EXPLANATORY STATEMENT

Issued by the authority of the National Data Commissioner

Data Availability and Transparency Act 2022

Data Availability and Transparency (National Security Measures) Code 2022

Purpose and operation

This explanatory statement accompanies the *Data Availability and Transparency (National Security Measures) 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. Section 126 of the Act provides that 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 entities, 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. The Code prescribes a number of requirements for data sharing agreements for the purposes of subsection 19(16) of the Act.

Data may only be shared under the scheme with accredited entities. Only the Commonwealth, states and territories, Commonwealth, state and territory government bodies and Australian universities may be accredited. Therefore, data may not be shared under the scheme with a foreign entity.

The Code manages national security risks that may arise if individuals who are foreign nationals who work within an accredited entity are able to access data shared under the scheme. The Code establishes a default rule that all data sharing agreements under the scheme must provide that access to data shared with an accredited entity under the scheme is restricted to individuals within the entity who are Australian citizens or permanent residents.

If a foreign national within an accredited entity is to be provided with access to shared data, the data sharing agreement covering the data sharing must specifically name the foreign national and provide details of their proposed role in the project. When negotiating the data sharing agreement, the parties must apply the data sharing principles in section 16 of the Act, including the 'people principle' in subsection 16(3) of the Act. This principle requires the data custodian sharing the data, the accredited user and any accredited data service provider involved in the data sharing project to be satisfied that data is only made available to appropriate persons. The *Data Availability and Transparency Code 2022* provides how the data sharing principles must be applied.

Additionally, if a foreign national within an accredited entity is to be provided with access to shared data, the Code in effect prevents any data sharing until at least 14 days after the accredited entity provides specified details of the foreign national to the Australian Security Intelligence Organisation (**ASIO**), together with a copy of the data sharing agreement. The Code achieves this by providing that entities involved in the data sharing project cannot be satisfied that the project is consistent with the people principle until a particular period of time has elapsed. The Act provides that a data custodian cannot share data under the Act unless they are satisfied the project is consistent with the data sharing principles, and that accredited entities cannot collect or use shared data unless they are satisfied the project is consistent with the data sharing principles.

Authorised Version Explanatory Statement registered 21/12/2022 to F2022L01722

If a foreign national is seeking access to data shared under the scheme, their details will be provided to ASIO to assess national security risks of the foreign national having access to the particular Australian Government data to be shared. If ASIO considers there to be national security risks, ASIO may provide advice to the data custodian regarding risks of data sharing, and, if necessary, advice to to the Commissioner.

Where data is shared under the scheme with or through an Australian university that is accredited under the Act, and a foreign national within the university is permitted to access shared data, the Code imposes additional requirements. In this circumstance, the Code requires the data sharing agreement covering the data sharing project to provide that the university must ensure that due diligence has been undertaken in relation to the foreign national and that the foreign national has undertaken training in national security issues. The data sharing agreement must also provide that the university must have regard to Australian Government guidance and reports regarding foreign interference in the higher education and research sectors.

Data may only be shared, collected and used under the Act in accordance with a registered data sharing agreement that is in effect and that meets the requirements of the Act, including requirements prescribed for the purposes of subsection 19(16) of the Act. Therefore if a data sharing agreement covering a data sharing project does not comply with the Code, sharing, collecting or using data as part of the project purportedly under the Act may be an offence under the Act and contravene a civil penalty provision in the Act.

In its report on its inquiry into the Data Availability and Transparency Bill 2020 and the Data Availability and Transparency (Consequential Amendments) Bill 2020 tabled in April 2021, the Senate Finance and Public Administration Legislation Committee made three recommendations. Recommendations 1 and 2 were as follows:

1. The committee recommends that assurances are provided to Parliament regarding appropriate ongoing oversight by security agencies of data sharing agreements and potential security risks.

2. The committee recommends that any relevant findings of the Parliamentary Joint Committee on Intelligence and Security inquiry into national security risks affecting the Australian higher education and research sector are taken into account as part of the development of any additional data codes and guidance material and inform continued engagement with the national security community.

The Code responds to these recommendations.

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 or more 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 (ADSP are specialist data service providers). The only entities that may be accredited as users or ADSPs are the

Authorised Version Explanatory Statement registered 21/12/2022 to F2022L01722

Commonwealth and Commonwealth bodies, State and Territory governments and their bodies, and Australian universities.

