into account in relation to a class or classes of data accessors, rather than in relation to each individual data accessor. This clarifies to scheme entities that they are not required to check every person who will access the data on an individual basis. It may be sufficient to ensure the class of people accessing the data all have appropriate security clearances in place for instance. The example under subsection 11(3) sets out an entity considering a class of data accessors by reference to the level of training they have undergone to handle sensitive data.

44. Subsections 11(4), (5) and (6) of the Code provide that the matters that must be taken into account include the following:
    - The attributes of the individuals, including whether they have security or other clearances the data custodian considers necessary
    - The qualifications of the individuals, including tertiary or formal qualifications.
    - The affiliations of the individuals, including employment, contractual obligations, sponsorships or scholarships and membership of associations.

45. Subsection 11(7) of the Code provides that an individual's affiliations may enhance or detract from their appropriateness to access data. Subsection 11(8) sets out the sorts of affiliations that will detract or enhance a data accessor's appropriateness to access data, and includes an example of this to provide clarity.

46. Subsection 11(9) of the Code sets out the sorts of expertise that would be relevant when considering the appropriateness of an individual to access data under subsections 16(3) and (4) of the Act. This includes formal and informal education and training, as well as expertise derived from practical or on-the-job training.

Section 12 - People principle—experience

47. Section 12 of the Code establishes experience as a criterion when considering an 'appropriate person' as part of the people principle in data sharing projects. This is to recognise the importance of an individual's past history in handling data when determining if they are an appropriate person under the people principle.

48. Subsection 12(1) of the Code limits the operation of the section to projects where the data sharing purpose includes informing government policy or research and development, including if delivery of government services is also a data sharing purpose.

49. Subsection 12(2) of the Code sets out that an individual's experience handling data is relevant to whether they are an appropriate person to access data under subsection 16(3) of the Act, and subsection 12(4) provides that an data accessor's experience in handling data may enhance or detract from their appropriateness to access data. Subsection 12(3) provides that an entity may consider experience in relation to a class of individuals, rather than each individual. This clarifies to scheme entities that they are not required to check every person who will access the data on an individual basis. It may be sufficient to ensure the class of people accessing the data all have appropriate security clearances in place for instance. The example under subsection 12(3) provides for an entity considering a class of individuals by reference to the appropriate experience they have in handling sensitive data.

50. The note under subsection 12(4) of the Code gives an example of how an individual's previous experience handling data could enhance or detract from their appropriateness to access data to provide clarity to the reader.

Setting principle

51. Section 13 of the Code provides guidance about the setting principle. This principle is that data is only shared, collected and used in an appropriately controlled environment (see subsection 16(5) of the Act). This principle considers the means by which data is to be shared and the security standards to apply for the collection and use of data. As the setting principle helps ensure safeguards so that data is accessed, stored, transmitted through, used or released in an environment that provides sufficient protections for data sharing, it is important to clarify to entities how to satisfy this principle.

Section 13 - Setting principle—reasonable security standards

52. Section 13 of the Code sets out matters that must be considered when an entity satisfies itself that the project is consistent with the setting principle, particularly in relation to the existence of reasonable security standards.

53. Subsection 13(1) provides that an entity must take into account the matters set out in this section when satisfying itself that a project is consistent with the setting principle set out in subsection 16(5) of the Act, including the element set out in paragraph 16(6)(b) of the Act.

54. Paragraph 16(6)(b) of the Act provides that a reasonable security standard will be proportionate to the sensitivity of the data and the risks posed by sharing, collecting or using the data. This means the application of reasonable security standards may, in some cases, mean that accredited entities that are not Commonwealth bodies must comply with Commonwealth security standards, or parts of them.

Data Principle

55. Section 14 of the Code provides guidance about the data principle. This principle is that appropriate protections are applied to shared data. The principle includes a requirement that only data reasonably necessary to achieve the data sharing purpose or purposes is shared. As the data principle helps the entities consider the nature of the data, and whether any technical or statistical treatments are necessary to control the risks of sharing it for a project, it is important to clarify how to satisfy this principle.

Section 14 - Data principle—appropriate protection

56. Section 14 of the Code prescribes matters that must be taken into account when considering whether appropriate protections are applied to the data under the data principle set out in subsections 16(7) and 16(8) of the Act. This section identifies 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.

57. Subsection 14(1) of the Code provides that an entity must comply with this section as part of satisfying itself that a project is consistent with the data principle set out in subsections 16(7) and 16(8) of the Act. Subsection 16(8) of the Act provides that the data principle includes (but is not limited to) only the data reasonably necessary to achieve the applicable data sharing purpose or purposes is shared, collected and used. This ensures no more data is shared than necessary, and

safeguards against the sharing of data that is extraneous or unrelated to a project, even if this requires additional treatment of the data to remove unnecessary elements.

