

## EXPLANATORY STATEMENT

**Issued by the authority of the Minister for Employment, Workforce, Skills, Small and Family Business**

*Data Availability and Transparency Act 2022*

*Data Availability and Transparency Regulations 2022*

### **Authority**

This Explanatory Statement accompanies the *Data Availability and Transparency Regulations 2021* (the Regulations).

The Regulations are made under section 134 of the *Data Availability and Transparency Act 2021* (the Act). The Act establishes a new data sharing scheme that authorises and regulates controlled access to (sharing of) Commonwealth data with accredited entities, with safeguards in place to manage risk and streamline processes. The Act will help maximise the value of public sector data by providing a mechanism to overcome existing barriers to sharing through an authorisation to override other laws where there are appropriate safeguards in place.

Section 134 of the Act provides that the Governor-General may make Regulations prescribing matters required or permitted to be prescribed by the Act, or necessary or convenient to be prescribed for carrying out or giving effect to the Act.

Section 17 of the Act sets out circumstances when data sharing is barred under the Act, including being prescribed in regulations under subsection 17(4) of the Act.

### **Purpose and operation**

The purpose of the Regulations is to prohibit Commonwealth data from being disclosed under the *Data Availability and Transparency Act 2022* (the Act) by prescribing specific data, data custodians, or circumstances in which particular data is barred from being shared under the data sharing scheme (the Scheme) established by the Act. The Regulations support the operation of the Act by ensuring scheme participants are aware of the data, and data custodians that would be prohibited from the Scheme. The Regulations would not expand the type of data that may be shared under the scheme.

Specific data and data custodians (or any of the individuals to whom the data custodian's authorisation extends under section 124 of the Act) are barred from the scheme under subsection 17(4) of the Act if listed in the regulations as:

- a provision of a law (17(4)(a)(i)); or
- an order, direction, certificate or other instrument made by an officer of the Commonwealth (including a Minister) under a provision of a law (17(4)(a)(ii)); or
- the data custodian of the data is prescribed by the regulations as an entity that must not share data in the capacity of data custodian (17(4)(b)); or
- any other circumstances prescribed by the regulations (17(4)(c)).

The Regulations bar specific data and specific data custodians from the scheme to balance the need for greater access to public sector data with other legitimate interests. This recognises that certain highly sensitive Commonwealth data should only be shared for the purposes for which it was collected, and under dedicated frameworks.

The barred public sector data includes Commonwealth intelligence and law enforcement related data. This includes, but is not limited to, data held by entities such as the Australian Federal Police, the Australian Secret Intelligence Service, the Australian Security Intelligence Organisation, and the Australian Signals Directorate, to preserve existing arrangements and frameworks that authorise and regulate their activities.

The Regulations made in relation to paragraph 17(4)(a) of the Act preserve non-disclosure obligations imposed by statute or through operation of certain instruments. This supplements the exclusions in subsection 17(2) of the Act, and the prohibition on sharing for a purpose that relates to, or prejudices, national security in subsection 15(2) of the Act. The Regulations made in relation to paragraph 17(4)(b) exclude sharing of data by prescribing data custodians. The Regulations made in relation to paragraph 17(4)(c) bar sharing of data by prescribing certain circumstances in which that data was collected, obtained or held in accordance with statute. This captures instances where prescription of the data under paragraph 17(4)(a) would not give proper effect to the intended exclusion.

## **Consultation**

The Department of the Prime Minister and Cabinet (the Department) developed the Act, the Regulations, and its underlying policy through extensive co-design and engagement with experts and others in the community. Consultation consisted of an Issues Paper, a Discussion Paper, Exposure Draft of the Bill, and a Limited Exposure Draft of Bill amendments. In addition, the Department commissioned and published three Privacy Impact Assessments. In the latest assessment, published in April 2021, the Department agreed in full or in principle to all 14 recommendations.