The Act establishes a risk management framework comprising five data sharing principles, which are the 'project principle', 'people principle', 'setting principle', 'data principle', and 'output principle'. 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. Using shared data in a manner that is contrary to the applicable data sharing agreement may be an offence and may contravene a civil penalty provision. The Code introduces additional requirements for data sharing agreements and the application of the data sharing principles.

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 a data code that included provisions equivalent to those in the Code, which was available on the Office of the National Data Commissioner's website. A total of 37 submissions were received as part of this consultation process. The Code reflects changes made following consultation to expand the range of information about foreign nationals to be provided to ASIO, and to minimise the number of entities who have access to this information.

ASIO was consulted on the information that will be provided to it by accredited entities as part of the implementation of the Code.

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

Section 1 of the Code provides that the name of the instrument is the *Data Availability and Transparency (National Security Measures) Code 2022*.

Section 2 - Commencement

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

Section 3 - Authority

Section 3 of the Code provides that the instrument is made under section 126 of the *Data Availability and Transparency Act 2022*, which provides that the Commissioner is authorised to make codes of practice about the scheme. Amongst other matters, the Code prescribes requirements for data sharing agreements for the purposes of subsection 19(16) of the Act.

Section 4 - Definitions

Authorised Version Explanatory Statement registered 21/12/2022 to F2022L01722

Section 4 of the Code notes that a number of terms used in the instrument are defined in the Act, including ***accredited entity***, ***ADSP-enhanced data***, ***data sharing agreement***, ***designated individual*** and ***output***.

Section 4 also defines 3 terms for the purposes of the Code:

> ***Act*** is defined to mean the *Data Availability and Transparency Act 2022*.
>
> ***foreign entity*** is defined to mean a body corporate incorporated outside Australia or an unincorporated body formed outside Australia that does not have its head office or principal place of business in Australia. This definition is not intended to cover foreign governments or authorities of foreign governments that are not bodies corporate. However, the definition is otherwise intended to be read broadly to cover bodies corporate established or controlled by foreign governments, private sector entities, not-for-profit entities and international organisations.
>
> ***permanent resident*** is defined to have the same meaning as in the *AusCheck Act 2007*. Under this definition, a person is a permanent resident if they are not an Australian citizen, they permanently reside in Australia, their presence in Australia is not subject to any limitation as to time imposed by law and they are not an unlawful non-citizen.

Section 5 - Access to data by individuals

Section 5 of the Code prescribes requirements for all data sharing agreements for the purposes of subsection 19(16) of the Act. All sharing, collection and use of data under the Act must be undertaken in accordance with the data sharing agreement covering the data sharing project (see sections 13, 13A, 13B and 13C of the Act).

Subsection 5(1)(a) of the Code provides that a data sharing agreement must require accredited entities involved in the data sharing project to ensure that access to shared data is restricted to ***designated individuals*** of the entity:

a. who are Australian citizens or permanent residents; or
b. for whom the name, nationality (or nationalities) and ***designation***, and a description of the individual's proposed role in the project, is included in the agreement.

Many data sharing projects will not involve individuals who are neither Australian citizens nor permanent residents (**foreign nationals**) accessing shared data. In these cases, the data sharing agreement could comply with the Code by including a clause that prohibits any designated individuals of accredited entities that are party to the agreement who are foreign nationals from accessing shared data. The data sharing agreement could also further limit access to particular named Australian citizens or permanent residents (this type of limitation may be required in a project for the data sharing purpose of informing government policy and programs, or research and development, as a result of applying the data sharing principles).

Where one or more foreign nationals who are designated individuals of an accredited entity will access shared data as part of a data sharing project, details of those foreign nationals must be included in the data sharing agreement, along with a clause that provides that no *other* designated individuals of accredited entities that are party to the agreement who are neither Australian citizens nor permanent residents may access shared data. This means that data may be accessed by the named foreign nationals, but no other foreign nationals.

When considering whether it is appropriate to permit a foreign national to access shared data, the parties must be satisfied the data sharing project is consistent with the data sharing principles described in section 16 of the Act, including the 'people principle' described in subsection 16(3) of the Act. The people principle provides, amongst other matters, that access to data is only provided to individuals who

Authorised Version Explanatory Statement registered 21/12/2022 to F2022L01722

have attributes, qualifications, affiliations or expertise appropriate for that access. The *Data Availability and Transparency Code 2022* explains how this principle must be applied.