58. Subsection 14(2) of the Code provides the entity must consider whether the data, before it is shared, should be treated in a way that contributes to the proportionate management of the risks of sharing, collecting and using the data.

59. The first note under subsection 14(2) of the Code provides that treatment might include processes that effectively reduce the detail of the data through deletion, modification or a combination of variables, categories or unit records to illustrate the practical application of the principle. The second note refers to the privacy protections under sections 16A and 16B of the Act and the requirements relating to de-identification or secure access data services in section 16C of the Act.

60. Subsection 14(3) of the Code provides that if the data is to be shared through an ADSP, the data custodian must consider the appropriateness of treating the data before sharing with the ADSP as an additional safeguard for data sharing.

61. Subsection 14(4) of the Code requires the entity to consider whether a reasonable person, who is properly informed, would agree that the data to be shared, collected or used is reasonably necessary to achieve the data sharing purpose or purposes of the project. It is intended that a reasonable person who is properly informed would, for the purposes of this section, be expected to have thorough and extensive knowledge of the project topic(s), such that they are capable of identifying the data necessary to achieve the project outcomes. This provision draws on the common law standard of a 'reasonable person' to help clarify the interpretation of the data principle for the reader.

62. The note below subsection 14(4) of the Code draws attention to other relevant provisions, including paragraph 13(2)(e) of the Act, which provides that data scheme entities should only share the minimum amount of personal information necessary to give effect to the project, The note also refers to the privacy protections in sections 16A and 16B of the Act.

Output Principle

63. Section 15 of the Code provides guiding information about the output principle, which is the principle that the only output of a project is the final output (as agreed by the parties involved in the project) and output reasonably necessary or incidental to the creation of this output (see subsection 16(9) of the Act). The final output must only contain the data reasonably necessary to achieve the applicable data sharing purpose(s). The output principle brings to the fore the need for data scheme entities to negotiate how the shared data will be used. As the output principle provides limitations on the release of unrelated data as output, it is important to clarify to entities how to satisfy this principle.

Section 15 - Output principle

64. Section 15 of the Code prescribes matters an entity must have regard to when considering whether a project is consistent with the output principle set out in subsection 16(9) of the Act, including the elements set out in subsection 16(10) of the Act. Subsection 16(10) of the Act provides that the output principle includes (but is not limited to) the data custodian of the data and the accredited user considering the nature and intended use of the output of the project, and requirements and procedures for the use of the output of the project. The final output should contain only the data reasonably necessary to achieve the applicable data sharing purpose(s).

65. Subsection 15(1) of the Code sets out that an entity must consider the matters set out in the section when considering if a project is consistent with the output principle.

66. Subsection 15(2) of the Code provides the entity must consider the nature and intended use of the output. These may include (but are not limited to) pre-filled forms, aggregated data sets (tables or unit records) for further analysis, mathematical models for monitoring government programs, and publications such as academic journals or government reports. The intention of this section is to prompt data scheme entities to consider the desired outcomes of the project early, so they are clearly defined and to enable inclusion of a mechanism in the data sharing agreement for the data to be accessed or released if necessary (see sections 20A-20F of the Act). This will ensure the ultimate intended use of the output is possible and permitted.

67. Subsection 15(3) of the Code prescribes that if a data sharing agreement permits data to be accessed or released, the data scheme entities must consider the appropriateness of this permission and whether procedures and processes should be included in the data sharing agreement to manage this. The intention of this provision is that the data custodian will need to consider this before sharing and the accredited user and ADSP will need to consider this before collection and use.

Part 3—Dealings with Personal Information

Section 16 - Purpose of Part

68. Section 16 sets out the purpose of Part 3 of the Code: setting out requirements for obtaining the consent of an individual for the sharing of personal information about the individual, for the purposes of sections 16A and 16B of the Act, which deal with general and purpose specific privacy protections respectively. Part 3 also sets out the principles to be applied when determining whether it is necessary to share personal information to properly deliver a government service, and whether the public interest to be served by a project justifies the sharing of personal information without consent. It also sets out requirements relating to consent under sections 20C, 20E and 20F of the Act.

Section 17 - Consent to sharing personal information—sections 16A and 16B of the Act

69. Section 17 of the Code relates to obtaining consent to share personal information under sections 16A and 16B of the Act. This section builds on the foundation provided by the Office of the Australian Information Commissioner and current privacy law guidelines on what constitutes consent.