In developing the Regulations, all Australian Government portfolios were invited to submit a list of legislation or subordinate legislation they wanted to be considered for barring from the data sharing scheme under the Act. The Department consulted with relevant agencies from August 2018 to second half of 2021 to develop the Regulations, ensuring they give effect to the intended purpose. The Department also undertook targeted consultation with a number of agencies responsible for national security, law enforcement, or with an integrity or oversight function. Specifically, this included the Attorney-General's Department, the Department of Health, the Department of Home Affairs, the Treasury, the Department of Finance, and relevant Divisions within the Department.

The Regulations are a legislative instrument for the purposes of the *Legislation Act 2003*, with the Regulations commencing on the day after the instrument is registered on the Federal Register of Legislation. Details of the Regulations are set out in [Attachment A](#).

## **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 [Attachment B](#).

## **Details of the *Data Availability and Transparency Regulations 2022***

### 1 Name

This section provides that the title of the Regulations is *the Data Availability and Transparency Regulations 2022*.

### 2 Commencement

This section provides for the commencement of the Regulations. It provides that the whole of the instrument commences on the day after the instrument is registered on the Federal Register of Legislation.

### 3 Authority

This section provides that the *Data Availability and Transparency Regulations 2022* are made under the *Data Availability and Transparency Act 2022*.

### 4 Definitions

This section defines terms used in the Regulations. A reference to Act means the *Data Availability and Transparency Act 2022*. A reference to System Operator has the same meaning as in the *My Health Records Act 2012*.

### 5 Prescribed provisions

This section prescribes provisions of Acts and legislative instruments for the purposes of subparagraph 17(4)(a)(i) of the Act. Provisions under which sharing data is barred under the scheme are listed in the table in Section 5.

These exclusions recognise there are certain circumstances in which secrecy or non-disclosure provisions should continue to have their ordinary operation, ensuring highly sensitive data continues to be handled in accordance with those provisions. Generally, provisions prescribed under this section fall into, but are not limited to, one of the following categories:

- national security and law enforcement;
- data collected by agencies as part of an integrity or oversight function; or
- data about children and other vulnerable persons.

#### *National security and law enforcement*

Section 5 prescribes provisions from a range of national security and law enforcement laws. These laws create dedicated pathways for the sharing of intelligence and law enforcement data, which are not affected by the Act's operation. As data may be collected intrusively under these laws, including through covert surveillance, it is appropriate for sharing to take place only under these purpose-built frameworks (which are subject to close and frequent scrutiny).

Some of the provisions that are prescribed complement paragraph 17(2)(a) of the Act, making it clear that existing protections for national security and law enforcement data

continue to operate. For example, provisions from the *Australian Crime Commission Act 2002* are prescribed to exclude data from the Australian Crime Commission.

*Data collected by agencies as part of an integrity or oversight function*

Agencies with integrity or oversight functions collect a range of potentially sensitive data that is necessary to perform these functions, such as processing complaints and undertaking investigations. The sharing of data associated with these functions is excluded from the scheme to maintain the independence of these agencies and avoid prejudicing their ability to collect data necessary to perform integrity and oversight functions, including in relation to the National Data Commissioner.

Subsection 11(3) and paragraph 17(2)(a) of the Act operate to prevent the sharing of data held by integrity and oversight agencies, specifically the Australian Commission for Law Enforcement Integrity (ACLEI), the Commonwealth Ombudsman, the Australian National Audit Office and the Inspector General for Intelligence and Security. As excluded entities, these agencies cannot participate in the scheme as a data scheme entity.

There are other agencies with integrity or oversight functions whose relevant data should be excluded from the scheme. Section 5 prescribes provisions that protect data collected by these agencies with an integrity or oversight function, such as the Australian Public Service Commissioner, the Merit Protection Commissioner, and the Inspector-General for the Australian Defence Force.