The terms ***designated individual*** and ***designation*** are defined in section 123 of the Act. Designated individuals for an entity include officers, employees, contractors and agents of the entity. Each designated individual has a designation. For example, an APS employee's designation is their duties as an APS employee. Section 124 of the Act provides that, generally, and subject to the terms of the applicable data sharing agreement, an accredited entity's authorisation to collect and use data shared under the scheme extends to authorise conduct of a designated individual of the accredited entity, acting within the actual scope of the individual's designation.

Where details of a foreign national are included in a data sharing agreement as provided in paragraph 5(1)(b) of the Code, the details include a description of the foreign national's proposed role in the project. Where such a description is included, subsection 5(2) of the Code requires the data sharing agreement to restrict the individual's involvement in the data sharing project to the specified role. Any expansion to the foreign national's role would require a variation to the data sharing agreement. This requirement ensures that all parties to the data sharing agreement, and ASIO (see further the explanation of section 6 of the Code below), can consider the appropriateness of the foreign national's involvement in the data sharing project in the context of the foreign national's role.

Section 6 - Access to data by foreign individuals—notice to Australian Security Intelligence Organisation

Section 6 of the Code only applies if a data sharing agreement covering a data sharing project permits a designated individual (**relevant individual**) of an accredited entity (**responsible entity**) who is a foreign national to access shared data. This section imposes requirements about how the 'people principle' described in subsection 16(3) of the Act is to be applied. Other requirements for how the people principle is to be applied are set out in the *Data Availability and Transparency Code 2022*.

Subsection 6(2) of the Code provides that the responsible entity cannot be satisfied that the data sharing project is consistent with the people principle unless:

a. the responsible entity has provided a copy of the signed data sharing agreement, and the details of the relevant individual specified in subsection 16(3) of the Code, to ASIO; and
b. at least 14 days have passed.

The Department of Finance provides a Whole-of-Australian-Government platform named Dataplace to assist Australian Government entities to provide controlled access to Australian Government data. Where a data sharing agreement is developed in Dataplace, Dataplace will facilitate the provision of the required information to ASIO.

On receipt of a copy of the signed data sharing agreement and the details of the relevant individual specified in subsection 16(3) of the Code, from the responsible entity, ASIO will use the details of the relevant individual to identify the individual and then consider whether, given the nature of the project, the involvement of the relevant individual is likely to give rise to any national security issues. If ASIO identifies any national security issues, it may provide advice as appropriate to the data custodian. The data custodian may then decide whether to proceed or continue with the project and, if the project is to proceed, whether additional controls should be put in place to mitigate national security risks. If necessary, ASIO could also raise national security issues with the Commissioner.

The responsible entity's authorisation to collect and use shared data under section 13A of the Act (if the responsible entity is an accredited user) or section 13B of the Act (if the responsible entity is an ADSP) only has effect if the responsible entity is satisfied the project is consistent with the data sharing principles. Subsection 6(2) of the Code operates to prevent the responsible entity reaching this state of satisfaction until at least 14 days after the data sharing agreement and required information is provided to ASIO. Collection or use of data otherwise than as authorised by the Act may constitute an offence in section 14A of the Act, or contravene a civil penalty provision in section 14A.

Authorised Version Explanatory Statement registered 21/12/2022 to F2022L01722

The data custodian may give the signed data sharing agreement to the Commissioner for registration under section 33 of the Act before, during or after the 14 day period mentioned in subsection 6(2) of the Code, and the Commissioner may register the agreement irrespective of whether the 14 day period has expired.

The Code does not impose any requirement on the responsible entity to provide the details mentioned in subsection 6(4) of the Code about the relevant individual to the data custodian or any other accredited entity that is a party to the data sharing agreement. However, some of the information mentioned in subsection 6(4) about the relevant individual, such as employment details and affiliations, may need to be provided to other parties to the data sharing agreement in order for those parties to apply the people principle described in subsection 16(3) of the Act, in accordance with the requirements set out in the *Data Availability and Transparency Code 2022*.

Where section 6 of the Code applies, the responsible entity may inform any other accredited entity that is party to the data sharing agreement covering the project and the data custodian that the responsible entity has provided the material mentioned in paragraph 6(2)(a) of the Code to ASIO (the **confirmation**). Where a data sharing agreement is developed in Dataplace, Dataplace will facilitate the provision of the confirmation.