70. Subsection 17(1) of the Code provides that section 17 is about an individual's consent to share personal information about the individual for the purposes of subsection 16A(1) and subparagraphs 16B(1)(a)(ii) and (3)(a)(i) of the Act. Subsection 16A(1) prohibits the sharing of biometric data under the scheme unless the individual to whom the biometric data relates expressly consents to the sharing. Subparagraph 16B(1)(a)(ii) requires that if the data sharing purpose of the project is the delivery of government services, personal information may only be shared with the consent of the individual to whom the personal information relates. Under subparagraph 16B(3)(a)(i), if the data sharing purpose of a project is informing government policy and programs, or research and development, generally the shared data cannot include an individual's personal information unless the individual consents to the sharing and only the minimum amount of personal information necessary for the project to proceed is shared. (Notably, subparagraph 16B(3)(b) provides very limited circumstances in which personal information can be shared without the individual's consent for the purposes of such projects.)

71. Subsections 17(2) to (7) of the Code provide that before consent is given, the individual must be adequately informed about the nature of the personal information to be shared, whether the information is to be shared more than once, and the accredited entity or entities with whom the information will be shared. The consent must relate specifically, and is limited, to the project for which the personal information is being used. The consent must be voluntary and withdrawal of consent must be express (whether orally or in writing). Consent is not current if the consent was withdrawn before the sharing occurred. The reference to consent needing to be 'current' is intended to align with the Australian Information Commissioner's guidance on how the concept of consent should be applied for the purposes of the Privacy Act. Subsection 17(5) provides that consent must be in effect at the time of sharing. Consent cannot be current if it has been withdrawn prior to that time, and reflects the position that consent, once given, does not remain in effect indefinitely. These provisions clarify the operation of consent, and provide safeguards that help ensure personal information is only shared when there is genuine consent from the individual to whom the personal information relates, to the extent that they consent to their personal information being shared.

72. Subsection 17(8) of the Code provides the consent must be given by the individual if the individual has the capacity to consent, or by a responsible person for the individual (within the meaning of the Privacy Act). This provides guidance on who must give consent, including in cases where an individual lacks the capacity to consent.

73. Subsection 17(9) of the Code provides that consent for the purposes of subparagraph 16B(1)(a)(ii) or (3)(a)(i) of the Act (discussed above) may be express (either oral or in writing) or implied (in circumstances where it may be reasonably inferred from conduct).

74. The note below subsection 17(9) clarifies that consent for biometric data is required to be express under subsection 16A(1) of the Act.

Section 18 - Consent to provision of access to or release of personal information—paragraph 20C(1)(b) of the Act

75. Section 20C of the Act permits a data sharing agreement to include a provision to allow an accredited user to provide access to specified output to another entity, or to release specified output, if three conditions set out in subsection 20C(1) of the Act are satisfied (these are discussed in more detail below).

76. Section 18 of the Code deals with an individual providing consent to the accredited user to provide access to, or release of, personal information for the purpose of paragraph 20C(1)(b) of the Act, which provides that if the output of a project includes personal information about an individual, it prohibits provision of access or release unless the individual consents. This section helps ensure a consistent approach to consent throughout the Code, particularly in relation to the approach taken in sections 19 and 20 of the Code.

77. Subsection 18(1) of the Code provides that a data sharing agreement may allow the accredited user to provide another entity with access to output of a project, or to release it, if the agreement meets all of the conditions specified in subsection 20C(1) of the Act, which include the following:

- Paragraph 20C(1)(a) of the Act which only allows a data sharing agreement to permit the provision of access, or release, or specified output, in particular circumstances if the provision of the access, or the release, would not contravene any other law of the Commonwealth or a law of a State or Territory (disregarding the operation of section 23 of the Act which is the override provision). For example, if secrecy provisions in another Commonwealth law would prevent output being released (disregarding the operation of

section 23 of the Act), subsection 20C(1) of the Act would not permit a data sharing agreement to provide for release of the output.

- Paragraph 20C(1)(b) of the Act which only allows a data sharing agreement to permit the provision of access, or release, or specified output if the agreement prohibits the provision of access or release of output that contains the personal information of an individual without the individual's consent. For example, a data sharing agreement may permit the release of a research report, but if the research report includes any personal information of individuals, the agreement must prohibit the release of the research report unless all of those individuals consent.
- Paragraph 20C(1)(c) of the Act which provides that, where a data sharing agreement allows for an accredited user to provide access to output to another entity, or to release output, it must also require the data custodian to be satisfied, before the provision of access or the release, that the access or release will be an authorised use of the output under section 13A of the Act. This is an important control to ensure that an accredited user does not provide access to, or release, output inappropriately.