Section 5 also prescribes sections 77B, 90(6) and 92 of the *Law Enforcement Integrity Commissioner Act 2006* (LEIC Act). The inclusion of these provisions is to make clear that data that is not originating with, held by, or received from ACLEI, but is nonetheless connected with its functions, is also excluded from the scheme. Prescribing these provisions from the LEIC Act is necessary as they may apply to persons other than excluded entities in certain circumstances. For example, section 86 of the LEIC Act allows persons outside ACLEI to be present during a hearing, meaning information concerning a current or ongoing hearing may not be information held by, originating with, or received from ACLEI until the record of the hearing is made under s 82(6) of the LEIC Act.

*Data about children and other vulnerable persons*

Section 5 also prescribes provisions relating to the protection of children and other particularly vulnerable groups. For example, provisions from the *Witness Protection Act 1994* are prescribed to protect the safety of persons under the protection of the National Witness Protection Program.

Similarly, provisions from the *National Redress Scheme for Institutional Child Sexual Abuse Act 2018* are prescribed to prevent the sharing of extremely sensitive information about survivors of institutional child sexual abuse, and to promote confidence in the redress scheme. Data collected about children under the *Child Support (Assessment) Act 1989* and *Child Support (Registration and Collection) Act 1988* is also excluded, as mishandling of this data could give rise to increased incidences of family violence, including harm against children.

## 6 Order or direction etc. under prescribed provision

Section 6 prescribes certain provisions from the *Foreign Proceedings (Excess of Jurisdiction) Act 1984* and the *National Security Information (Criminal and Civil Proceedings) Act 2004* (NSI Act) for the purposes of subparagraph 17(4)(a)(ii) of the Act.

Subparagraph 17(4)(a)(ii) of the Act excludes sharing if disclosure of the data in such circumstances would contravene an order, direction, certificate or other instrument made by an officer of the Commonwealth under a prescribed provision. The Attorney-General is ordinarily the relevant ‘officer of the Commonwealth’ for the provisions prescribed in this section.

This exclusion preserves non-disclosure obligations that operate by virtue of an order or other instrument made by an officer of the Commonwealth, including non-disclosure certificates under the NSI Act. By comparison, section 5 of the Regulations preserves statutory non-disclosure obligations, while paragraph 17(6)(c) of the Act preserves non-disclosure obligations arising under a court or tribunal order.

The exclusions are necessary as the inappropriate release of information covered by an order or other instrument made by the Attorney-General under these Acts could cause serious harm and threaten Australia’s national interests or national security. Prescribing provisions from the *Foreign Proceedings (Excess of Jurisdiction) Act 1984* prevents data from being shared where the Attorney-General has determined that it is in the national interest to prevent that data from being cited as evidence in foreign proceedings or from being disclosed in compliance with an order by a foreign government or related entity, including a foreign court. Instruments made under the prescribed NSI Act provisions cover instances where the Attorney-General considers that the disclosure of information is *likely* to prejudice national security. This is broader than paragraph 15(2)(b) of the Act, which precludes sharing for a purpose that actually prejudices national security.

## 7 Barred data custodians: entities acting in a capacity under *My Health Records Act 2012*

This section prescribes data custodians who are barred from sharing data under the data sharing scheme, for the purposes of subparagraph 17(4)(b) of the Act. Section 7 bars entities acting in a specific capacity in relation to the *My Health Records Act 2012* (MHR Act) from sharing data under the Act.

This exclusion completely removes data held within the My Health Record (MHR) system from the data sharing scheme, recognising the sensitivity of this data. This exclusion does not apply to data held outside the MHR system. That is, the exclusion does not apply to data which is otherwise held by or on behalf of Commonwealth bodies in a different context, where the same data may also be separately held within the MHR system.

Subsection 7(a) excludes the System Operator, the Australian Digital Health Agency (ADHA), from sharing data while acting in its capacity as System Operator under the MHR Act. Any data the ADHA holds in a capacity other than System Operator is not covered by this exclusion.