While the responsible entity is not legally obliged to provide the confirmation, no data may be shared as part of the data sharing project until at least 14 days after the confirmation has been provided. This is because subsection 16(3) of the Code provides that any other accredited entity that is party to the data sharing agreement, and the data custodian, cannot be satisfied that the data sharing project is consistent with the people principle until at least 14 days after the confirmation is received. The authorisation of the data custodian to share data under section 13 of the Act only has effect if the data custodian is satisfied the project is consistent with the data sharing principles. The authorisation of an accredited entity to collect and use shared data under section 13A of the Act (if the entity is an accredited user) or section 13B of the Act (if the entity is an ADSP) only has effect if the entity is satisfied the project is consistent with the data sharing principles.

An entity receiving confirmation from an accredited entity under subsection 6(3) of the Code may rely on the confirmation for the purposes of the Code, and does not need to take steps to ensure the confirmation is correct. For example, if a data custodian is informed by an accredited user that the user has provided the material mentioned in subsection 6(3) to ASIO, the data custodian is under no obligation to confirm with ASIO that the material has in fact been received. The data custodian may proceed on the basis that, 14 days after receiving the confirmation, it may form the view that the project is consistent with the data sharing principles. However, if the confirmation is false or misleading, the entity providing the confirmation may contravene the civil penalty provision in subsection 32(2) of the Act.

Section 7 - Access to data by foreign individuals—Australian universities

Additional requirements for data sharing agreements apply where an accredited entity that is party to the agreement is an Australian university, and a designated individual within the university who is a foreign national is to be permitted to access shared data as part of the data sharing project. In these circumstances, subsection 7(2) of the Code provides that the data sharing agreement must require the Australian university to:

a. ensure that due diligence has been carried out with respect to foreign national; and
b. ensure that the foreign national has undertaken training in national security issues including foreign interference; and
c. have regard to any guidance and reports published by Australian government security or regulatory agencies responsible for regulating the higher education or research sectors,

Authorised Version Explanatory Statement registered 21/12/2022 to F2022L01722

(including the *Guidelines to counter foreign interference in the Australian university sector* published by the Department of Education).

This section of the Code has been informed by the report of the Parliamentary Joint Committee on Intelligence and Security's inquiry into national security risks affecting the Australian higher education and research sector, tabled in March 2022.

The training for a foreign national referred to in paragraph 7(2)(a) of the Code may be delivered to the foreign national by the Australian university or another provider.

The Guidelines referred to in paragraph 7(2)(b) of the Code were developed collaboratively between the Australian Government and the university sector to further uplift the foundational elements essential for building awareness and resilience to foreign interference within universities. The Guidelines are available on the Department of Education's web site. The Department of Education's web site also includes a range of other tools and resources for Australian universities that will assist them to comply with a requirement in a data sharing agreement included in compliance with paragraph 7(2)(b) of the Code.

Authorised Version Explanatory Statement registered 21/12/2022 to F2022L01722

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 (National Security Measures) 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 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 is appointed under the Act as an independent regulator of the scheme. Section 126 of the Act provides that the Commissioner is authorised to make (and in some cases is required to make) codes of practice about the scheme.

Data may only be shared under the scheme with accredited entities. Only the Commonwealth, states and territories, Commonwealth, state and territory government bodies and Australian universities may be accredited. Therefore, data may not be shared under the scheme with a foreign entity.

The *Data Availability and Transparency (National Security Measures) Code 2022* (the **Code**) manages national security risks that may arise if individuals who are foreign nationals who work within an accredited entity are able to access data shared under the scheme. The Code establishes a default rule that all data sharing agreements under the scheme must provide that access to data shared with an accredited entity under the scheme is restricted to individuals within the entity who are Australian citizens or permanent residents.

If a foreign national within an accredited entity is to be provided with access to shared data, the data sharing agreement covering the data sharing must specifically name the foreign national and provide details of their proposed role in the project. When negotiating the data sharing agreement, the parties must apply the data sharing principles in section 16 of the Act, including the 'people principle' in subsection 16(3) of the Act. This principle requires the data custodian sharing the data, the accredited user and any accredited data service provider involved in the sharing to be satisfied that data is only made available to appropriate persons. The *Data Availability and Transparency Code 2022* provides how the data sharing principles must be applied.