78. Subsections 18(2) to (7) of the Code provide that before consent is given, the individual must be adequately informed about the nature of the personal information to be shared, and the accredited entity or entities with whom the access to the information will be provided. The consent must relate specifically, and is limited, to the provision of access or release. The consent must be voluntary and withdrawal of consent must be express (whether orally or in writing). Consent is not current if the consent was withdrawn before the access or release occurred. The reference to consent needing to be 'current' is intended to align with the Australian Information Commissioner's guidance on how the concept of consent should be applied for the purposes of the Privacy Act. Subsection 17(5) provides that consent must be in effect at the time of sharing. Consent cannot be current if it has been withdrawn prior to that time, and reflects the position that consent, once given, does not remain in effect indefinitely. Subsections 18(2) to (7) of the Code clarify the operation of consent, and provide safeguards that help ensure access or release of personal information occurs only when there is genuine consent from the individual whom the information is about, to the extent they consent to the access or release.

79. Subsection 18(8) of the Code provides the consent must be given by the individual if the individual has the capacity to consent, or by a responsible person for the individual (within the meaning of the Privacy Act). This provides guidance on who must give consent, including in cases where an individual lacks the capacity to consent.

80. Subsection 18(9) of the Code provides that consent for the purposes of a provision of a data sharing agreement included for the purposes of paragraph 20C(1)(b) of the Act (prohibiting access to personal information included in the output unless the individual consents) may be express (either oral or in writing) or implied (in circumstances where it may be reasonably inferred from conduct). This provides clarity to the reader about the operation of consent for the purposes of paragraph 20C(1)(b) of the Act.

Section 19 - Consent to exit of personal information—paragraph 20E(4)(c) of the Act

81. Section 20E of the Act provides for the exit of a copy of personal information from the scheme in projects with the data sharing purpose of the delivery of government services, by permitting an individual to expressly consent to both the sharing of their personal information with an accredited user, and the accredited user's use of that personal information without the use constraints imposed by the scheme. Where a project with the data sharing purpose of the delivery of government services permits a copy of personal information to exit the scheme under subsection 20E(4) of the Act, subsection 16B(2) of the Act requires that the data sharing agreement for the project specify this.

82. Section 19 of the Code deals with consent given by an individual for the purposes of paragraph 20E(4)(c) of the Act. This section helps ensure a consistent approach is taken to how consent requirements are applied in the scheme. Paragraph 20E(4)(c) of the Act provides that a copy of output of the project held by the accredited user exits the scheme at the time applicable under subsection 20E(5) of the Act. The applicable time will be at the time the accredited user collects the shared data, or if the individual's consent specifies a later time, that later time.

83. Subsection 19(1) of the Code explains that a copy of output of a project may exit the scheme in some circumstances under subsection 20E(4) of the Act with an individual's consent, and that section 19 sets out how the requirement in the Act for consent is to be applied. When a copy of output 'exits' the scheme it means the requirements of the Act no longer apply to the use of that copy.

84. Subsections 19(2) to (3) of the Code provide that, before the consent is given, the individual must be adequately informed about the sharing, including the nature of the personal information to be shared, whether the personal information is to be shared more than once, and the accredited entity or entities with whom the information will be shared. The individual must be adequately informed that the personal information will be shared under the Act. The individual must also be adequately informed that, generally, the use of personal information and other data shared under the Act is limited by the Act, and if the individual gives the consent sought, the Act will not limit use of the personal information by the accredited user. This helps ensure the full and informed consent of the individual to the sharing and use of their data in this way.

85. Subsection 19(4) of the Code provides that the individual may be informed about other laws that will limit the use and disclosure of the personal information by the accredited user, if the individual gives the consent sought. While this information may be helpful to the individual in some circumstances, the Code does not require this information to be provided to the individual.

86. Subsection 19(5) of the Code provides that the consent may be sought by the data custodian or by the accredited user.

87. Subsections 19(6) to (9) of the Code provide that the consent must be voluntary and must relate specifically to the sharing of the personal information with the accredited user and the accredited user's use of the personal information. Consent must also be current at the time of the sharing, and is not current if the consent was withdrawn before that time. The reference to consent needing to be 'current' is intended to align with the Australian Information Commissioner's guidance on how the concept of consent should be applied for the purposes of the Privacy Act. Subsection 17(5) provides that consent must be in effect at the time of sharing. Consent cannot be current if it has been withdrawn prior to that time, and reflects the position that consent, once given, does not remain in effect indefinitely. These provisions clarify the operation of consent in the Scheme, and provide safeguards that help ensure sharing of personal information is only done when there is genuine consent from the individual to whom it is about, to the extent they consent to the sharing.

88. Subsections 19(10) and (11) of the Code provide that withdrawal of consent has effect only if done expressly (orally or in writing) and before the time of the sharing. Consent must also be given by the individual if they have capacity to consent, or by a responsible person for the individual (within the meaning of the Privacy Act). This provides guidance on who must give consent, and when, including in cases where an individual lacks the capacity to consent.