Subsection 7(b) excludes the Australian Institute of Health and Welfare (AIHW) from sharing data under the Act, while acting in its capacity as data custodian within the meaning of the MHR Act. This paragraph does not affect the AIHW's ability to share data under the scheme in its capacity as data custodian within the meaning of subsection 11(2) of the Act.

Subsection 7(c) excludes the Chief Executive Medicare from sharing data under the Act when acting in his or her capacity as the registered repository operator (within the meaning of the MHR Act). As above, this paragraph does not prevent the Chief Executive Medicare from sharing data under the Act when otherwise acting in his or her capacity as the Chief Executive Medicare (as defined in the *Human Services (Medicare) Act 1973*).

Subsection 7(d) excludes any other entity that is a 'participant in the MHR system' (within the meaning of MHR Act) from sharing data when acting in their capacity as a participant of the MHR system. Examples of participants in the MHR system include the System Operator, registered repository operator, and registered healthcare provider organisations. However, this exclusion necessarily only applies to participants in the MHR system that are also Commonwealth bodies, as only Commonwealth bodies are authorised to share data as data custodians under the Act. The introductory text to section 7 helps to qualify the extent of the exclusion, referring to 'entities that must not share data ... in the capacity of data custodian as defined in the Act.' If the entity is acting in any other capacity, they are not prevented from sharing data under the Act.

By excluding entities acting in a particular capacity under the MHR Act, not particular data, this avoids potential complexities associated with excluding copies of particular data held within the MHR system from the scheme, while copies of the same data outside the MHR system are not excluded. This exclusion means the collection, use or disclosure of data held within the MHR system are governed by the MHR Act and related rules, consistent with community expectations about how such data should be handled. The Act does not provide an alternative pathway for data held within the MHR system to be shared.

#### 8 Circumstances in which sharing is barred: *Commonwealth Electoral Act 1918*

Section 8 excludes the sharing of data collected for the purposes of the *Commonwealth Electoral Act 1918* or the *Referendum (Machinery Provisions) Act 1984*. This information is excluded from sharing under the Act given the compulsory nature of the collection of this data for the discrete purpose of maintaining Australia's political system and democracy, and prevents the disclosure of information that can, in certain instances, facilitate the reverse engineering of electoral Roll information.

Ensuring confidence in the handling of the electoral Roll is crucial to maintaining public confidence in the electoral process. Exempting the electoral Roll, enrolment and elector information avoids any perception that the Roll's management and processes permit inappropriate voting or electoral manipulation, or that they disenfranchise people who are entitled to vote.

#### 9 Circumstances in which sharing is barred: *Director of Public Prosecutions Act 1983*

Paragraph (a) excludes sharing of the contents of (or an extract from) a direction or guideline given by the Attorney-General to the Commonwealth Director of Public Prosecutions (DPP) under section 8(1) of the *Director of Public Prosecutions Act 1983*, (DPP Act) which may

relate to circumstances in which the DPP should institute or carry on prosecutions for offences.

Paragraph (b) qualifies that this exclusion only applies if the ‘relevant time’ (as defined in section 8 of the DPP Act) has not occurred. The effect of paragraph (b) is to maintain the confidentiality of a direction or guideline prior to its publication in an instrument in the Gazette, after which time its contents will be publicly available.

#### 10 Circumstances in which sharing is barred: *Health Insurance Act 1973*

Section 10 excludes sharing of data held by the Director of the Professional Services Review Scheme (PSR Scheme) for the purposes of Part VAA of the *Health Insurance Act 1973*.

The PSR Scheme is the Australian Government's means of investigating inappropriate clinical practice within Medicare and the Pharmaceutical Benefits Scheme. This exclusion prevents the sharing of data associated with these functions, helping to maintain the independence of PSR and avoid prejudicing its ability to collect the data necessary to perform its statutory functions. The exclusion protects sensitive medical information that is held by PSR but is unable to be de-identified.