Additionally, if a foreign national within an accredited entity is to be provided with access to shared data, the Code in effect prevents any data sharing until at least 14 days after the accredited entity provides full details of the foreign national to the Australian Security Intelligence Organisation (**ASIO**), together with a copy of the data sharing agreement. The Code achieves this result by providing that entities involved in the data sharing project cannot be satisfied that the project is consistent with the people principle until a particular period has expired. The Act provides that a data custodian cannot share data under the Act unless they are satisfied the project is consistent with the data sharing principles, and that accredited entities cannot collect or use shared data unless they are satisfied the project is consistent with the data sharing principles.

Authorised Version Explanatory Statement registered 21/12/2022 to F2022L01722

When provided with the details of a foreign national who may access data shared under the scheme, ASIO will assess whether national security risks may arise if the foreign national is permitted to access the particular data to be shared. If ASIO considers that national security issues may arise, ASIO will provide advice to the data custodian before data is shared. ASIO will deal with all information provided to it as permitted by the *Australian Security Intelligence Organisation Act 1979*.

Where data is shared under the scheme with or through an Australian university that is accredited under the Act, and a foreign national within the university is permitted to access shared data, the Code imposes additional requirements. In this circumstance, the Code requires the data sharing agreement covering the data sharing project to provide that the university must ensure that due diligence has been undertaken in relation to foreign national and that the foreign national has undertaken training in national security issues. The data sharing agreement must also provide that the university must have regard to Australian Government guidance and reports regarding foreign interference in the higher education and research sectors.

All data sharing under the scheme must be undertaken consistently with the *Privacy Act 1988* because the sharing of data in a manner inconsistent with the *Privacy Act 1988* or instruments made under that Act is barred by subsection 17(5) of the *Data Availability and Transparency Act 2022*.

Human rights implications

The Code engages the right to protection from arbitrary or unlawful interference with privacy. 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]

Where an individual within an accredited entity who is neither an Australian citizen nor a permanent resident is to be permitted to access data shared under the scheme, in effect, the Code operates to restrict the sharing of data under the scheme until the accredited entity provides specified information about the individual to ASIO. This required information about the individual is 'personal information', could include 'sensitive information' as defined by the *Privacy Act 1988*. While the foreign national is under no legal obligation to provide this personal information to the accredited entity so it can in turn provide the information to ASIO, the practical effect of not providing the personal information is that the data sharing project cannot proceed under the scheme. In such a case, the Australian Government data may be able to be shared under an alternate legal mechanism for sharing data, or the data sharing agreement covering the project could be amended to provide that only individuals who are Australian citizens or permanent residents may access shared data (in which case the personal information of the foreign national would not need to be collected by the accredited entity, or provided to ASIO).

[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.

Authorised Version Explanatory Statement registered 21/12/2022 to F2022L01722

In the limited cases where the Code, in effect, requires the personal information of a foreign national to be provided to ASIO if a project is to proceed under the scheme, the Code engages the foreign national's right to protection from arbitrary interference with privacy.

The Code pursues the legitimate objective of ensuring that ASIO has sufficient information to provide advice about national security risks where Australian Government data is proposed to be shared under the scheme with foreign nationals.

The interference with privacy as a result of the operation of the Code is reasonable, necessary and proportionate to achieve this objectives for three reasons.

First, the instrument limits who has access to the personal information of the foreign national. The Code has been drafted so there is no requirement for this personal information to be included in the data sharing agreement, where it would be accessed by the data custodian, any other accredited entity that is party to the data sharing agreement and the National Data Commissioner.

Secondly, the Code specifies the minimum amount of personal information to be provided to ASIO that is necessary to enable ASIO to properly identify the foreign national and assess national security risks.

Thirdly, if ASIO cannot effectively provide national security advice in advance of the sharing of Australian Government data with a foreign national, data may be shared under the scheme in a manner that gives rise to national security risks for Australia that are difficult to mitigate after the data has been accessed by the foreign national.

The Parliament has recognised that the disclosure of personal information to ASIO may be a legitimate interference with privacy (for example, subsection 7(1A) of the *Privacy Act 1988* provides that a reference in the Act to an act or practice generally does not include an act or practice so far as it involves the disclosure of personal information to ASIO).

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.

Gayle Milnes, National Data Commissioner

Authorised Version Explanatory Statement registered 21/12/2022 to F2022L01722