Section 20 - Consent to use of personal information by new data custodian—paragraph 20F(3)(b) of the Act

89. A data sharing agreement for a project may appoint the accredited user in the project as the data custodian of specific output of the project in the circumstances set out in subsection 20F(2) of the

Act. These include that either the agreement allows the user to provide access to the specific output in circumstances allowed by section 20C or 20D, or (if the agreement does not make such provision) the conditions for exit in subsection 20F(3) of the Act are met in relation to the specific output. Paragraph 20F(3)(b) of the Act applies if the specified output includes personal information about an individual. In this case, the condition is only satisfied if the individual has expressly consented to their personal information being used by the accredited user without the requirements of the Act applying to that use.

90. Section 20 of the Code deals with individuals providing consent for the use of their personal information for the purposes of paragraph 20F(3)(b) of the Act. This section helps ensure a consistent approach is taken to how consent requirements are applied in the scheme.

91. Subsection 20(1) of the Code explains that the accredited user under a data sharing agreement for a project may be appointed as the data custodian of specified output if certain conditions are met as set out in subsection 20F(2) of the Act (discussed above). If the specified output includes personal information, these conditions include that a person whose personal information forms part of the specified output must have expressly consented to that information being used by the accredited user without the requirements of the Act applying (paragraph 20F(3)(b) of the Act.)

92. Subsections 20(2) and (3) of the Code provide that before consent is given, the individual must be adequately informed about the nature of the personal information and the identity of the accredited user. The individual must also be adequately informed that, generally, the use of personal information and other data shared under the Act is limited by the Act, and if the individual gives the consent sought, the Act will not limit use of the personal information by the accredited user. This helps ensure the full and informed consent of the individual to the use of their data in this way.

93. Subsection 20(4) of the Code provides that the individual may be informed about other laws that will limit the use and disclosure of the personal information by the accredited user, if the individual gives the consent sought.

94. Subsections 20(5) to (6) of the Code provide that the consent may be sought by either the data custodian or the accredited user, and must be voluntary. This clarifies to the entities who has responsibility for obtaining consent, and that the consent must be freely given.

95. Subsections 20(7) to 20(9) of the Code require that consent relate specifically to the accredited user being able to use personal information without the requirements of the Act applying to use and that it is current at the time the personal information exits the scheme. Without limiting subsection 20(8), consent is not current at the time of the sharing if the consent was withdrawn before that time. The reference to consent needing to be 'current' is intended to align with the Australian Information Commissioner's guidance on the operation of consent in the Privacy Act, and means that consent must be in effect at the time of sharing. Consent cannot be current if it has been withdrawn prior to that time, and reflects the position that consent, once given, does not remain in effect indefinitely. These provisions clarify the operation of consent, and provide safeguards that help ensure sharing of personal information is only given when there is genuine consent from the individual to whom it relates, to the extent that they consent to the sharing.

96. Subsections 20(10) and (11) provide that withdrawal of consent has effect only if done expressly (orally or in writing) and before the time of exit. Withdrawal of consent has no effect if the data has already exited the scheme. Consent must also be given by the individual if they have capacity to consent, or by a responsible person for the individual (within the meaning of the Privacy Act). This provides guidance on who must give consent, and when, including in cases where an individual lacks the capacity to consent.

Section 21 - Unreasonable or impracticable to seek consent

97. Section 21 of the Code provides that for the purposes of paragraph 16B(4)(a) of the Act, the data custodian's conclusion that it is unreasonable or impracticable to seek an individual's consent to the sharing of data that includes personal information about the individual must be based on the following considerations:
    - whether the data custodian is able to contact the individual to seek consent, including whether the data custodian has resources, systems and practices to do so;
    - whether the proposed sharing is authorised by any other law (for example, under the Privacy Act or the law which originally authorised the collection of the individual's personal information);
    - the likely impact (whether positive or negative, or direct or indirect) of the project of which the sharing is a part on the individual about whom personal information will be shared, or a group of people that includes the individual;
    - the likely impact on the individual of seeking, or not seeking, the individual's consent;
    - whether the sharing relates to a serious threat to, or urgent situation involving, the individual about whom personal information will be shared, or a group of people that includes the individual.

98. These criteria are designed to provide clarity and guidance to the data custodian when reaching the conclusion that consent is unreasonable or impracticable to obtain, which helps ensure data sharing without consent will only be undertaken when this high threshold is met, and require a consideration of a range of factors, including the direct or indirect impact on individuals and groups of individuals to whom the data relates.