#### 11 Circumstances in which sharing is barred: *Migration Act 1958*

Section 11 excludes sharing of immigration detainees’ health records held by, or on behalf of, the Department administered by the Minister administering the *Australian Border Force Act 2015*. This exclusion protects the data of vulnerable persons (in this case, persons in immigration detention, as defined in the *Migration Act 1958*).

Paragraphs (a)-(c) together operate to exclude the health records of current and former detainees (the latter being persons who have left immigration detention or who are deceased).

Paragraph (a) outlines what is meant by ‘health information about a person’ and clarifies that the concept extends to health information about deceased persons.

Paragraph (b) identifies the Department administered by the Minister administering the *Australian Border Force Act 2015* (currently the Department of Home Affairs) as the data custodian of the health information. This health information may be included in a record held by the Department or held on its behalf, recognising that third parties may provide health services at immigration detention centres.

Paragraph (c) clarifies that the records referred to in paragraph (b) include the records of current detainees and the records of former detainees (provided the record was created during the person’s time in immigration detention).

#### 12 Circumstances in which sharing is barred: *Privacy Act 1988*

This section provides that sharing is excluded if the data to be shared is COVIDSafe app data (within the meaning of the *Privacy Act 1988*). The intention is that any collection, use or disclosure of COVIDSafe app data is left to the dedicated framework in Part VIIIA of the *Privacy Act 1988*.

This section uses the definition of COVID app data in subsection 94D(5) of the *Privacy Act 1988* to completely exclude COVIDSafe app data from the scheme. The definition of COVID app data includes data that is, or has been, stored on a communication device, meaning this section excludes the sharing of all COVID app data, irrespective of whether the data is stored on a communication device or has been uploaded from a device to the National COVIDSafe Data Store.

### 13 Circumstances in which sharing is barred: *Royal Commissions Act 1902*

This section provides for the exclusion of the sharing of data produced by, given to, or obtained by, a Royal Commission, recognising the particular sensitivity of information that is made available to Royal Commissions.

This exclusion complements the exclusion in subsection 17(6) of the Act, which excludes information that was collected using a tribunal, authority or other person's compulsory information-gathering powers and is being held as evidence. This section extends the exclusion to:

- all materials before Royal Commissions that were compulsorily acquired (not just formal evidence);
- information provided voluntarily to Royal Commissions;
- information provided in a private session of a Royal Commission; and
- information from a Royal Commission that has concluded.

However, the exclusion does not apply to any information that has been made publicly available in accordance with the *Royal Commissions Act 1902*, such as through a report of a Royal Commission's findings.



## **Statement of Compatibility with Human Rights**

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

The Regulations are 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 Regulations**

The *Data Availability and Transparency Regulations 2021* (the Regulations) exclude certain data and data custodians from the data sharing scheme (the Scheme) established under the *Data Availability and Transparency Act 2022* (the DAT Act). The DAT Act authorises Commonwealth bodies to share (provide controlled access to) public sector data with accredited entities for specific purposes in the public interest, with safeguards to mitigate risk, including in relation to privacy.

The Regulations prescribe certain data from being shared (including data created in certain circumstances) and certain data custodians from the Scheme only where strictly necessary to balance the need for greater access to public sector data, whilst upholding other legitimate interests. This approach acknowledges there are circumstances where certain secrecy or non-disclosure provisions should not be overridden by the DAT Act, and ensures highly sensitive data continues to be handled under dedicated frameworks.

If a provision or circumstance is not prescribed in the Regulations, it remains at the discretion of the data custodian to decide whether it is appropriate to share data in that particular circumstance, as the DAT Act creates no duty to share (noting reasonable requests must be considered, and reasons for refusal be provided).

The Regulations do not expand the type of data that may be shared under the Scheme.

### **Human rights implications**

The Regulations engage 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 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.

