



August 1, 2018

Australian Government
Department of the Prime Minister and Cabinet
PO Box 6500
Canberra ACT 2600
Australia

Submitted via electronic filing to <https://www.pmc.gov.au/>

Re: Microsoft's Comments on the Issues Paper Consultation on the New Australian Government Data Sharing and Release Legislation

I. Introduction

Microsoft welcomes this opportunity to offer its comments on the Issues Paper for Consultation on the New Australian Government Data Sharing and Release Legislation (hereinafter the "Issues Paper"). Microsoft has long been a proponent of making public sector data open and interoperable in order to improve government processes and services and streamline government functions. For its part, Microsoft has assisted many government organizations in meeting their goals of improving transparency, citizen participation, interoperability, and efficient agency collaboration through expanded access to public sector data. This includes the development of software assets that allow government agencies to securely publish and interact with their data on the cloud.

Microsoft also strongly agrees that open public sector data is an essential driver of innovation. In fact, Microsoft has recently launched [Microsoft Research Open Data](#), which makes available datasets created by researchers at Microsoft and published in conjunction with their research. We are confident that such open data repositories will have wide-ranging benefits for the public, including fostering and facilitating collaboration among researchers and creating a more level playing field for businesses. The increase of easily accessible, interoperable, and reusable private and public sector datasets across the globe creates opportunities to improve government functions, democratize technology, and fuel innovation and economic growth. Expanding access to Commonwealth datasets—including by industry and others in the private sector—also will be critical to ensuring that Australians reap the full benefits of artificial

intelligence, big data analytics, and related technologies, all of which depend directly on access to high-quality and extensive datasets.

II. Specific Comments for Consideration

Microsoft applauds the Australian Government's efforts to create a transparent process through which to share and release public sector data within the government and to the public. Although we believe the Issues Paper provides a strong foundation for a Data Sharing and Release ("DS&R") Bill, we respectfully urge the Government to clarify or reconsider a few critical issues.

A. Promoting Public Trust, Transparency, and Privacy

As the Issues Paper notes, the Australian Government holds a large amount of data, varying in sensitivity. Microsoft agrees that the DS&R Bill must strike a balance between meeting the public's expectations for how this information will be handled and the goal of making public sector data as open as possible.

Transparency in the process is one way to garner public trust in the DS&R program. We note that the proposed process for sharing data does not appear to require Commonwealth data custodians to provide an explanation either when denying a data access request, or if they decide not to provide open access to data in the first instance, however. Microsoft suggests that the DS&R Bill require data custodians to provide such an explanation. Doing so has a range of benefits in addition to promoting public trust in the program; for example, transparency can make potential users aware of relevant datasets in the Commonwealth's possession, ensure that Commonwealth data controllers make data accessible unless there is a material reason not to (*e.g.*, if disclosure would be inconsistent with applicable law or policy), and may even provide enough information to allow requestors to alter their requests to address the data custodian's concerns. In light of these benefits, it is no surprise that the European Union's Directive on the Re-use of Public Sector Information (the "PSI Directive") requires government entities to "communicate the grounds for refusal to the applicant" and include "a reference to the means of redress in case the applicant wishes to appeal the decision."¹

It is also not clear whether the proposed process for sharing data will require data controllers to consider options beyond "release" or "do not release" when evaluating

¹ Directive 2013/37/EU of the European Parliament and of the Council on the re-use of public sector information 2013 O.J. L 175/4, Ch. II, Art. 4 (June 27, 2013), *available at* <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0037&from=FR>.

whether to provide access to data, either at the outset or in response to a data request. Microsoft foresees situations where the release of more sensitive information may be useful for research or development of services that have a significant public benefit (e.g., the development of specific medical interventions). In these scenarios, the DS&R process should require Commonwealth data controllers to evaluate whether such sensitive datasets can be de-identified, culled, or released to users under conditions that maintain individuals' privacy.