99. Subsection 21(2) of the Code provides that it may be unreasonable or impracticable to seek consent if seeking consent would be excessively burdensome in all the circumstances. However, subsections 21(3) and 21(4) of the Code provide that it is not unreasonable or impracticable to seek consent merely because it would be inconvenient, time-consuming or incur costs or because the consent of a very large number of individuals needs to be sought. The test that seeking consent must be 'unreasonable or impractical' and 'excessively burdensome' is intended to align with the test of 'unreasonable or impractical to obtain the individual's consent' in section 16A of the Privacy Act. The Code broadly aligns with the guidance published by the Australian Information Commissioner on the operation of section 16A of the Privacy Act. The expressions 'unreasonable or impractical' and 'excessively burdensome' would be assessed objectively by a court from the standpoint of a hypothetical reasonable person, which would require consideration of all the relevant facts in their context. It is not sufficient for a data sharing entity under the scheme to merely hold a subjective view that seeking consent would be excessively burdensome.

Section 22 - Personal information—determining necessity of sharing and minimum amount necessary

100. Section 22 of the Code sets out considerations for determining the necessity of sharing and the minimum amount of personal information necessary to adequately inform the project. It provides the principles to be applied by data custodians when determining whether it is necessary to share personal information to properly deliver the government service. This provides clarity to data custodians, to ensure no more data is shared than is necessary for the project to deliver the government services.

101. Subsection 22(1) of the Code notes that section 22 sets out the principles to be applied by data custodians in relation to projects that have the data sharing purpose of delivery of government services, when determining whether it is necessary to share personal information to deliver the service properly. The term 'delivery of government services' is defined in subsection 15(1A) of

the Act to mean the provision of the following services by the Australian Government, or by a government of a State or a Territory:

- the provision of information;
- the provision of a service that is not a service relating to a payment, entitlement or benefit;
- determining eligibility for a payment, entitlement or benefit; and
- paying a payment, entitlement or benefit.

102. Subsection 22(2) of the Code sets out the general principle that it is not necessary to share personal information to properly deliver a government service, except as provided by this section. This helps ensure sharing of personal information to deliver government services is limited to specific situations allowed under this section of the Code.

103. Subsection 22(3) of the Code provides that to properly deliver a government service mentioned in paragraph 15(1A)(a) of the Act, it is necessary to share personal information that is contact information for the individual to whom the service is being delivered; or any information relevant to the timing of the provision of the information, or to the content of the information. This clarifies the limitations on sharing of personal information for delivering government services in relation to paragraph 15(1A)(a) of the Act.

104. Subsection 22(4) of the Code provides that it is necessary to share the following personal information to properly deliver a government service mentioned in paragraph 15(1A)(b) of the Act: contact information for the individual to whom the service is being delivered, and any information relevant to the timing of the provision of the service, or to the scope or content of the service. This clarifies the limitations on sharing of personal information for delivering government services in relation to paragraph 15(1A)(b) of the Act.

105. Subsection 22(5) of the Code provides that it is necessary to share the following personal information to properly deliver a government service under legislation for the delivery of the government services under paragraph 15(1A)(c) or (d) of the Act: contact information for the individual to whom the service is being delivered, and any information about the individual that, under the legislation, may be considered and is expected to be considered when delivering the service. This clarifies the limitations on sharing of personal information for delivering government services done under legislation in relation to paragraphs 15(1A) (c) or (d) of the Act.

106. Subsection 22(6) of the Code provides that if the delivery of a government service is being done other than under legislation then, to properly deliver the service, it is necessary to share the following personal information if the delivery of a government service is being done other than under legislation under paragraph 15(1A)(c) or (d) of the Act: contact information for the individual to whom the service is being delivered, and information about the individual that may be considered in accordance with any written policies, procedures, processes or guidance applicable to delivery of the service, and other information about the individual that may lawfully be considered in relation to delivery of the service and is expected to be considered when delivering the service. This clarifies the limitations on sharing of personal information for delivering government services being done other than under legislation in relation to paragraphs 15(1A)(c) or (d) of the Act.

Section 23 - Whether public interest justifies sharing personal information without consent

107. Section 23 of the Code sets out when the public interest justifies sharing personal information without consent. When making this assessment, the decision-maker should have regard to all the relevant factors listed in this section. This provides clarity that helps ensure personal information is only shared without consent in very restricted circumstances.

108. Subsection 23(1) of the Code sets out the principles to be applied by data custodians when determining circumstances, or categories of circumstances, where the public interest to be served by a project justifies the sharing of personal information without consent for the purposes of subparagraph 126(2C)(b)(ii) of the Act.

109. Subsection 23(2) of the Code provides that any adverse impacts on individuals that are likely to be caused by the sharing of the personal information are to be identified. The public interest to be served by the project only justifies the sharing if the ways in which the public interest is served by the project outweigh all of the likely adverse impacts. This ensures there is a proper process and calculation of the risks and impacts of sharing, and an assessment that is formulated after weighing up the likely impacts.