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 Regulations uphold the right to privacy by precluding the sharing of highly sensitive data, including, but not limited to data related to national security, the electoral Roll and certain health and children's data. By listing these provisions and circumstances where sharing is excluded in the Regulations, the existing laws that protect,

and regulate the use of, government data are preserved, and this ensures channels for data access within those dedicated frameworks are not affected.

The Regulations bar provisions of a number of national security and law enforcement legislation, including, but not limited to, the Criminal Code and the *Intelligence Services Act 2001*, in recognition that data may be collected intrusively under these Acts, including through covert surveillance. While collection of this data under the respective legislation is reasonable, necessary and proportionate to protect national security, it is not necessary to achieve the DAT Act's permitted purposes. The Regulations consequently support the right to privacy by preserving existing national security legislation and excluding these Acts from the DAT Act's override authority.

The Regulations also bar protected information under the *Child Support (Assessment) Act 1989*, *Child Support (Registration and Collection) Act 1988*, and the *National Redress Scheme for Institutional Child Sexual Abuse Act 2018*. This excludes sensitive data collected about children, including vulnerable children. Mishandling of this data could give rise to increased incidences of family violence, including harm against children. The exclusion of sensitive children's data from the Scheme therefore promotes the right to privacy.

As a further privacy enhancing measure, the Regulations also prescribe several circumstances where sharing is barred. For example, the Regulations bar the sharing of:

- Commonwealth electoral Roll and Roll related data: This is necessary given the compulsory nature of the data's collection for the discrete purpose of maintaining Australia's political system and democracy. Barring this data from the Scheme ensures the protection of residential addresses and other personal data. This is particularly important for individuals registered as silent electors whose safety would be compromised if their address were to be made publicly available. Ensuring confidence in the handling of the Commonwealth Electoral Roll is crucial to maintaining public confidence in the electoral process and promoting an individual's right to privacy.
- My Health Record and COVID Safe App data: Barring this data supports the right to privacy by maintaining current legislative frameworks that are dedicated to handling health data appropriately, in line with community expectations.
- Migrant information, which includes health and security related data, collected under the *Migration Act 1958*: Barring this data further supports the right to privacy by protecting the identity and health information of migrants, in line with community expectations.
- Data produced by, or obtained by, a Royal Commission and that has not been released in accordance with the *Royal Commission Act 1902*, or data pertaining to the *Director of Public Prosecutions Act 1983*. By protecting sensitive information obtained in the course of proceedings, including private sessions, barring this data upholds the right to privacy.

Preserving these existing legal protections advances privacy protections for individuals, including children and other vulnerable groups, and safeguards the confidentiality of their sensitive information.

### **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.<sup>1</sup>

The Regulations impose 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. The Regulations achieve this balance by precluding the sharing of highly sensitive information within the data sharing scheme. This aligns with the intent of the DAT Act to preserve existing rights and privileges over public sector data by precluding any sharing that would contravene such interests.

Strictly necessary exclusions in the Regulations ensure sharing of highly sensitive data, particularly data involving national security purposes and entities, continues to be handled under dedicated frameworks. These restrictions are reasonable as they limit the transmission of information to the extent necessary to protect national security or to safeguard the privacy of individuals where legitimate risks are posed.

The Regulations represent a proportionate means of restricting access to data under the scheme as exclusions have been designed through extensive consultation with relevant agencies, and only granted from the scheme where strictly necessary, and where broader exclusions on the face of the DAT Act do not apply.

For the reasons outlined above, the Regulations and their operation alongside the Scheme constitute a permissible limitation to the Right to freedom of expression, including to seek, receive and impart information.

## **Conclusion**

The Regulations are compatible with human rights as they strengthen the protection of human rights. Where the Regulations may limit particular rights, the limitations are reasonable, necessary, and proportionate with human rights.

**The Hon. Stuart Robert MP, Minister for Employment, Workforce, Skills, Small and Family Business**

---

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