Microsoft also notes that the Issues Paper is largely focused on the guiding principles, processes, and roles and responsibilities of the anticipated DS&R program. Once the framework is outlined, however, it may be prudent to include guidance for government entities on strategic planning and best practices to manage, share, and release data. For example, in the United States, the Office of Management and Budget's Open Data Policy includes requirements to collect and create information in a way that supports downstream dissemination, build information systems to support interoperability and accessibility, and maintain enterprises data inventories and public data listings.² This includes incorporating privacy analyses into each stage of the information's life cycle to determine whether it can be made publicly available pursuant to applicable law.³ Such guidance may help Commonwealth agencies efficiently transition to compliance with the DS&R Bill and ensure that data is prepared for release or sharing from collection or creation.

B. *Ensuring Public Sector Data is Accessible*

Microsoft believes that public sector data should be made available to the widest range of users and for the broadest purposes permitted by law, subject to appropriate safeguards to protect personal information. The following comments address what we perceive to be potential hindrances to achieving those ends.

1. *Greater Clarity in the Obligations of Data Custodians*

As an initial matter, the Issues Paper would benefit from greater clarity in the obligations of Commonwealth data custodians to expand access to public sector data. Although several passages in the Issues Paper make clear that data custodians should strive towards this outcome (see, e.g., p. 12, citing to *Public Data Policy Statement*), other

² Sylvia Burwell, *M-13-13 — Open Data Policy—Managing Information as an Asset*, Office of Management and Budget § III(1) (May 9, 2013), available at <https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf> (hereinafter "U.S. Open Data Policy").

³ U.S. Open Data Policy § III(4).

passages could be read to suggest that these entities will have no affirmative duty to provide access to data in their control and are only required to evaluate whether to provide such access in response to a request (*see, e.g.*, pp. 12-13, indicating that “the process for sharing data under the DS&R Bill” begins with a “Request for data to data custodian”; p. 18, stating that it is the responsibility of data custodians to “assess[] requests for access to data under the DS&R Bill”).

We respectfully urge the Government to clarify that a key responsibility of Commonwealth data custodians will be to make data in their control open and accessible—unless doing so would be inconsistent with applicable law or policy, in which case they should undertake the Five-Safes framework to determine whether they can release the data subject to appropriate controls and safeguards. Absent such an affirmative duty of access, large swaths of Commonwealth data that are entirely appropriate for access or reuse might remain hidden away and inaccessible—a result that would undermine the goals that the Government seeks to achieve.

The EU’s PSI Directive again offers a model here. It provides, as a founding principle, that EU Member States “shall ensure that documents to which this Directive applies . . . shall be re-usable for commercial or non-commercial purposes.” (Article 3(1)). We note, more generally, that the EU is in the midst of reforming the PSI Directive to promote even greater openness and availability of public sector data.⁴

2. *The Purpose Test Appears Limited to Government Uses*

The DS&R Bill’s proposed process for sharing public sector data includes a step that requires the data custodian to determine whether the use of the requested data meets a purpose test. As enumerated, the purpose test appears to be skewed towards government uses and envisions only very limited private-sector access to data (*see, e.g.*, p. 14 of the Issues Paper). All four listed purposes appear to anticipate uses only by either government entities, or by “research institutions and academics.” (*Id.*) Missing from the purpose test is use by private sector entities for research and development of new products or services, including products or services that may not, at the time of the request, have “clear and direct public benefits.” As a result, the purpose test may prevent private-sector persons and entities from accessing public-sector data for lawful and appropriate purposes—an outcome that would put Australian industry and society at a disadvantage to those in the United States, the EU, and other jurisdictions that impose no such “purpose” restrictions on private-sector access to public-sector data.

⁴ The proposed amendments to the EU’s PSI Directive are *available at* <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:0234:FIN>.

Although concerns about inappropriate uses of government data are valid, these can and should be addressed by the Five Safes framework (or whichever risk management framework is ultimately incorporated into the DS&R Bill). Specifically, the “safe people” and “safe project” elements of the Five Safes frameworks appear to encompass the concerns underling the purpose test.

Microsoft recommends that the Australian Government either remove the purpose test from the DS&R or include additional appropriate purposes that encompass use by private sector entities and others outside of the government. Removing the purpose test and relying on the Five Safes framework to ensure the data is used appropriately would also eliminate a step in the process, potentially streamlining the sharing and releasing of public sector data.