110. Subsection 23(3) of the Code prescribes considerations a data custodian must take into account when determining whether the public interest is served by a project that shares data containing personal information without consent. Those considerations include:
- whether the project relates to preventing, or responding to, a serious threat to life, or to the health, safety or welfare of the public;
- whether the project includes any safeguards to minimise any impact on an individual, such as security measures specified in the data sharing agreement;
- whether personal information is to be shared with the accredited user, or whether it is only to be shared with an ADSP that will either de-identify the information, or provide the accredited user with ADSP-controlled access;
- the benefits to individuals or groups of people, and the likelihood of the project achieving those benefits;
- the adverse impacts to individuals or groups of people that can reasonably be expected as a result of sharing the data.

111. These criteria are designed to provide clarity and guidance to the data custodian when reaching the conclusion that the public interest is met by sharing data personal information without consent, and that it will only be undertaken when a careful evaluation of a range of factors is made.

112. Subsection 23(4) of the Code gives the data custodian discretion to take into account any other considerations it considers relevant to whether the public interest justifies sharing personal information without consent. Relevant matters may include:
- any issues relevant to Australia's national interests, as set out in policies of the Australian government;
- the social, economic, environmental, cultural and other benefits that can reasonably be expected to result from the project; or
- the social, economic, environmental, cultural and other costs that can reasonably be expected to result from the project, or to result from the project not being undertaken.

Part 4—Miscellaneous

Section 24 - Information and documents required at time of giving documents under subsection 33(1) of the Act

113. Section 24 of the Code relates to giving information and documents under subsection 33(1) of the Act, which requires a data custodian to provide the Commissioner with an electronic copy of any data sharing agreement (including varied agreements) it enters into. The copy must be provided in a form approved by the Commissioner (if any) within 30 days of making the agreement or variation. This clarifies the obligations of entities to provide the Commissioner with specific documents under section 33(1) of the Act, and the content of those documents.

114. The Commissioner is required to maintain a public register of data sharing agreements, which will support the Commissioner in administering and reporting on the scheme, and provide transparency about data sharing activities for data scheme entities and the public more broadly. This requirement provides the Commissioner with oversight of sharing activities necessary for its regulatory function and also promotes compliance.

115. Subsection 24(1) of the Code prescribes the information required for the purposes of satisfying subsection 33(2) of the Act, that being the information set out in subsection (2) of this section, in an approved form (if any). If the data sharing agreement, or variation, has an attachment, the attachment must be provided, and any other information or documents the entity considers relevant in relation to registration of the data sharing agreement or variation.

116. Subsection 24(2) of the Code prescribes the information required under subsection 33(2) of the Act, that being any other information or document required by a data code. This must be given to the Commissioner at the same time as the document mentioned in subsection 33(1) of the Act.

Section 25 - Applicable period for notifying Commissioner of certain information

117. Section 25 of the Code relates to applicable period for notifying the Commissioner of certain information for the purposes of paragraph 34(4)(a) of the Act. Section 34 of the Act requires data scheme entities to support the Commissioner to prepare an annual report on the operation of the Scheme. These provisions promote the enhanced integrity and transparency of sharing public sector data and support transparency under the scheme.

118. Section 34 of the Act outlines the specific information that a data custodian must notify the Commissioner in relation to for the financial year. This includes the number of data sharing requests from accredited users and the reasons for agreement or refusal to share, the number of complaints received (if any), and the number of data sharing agreements it entered into. The data custodian and an accredited entity must give the Commissioner any other information and provide reasonable assistance in relation to the preparation of the annual report.

119. Section 25 of the Code provides that the period for notifying the Commissioner of this information is the period ending on 31 July.

Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

Data Availability and Transparency Act 2022
Data Availability and Transparency Code 2022

This instrument is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*

Overview of the legislative instrument

The *Data Availability and Transparency Code 2022* (the **Code**) provides guidance for scheme participants on best practice data sharing that covers matters including:

- The data sharing principles scheme participants must apply when entering into a data sharing agreement. These principles go to ensuring appropriate controls on the project, people, setting, data and output.
- Privacy protections, including how individual consent is to be collected and the circumstances where it is permissible not to collect consent.

The Code sets out how definitions in the Act are to be applied and imposes additional requirements on data scheme participants that are not contrary to, or inconsistent with, the Act. Section 26 of the Act provides that a data scheme entity must comply with the Code.

It remains at the discretion of the data custodian to decide whether it is appropriate to share data in circumstances not excluded by the Code, or other legislation under the data scheme, as the Act creates no duty to share (noting reasonable requests must be considered, and reasons for refusal must be provided).

The Code does not expand the types of data that may be shared under the Scheme.

Human rights implications

The Code engages the following rights:

- the right to protection from arbitrary or unlawful interference with privacy; and
- freedom of expression, including to seek, receive and impart information.

Right to protection from unlawful or arbitrary interference with privacy

The purpose of the Code is to provide a best practice code in relation to certain parts of the Act. All data sharing under the Act must be consistent with the Privacy Act because sharing that is inconsistent with the Privacy Act is barred by subsection 17(5) of the Act.

