Australian Government

Department of the Prime Minister and Cabinet

ANDREW FISHER BUILDING
ONE NATIONAL CIRCUIT
BARTON

Senator Claire Chandler
Chair
Finance and Public Administration Legislation Committee
Parliament House
CANBERRA ACT 2600

Dear Senator

I write to provide additional information to the Committee following my appearance before the Finance and Public Administration Legislation Committee (the Committee) at the hearing on the Data Availability and Transparency Bill 2020 (the Bill) and Data Availability and Transparency (Consequential Amendments) Bill 2020 (the Consequential Amendments Bill) on Tuesday 20 April 2021.

If passed, the Bill would operate together with Australian Government policy, legislation and activities in relation to national security, cyber security and privacy protection. These areas were covered in written submissions and oral evidence to the Committee. This letter clarifies and provides additional information on the Bill's interaction with these matters.

National security

I answered a number of questions during the public hearing that related to national security issues and the involvement of the Australian Security Intelligence Organisation (ASIO) in the process of sharing Australian Government data under the proposed scheme, especially with foreign entities.

National security community involvement

The Office of the National Data Commissioner had significant engagements and consultations with Australian intelligence agencies during the development of the Bill. The input and feedback have been critical to ensure the Bill establishes a series of protections to prevent Australian Government data from being used inappropriately by foreign entities.

Formalising ASIO role

The National Data Commissioner (Commissioner) will enter into a memorandum of understanding with ASIO to document the everyday working relationship in relation to the accreditation process and other matters, if the Bill is enacted.

National security considerations and conditions on accreditation

Data can only be shared under the scheme with entities that are accredited as users by the Commissioner. Any foreign entity seeking accreditation must meet the accreditation criteria, which include that "the entity's participation in the data sharing scheme would not pose concerns for reasons of security (within the meaning of the

Australian Security Intelligence Organisation Act 1979)" (clause 77(1)(g) of the Bill). When assessing whether this criterion is met, the Commissioner will rely upon advice from ASIO in the form of a security assessment. If an entity is not accredited because of an ASIO recommendation, it will not be able to receive any data under the scheme. ASIO recommendations can also result in the imposition of conditions of accreditation on a foreign entity for security reasons, including constraints on data or the individuals who can access shared data.

Importantly, decisions by the Commissioner to suspend, cancel or impose a condition on the accreditation of a foreign entity for security reasons are not reviewable by the Administrative Appeals Tribunal (clause 118 of the Bill).

Ongoing accreditation monitoring and reviews

The security review is an ongoing process that continues past the accreditation stage. ASIO will have access to the names of the accredited entities and the data sharing agreements these entities enter into. If, at any time, ASIO has security concerns they can make a recommendation to the Commissioner.

Additional restrictions and constraints on data access

Under the Bill, an accredited entity, foreign or otherwise, does not have any enforceable right to access data. The decision to share data rests with the relevant data custodian – an Australian Government agency.

When considering whether to share data, the data custodian would need to be satisfied that:

- the sharing was for an appropriate purpose (clause 15(1) of the Bill);
- the sharing would not be for a purpose that relates to, or prejudices, national security (clause 15(2) of the Bill); and
- the data sharing is consistent with the data sharing principles (clause 16 of the Bill) including:
    - sharing would be in the public interest;
    - the data was only being made available to an appropriate person; and
    - appropriate security controls are applied to the data.

Accessing data from secure environments

In many cases it would be appropriate to require an accredited user to access Australian Government data in a secure environment in Australia. Further, the Commissioner may make a data code (which is disallowable legislative instrument binding on all scheme entities) requiring that certain Australian Government data is only accessed in Australia.

Transparency of decisions to share

Data can only be shared with any entity, including a foreign entity, through a legally binding data sharing agreement that sets out the details of what data is being shared with whom, and with what controls. The key terms of data sharing agreements will be public.

Purpose restrictions in data sharing agreements

The specific purpose for which shared data can be used must be set out in the data sharing agreement and any other use is expressly prohibited. Any "output" from the use of shared data remains subject to the controls to be established by the Bill, unless the data custodian expressly agrees and documents in the data sharing agreement that a particular output can be made public.

Redress and penalties and extraterritorial operation

If an entity fails to comply with a data sharing agreement or any other requirements to be imposed by the Bill, they are subject to civil penalties or injunctions. The Bill has extraterritorial operation (clause 7 of the Bill).