In this regard, we also respectfully urge the Government to clarify that, where the data in question raises no privacy concerns (*i.e.*, it cannot be used to identify any individual) and is otherwise non-sensitive (*e.g.*, it is neither proprietary nor confidential), it should qualify as “safe data” under the first element of the Five Safes test and should therefore not be subject to any further restrictions on access. As the Issues Paper itself notes, “Much of the Australian Government’s data is not personal or sensitive” (p. 8), and with regard to such data—*e.g.*, weather data; public bus schedules; aggregate, non-proprietary economic data, etc.—there is no legitimate reason to limit access to it.

3. *The Proposals on Trusted Users and Accreditation Should Be Narrowed*

The Issues Paper introduces the concept of “trusted users,” which it defines broadly as “the end-users of data shared or released by [Commonwealth] data custodians” (p. 19). It also provides that “trusted users would be accredited by demonstrating they can safely use and handle data under the requirements of the DS&R Bill, including the Five-Safes framework” (*id.*). Although we support the goal of promoting responsible data use, we respectfully urge the Government to consider two modifications to this “trusted user” approach.

First, it would be helpful for the Government to clearly articulate those scenarios in which access to data should be available only to “trusted users.” As already noted, much of the data held by Commonwealth is neither private nor sensitive, and providing access to this data raises no privacy or other policy concerns. In these situations, there is no legitimate reason to limit access only to persons or entities that qualify as “trusted.” On the contrary, access to such data should face the fewest barriers possible to broad public access so as to maximize its potential value for Australian society. In our view, data custodians should limit data access to “trusted users” only in those cases

where other appropriate controls and safeguards (e.g., anonymization of data) cannot adequately address the identified risks.

Second, we urge the Government to reconsider whether accreditation is the best path for designating users as “trusted.” It is likely that different types of data and use-scenarios will vary significantly with regard to the safeguards they require in order to avoid data misuse. Given this variation, a one-size-fits-all accreditation regime might not be the most efficient or effective means to protect against such misuse. For instance, data custodians might be able to achieve these goals more effectively by imposing contractual restrictions on users (where necessary and appropriate) that are uniquely tailored to the specific risks identified. Although the current lack of detail in the proposed accreditation regime makes it difficult to assess its merits more precisely, we urge the Government to give this idea further thought and to seek further stakeholder input once this accreditation concept is further developed.

4. *Licensing Should be Clearly Addressed in the DS&R Bill*

The Issues Paper does not appear to address whether open government data will be subject to any licensing requirements.⁵ To be useful for government efficiencies and private sector innovation, Microsoft recommends that the DS&R Bill make open government data available subject to open licenses (or the equivalent Creative Commons licenses) with limited, if any, restrictions on its use. For example, the U.S. Open Data Policy requires government agencies to apply open licenses to data as it is collected or created so that there are no restrictions on copying, publishing, distributing, transmitting, adapting, or otherwise using the information for non-commercial or for commercial purposes once it is made public.⁶ Similarly, the EU’s PSI Directive requires that any licenses for the re-use of public sector information should include as few restrictions as possible.⁷

5. *Exclusivity Should be Clearly Addressed in the DS&R Bill*

We note that while exclusivity is discussed in the Productivity Commission Report,⁸ the Issues Paper does not discuss whether the DS&R Bill will prohibit government agencies

⁵ Licensing is briefly mentioned in the Australian Government Public Data Policy Statement, but Microsoft recommends that licensing requirements be explicitly set forth in the DS&R Bill.

⁶ U.S. Open Data Policy § III(1)(c).

⁷ PSI Directive, Ch. III, Art. 8.

⁸ Productivity Commission, *Data Availability and Use*, Report No. 82 at p. 139 (2017).

from granting exclusive rights to any government data. Other governments have recognized that the imposition of exclusive access limitations on public sector data is contrary to the public interest and can rarely be justified. For example, the EU has prohibited such exclusive arrangements, stating that the government “shall not grant exclusive rights” unless it “is necessary for the provision of a service in the public interest.” Furthermore, in the event an exclusive right is granted, its validity must be reviewed every three years.⁹ Microsoft recommends that the DS&R Bill similarly include a prohibition of granting exclusive rights and clearly enumerate any exceptions.

**

**

**

Microsoft greatly appreciates this opportunity to provide its perspective on the Issues Paper and DS&R Bill. We would be happy to further discuss any of our comments at your convenience.

⁹ PSI Directive, Ch. IV, Art. 11.