The right to protection from arbitrary or unlawful interference with privacy is recognised in Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR). This right encompasses respect for informational privacy, including the right to respect the storing, use and sharing of private and confidential information.

In order to be permissible, an interference with the right to privacy must be reasonable in the circumstances and authorised by a law consistent with the ICCPR. The United Nations Human Rights Committee (UNHRC) has interpreted 'reasonable' to mean 'any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case.'[1]

The right to privacy is also recognised in Article 16 of the *Convention on the Rights of the Child* which states that no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation. The Code upholds and enhances the right to privacy by strengthening the safeguards under the Act. By setting out in detail the circumstances in which sharing of data can happen under the Act, the Code preserves and enhances the existing laws that protect, and regulate the use of, government data, and this helps ensure channels for data access within those dedicated frameworks are not affected.

Further privacy enhancing measures in the Code include:

- Strengthening the data sharing principles, which are a key safeguard of the scheme by explaining how they operate and introducing new requirements to satisfy the principles. These include the introduction of steps to resolve conflicts of interest and to take an individual's experience handling data into account when considering the people principle.
- Setting specific requirements around getting consent to share data, including data which contains personal information, wherever consent is needed under the Act (see sections 16A, 16B, 20C, 20E and 20F of the Act).
- Limiting the amount of personal information that is shared to the minimum amount necessary to achieve the purpose of the project.
- Requiring the data scheme entities to consider the appropriateness of access or release and any procedures or processes to manage access to or release of the data at the beginning of the project and again prior to actioning.

Parts of the Code proportionately and necessarily interfere with the right to protection from arbitrary or unlawful interference with privacy in the following ways:

Information provided by data scheme entities to satisfy the people principle

Data scheme entities, data accessors and designated individuals are required by sections 10-12 of the Code to provide details of conflicts of interest, attributes, qualifications, affiliations, expertise and experience which will necessarily include disclosure of personal information and possibly sensitive personal information.

However, this is proportionate and necessary for data custodians to be satisfied that the individuals who will be using and collecting government data, which could include personal information or other sensitive information, are appropriate people to use and collect data. Data custodians, as Australian

[1] Office of the United Nations High Commissioner for Human Rights, *Toonen v Australia*, Communication No. 488/1992, UN Doc CCPR/C/50/D/488/1992 (10 April 1992, adopted 31 March 1994)
[8.3]: https://juris.ohchr.org/Search/Details/702.

government agencies, are required to comply with the Privacy Act in respect of their collection, use and storage of that personal information.

Unreasonable or impracticable to seek consent

The Act provides for sharing of data without consent where it is unreasonable or impracticable to seek consent. The Code supports this, but only in very specific circumstances, which are more limited than *Australian Privacy Principles Guidelines* provided by the Australian Information Commissioner under section 28(1)(a) of the Privacy Act. In addition to the limitations in that guidance, the Code also states that it is not unreasonable or impracticable to seek consent merely because a very large number of individuals would need to be contacted. This interference with privacy is necessary for the functioning of the Act and is a proportionate and just limitation on human rights and carefully controlled.

Right to freedom of expression, including to seek, receive and impart information

Article 19 of the ICCPR establishes the right to freedom of expression, including the freedom to seek, receive and impart information and ideas. The exercise of this right may be subject to restrictions only if provided by law and where it is necessary for the protection of national security, or to respect the rights of others. Facilitating access to data is consistent with the freedom to seek and impart information.[2]

The Code clarifies the operation of some legitimate, necessary and proportionate limitations on the right to seek, receive, and impart information to protect national security interests and to respect others' rights, which are embedded in the Act. While it clarifies the operation of these limitations, which are set out in the Act, it does not further limit this right. Consistent with the Act, the Code preserves existing rights and privileges over public sector data by precluding any sharing that would contravene such interests.

The Code, in alignment with the Act, represents a proportionate means of restricting access to data under the scheme through exclusions from data access that have been designed through extensive consultation with relevant agencies and stakeholders, and only granted from the scheme where strictly necessary to achieve the goals of protecting public sector data.

For the reasons outlined above, the Code and its operation alongside the scheme constitutes a permissible limitation to the Right to freedom of expression, including to seek, receive and impart information.

Conclusion

The Code is consistent with human rights because any limitation on the right to protection from arbitrary or unlawful interference with privacy is reasonable, necessary and proportionate.

---

[2] Office of the High Commissioner for Human Rights, *Freedom of opinion and expression*, GA Res 44/12, UNHRC, 44th sess, 27th mtg, Agenda Item 3, UN Doc A/HRC/44/L.18/Rev.1 (14 July 2020, adopted 16 July 2020).

Gayle Milnes, National Data Commissioner