



Australian Government

Australian Government response to the
Senate Finance and Public Administration Legislation Committee report:

Data Availability and Transparency Bill 2020 [Provisions] and Data
Availability and Transparency (Consequential Amendments) Bill 2020
[Provisions] April 2021

MARCH 2023

Introduction

The Australian Government welcomes the opportunity to provide a response to the Senate Finance and Public Administration Legislation Committee (committee) report, *Data Availability and Transparency Bill 2020 [Provisions] and Data Availability and Transparency (Consequential Amendments) Bill 2020 [Provisions]*, tabled on 29 April 2021. The Government acknowledges the work and recommendations by members of the Committee.

The Government would also like to thank those who made submissions or gave evidence to the inquiry for their contribution, which shaped the report and recommendations.

The Committee looked into the provisions of the Data Availability and Transparency Bill 2020 (the Bill) and the provisions of the Data Availability and Transparency (Consequential Amendments) Bill 2020 (the Consequential Amendments Bill) after referral by the Senate on 4 February 2021.

Recommendations

Recommendation 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.

Response:

The Government **supports** this recommendation.

An amendment was moved in the other chamber to ensure that data sharing agreements take effect only once registered by the National Data Commissioner (the Commissioner), rather than upon parties' signature. This change mitigates potential risks by supporting the Commissioner to work with relevant security agencies to identify agreements which may pose security risks, or not comply with the data sharing scheme, prior to any data being shared. In addition, amendments were moved to ensure that foreign entities are not able to become accredited, which means that data cannot be shared with a foreign entity under the scheme.

Recommendation 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.

Response:

The Government **supports** this recommendation.

Since passage of the Bills, the Commissioner has made a data code, the *Data Availability and Transparency (National Security Measures) Code 2022*, establishing a default rule that all data sharing agreements made under the scheme must provide that access to data shared with an Australian university accredited under the scheme is restricted to individuals within the entity who are Australian citizens or permanent residents. If a foreign national within an Australian university 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.

This data code takes into account the findings of the Parliamentary Joint Committee on Intelligence and Security inquiry into national security risks affecting the Australian higher education and research sector, and the Guidelines to Counter Foreign Interference in the Australian University Sector.

Recommendation 3: The committee recommends that consideration is given to whether amendments could be made to the bill, or further clarification added to the explanatory memorandum to provide additional guidance regarding privacy protections, particularly in relation to the de-identifying of personal data that may be provided under the bill's data-sharing scheme.

Response:

The Government **supports** this recommendation.

Amendments were moved in the other chamber directly addressing the committee's concerns and strengthened the privacy protections in the Bill.

The privacy protections include:

- Minimising the sharing of personal information as far as possible without compromising the data sharing purpose.
- Prohibiting the re-identification of data that has been de-identified.
- Prohibiting the storing or accessing of personal information outside of Australia.
- Making it mandatory for Accredited Data Service Providers to undertake any complex data integration for projects to inform government policy and programs, and research and development.
- Requiring express consent for the sharing of biometric data.

Furthermore, the Commissioner has made a data code, the *Data Availability and Transparency Code 2022*, requiring consent to be current and specific, and providing that an individual may withdraw consent at any time with prospective effect.

Additional privacy protections are also required, dependent on the data sharing purpose. Personal information will be able to be shared without consent for the delivery of government services where the individual concerned is receiving the service. The amended Bill minimises the sharing of personal information for informing government policies and programs, and for research and development, by promoting de-identification of data.