Authorisation for Commissioner to disclose and receive information

If matters arise with data sharing under the scheme that fall within the remit of other regulators or integrity bodies (including ASIO and law enforcement), the Bill creates an authorisation to provide information to those bodies if the Commissioner is satisfied that the information will assist those bodies to perform any of their functions or exercise any of their powers (clause 108 of the Bill).

Cyber-security

I was asked about the risks that could arise if hackers and cyber-attackers accessed Australian Government data shared under the scheme. I note that the Government is already expected to meet strong cyber-security standards and to protect data from unauthorised access.

Government data security is managed through a number of legislative and policy mechanisms such as the Protective Security Policy Framework. The whole-of-Government Hosting Strategy and Hosting Certification Framework further supports the Government's approach to secure data storage and provides clear data security guidance for commercially owned data centres that house Government data.

As part of Australia's Cyber Security Strategy 2020, the Government also made a commitment to consider legislative changes to make Australian businesses more resilient to cyber security threats. This work will complement reforms to the *Security of Critical Infrastructure Act 2018* by ensuring that all businesses in the digital economy are cyber resilient.

As Australian Government policies evolve over time, data custodians will be expected to apply the updated policies, as applicable, to entities receiving data shared under the scheme.

This expectation will be included in guidance to be issued by the Commissioner, and if necessary, in a data code issued by the Commissioner, which, as noted earlier, is a disallowable legislative instrument binding on all scheme entities.

Security requirements on the accredited user must be included in the data sharing agreement, which is legally binding on the accredited user and which will be published by the Commissioner.

Role of accredited data service providers

Where accredited users cannot meet the security standards required by the data custodian, consideration can be given to sharing the data with the accredited user using a secure facility operated by an accredited data service provider. Accredited data service providers are organisations that have been accredited as having relevant technical expertise and can offer complex data integration and/or share data on behalf of a data custodian. The security standards for these providers will be assessed as part of the accreditation process. The standards applied will draw on existing government policies which are currently observed by those running existing secure facilities such as the ABS DataLab.

Privacy

The Committee heard from a number of witnesses who had concerns about privacy issues associated with the sharing of personal information under the scheme. In this context it may be helpful to clarify the interaction between the Bill, if passed, and the *Privacy Act 1988*.

As principles-based legislation, the Bill has been designed to work with, and to be supported by, the *Privacy Act 1988* (as it may be in force from time to time), rather than the Bill replicating particular provisions in the *Privacy Act 1988* at a point in time. If the *Privacy Act 1988* is amended in the future (for example, following the current review), the provisions of the Bill will continue to operate in the context of the amended provisions of the *Privacy Act 1988*.

The Bill, if passed, and the *Privacy Act 1988*, work together. The Bill will provide in certain limited circumstances an express authorisation for personal information to be shared, collected and used. This type of express statutory authorisation to disclose, collect and use personal information is common in Commonwealth legislation. Many secrecy provisions in Commonwealth legislation enable information covered by the provision to be disclosed for particular purposes, such as in the public interest. The authorisation in the Bill works with Australian Privacy Principle 6 to allow the sharing of personal information by the data custodian, and the collection and use of the personal information by the accredited user, to happen consistently with the Commonwealth *Privacy Act 1988*.

Clause 28 of the Bill requires that, where personal information is shared, the accredited user be covered by the *Privacy Act 1988,* or an equivalent state or territory law. If an accredited user engages in an activity with personal information that is not authorised by the relevant data sharing agreement, this will be a breach of the applicable privacy legislation and any individual who is adversely affected can seek redress. Part IIIC of the *Privacy Act 1988*, relating to the mandatory notification of eligible data breaches, apply to data breaches involving data shared under the scheme. In addition, any breach of the mandatory provisions in a data sharing agreement will be a breach of the provisions in the Bill that can result in the imposition of civil penalties.

Availability of Regulations and Guidelines

I understand that the Minister's intention is to make available another version of the draft Regulations before the Bill is debated in the House of Representatives. The Regulations will prescribe additional kinds of data that cannot be shared under the scheme.

Regulations, other legislative instruments and guidelines for the scheme cannot be made until after the Bill is passed. However, it is the intention that any necessary data code and guidance material is available before the sharing of data commences under the new scheme.

As data sharing can only occur with entities accredited under the scheme, the initial focus will be on undertaking user accreditation. This will allow time for the Office of the National Data Commissioner to finalise and publish materials to support decisions by data custodians to share data.

Yours sincerely

Ms Deborah Anton
Interim National Data Commissioner
Department of the Prime Minister and Cabinet
22 April 2021