Office of the Victorian Information Commissioner

t 1300 00 6842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

8 August 2018

Data Legislation Team
Department of the Prime Minister and Cabinet
PO BOX 6500
CANBERRA ACT 2600

Dear Data Legislation Team,

Submission in response to the New Australian Government Data Sharing and Release Legislation Issues Paper

The Office of the Victorian Information Commissioner (**OVIC**) is pleased to provide a submission in response to the *New Australian Government Data Sharing and Release Legislation: Issues Paper for Consultation* (**the Issues Paper**).

OVIC has combined oversight of privacy, data protection and freedom of information in Victoria, and administers the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**) and the *Freedom of Information Act 1982* (Vic). My legislative responsibilities include commenting on matters affecting the personal privacy of individuals,[1] and ensuring that the objects of the PDP Act are upheld.

I thank you for the opportunity to comment on the Issues Paper. I have organised my comments below based on key themes, and where possible, have drawn reference to the relevant questions asked in the Issues Paper.

The four key points in this submission are:

1. Community trust is crucial for the success of this scheme. To ensure community trust, the scheme should draw on principles developed in privacy law to balance the potentially competing interests of data subjects and data users.
2. The proposed 'purposes test' and the 'Five-Safes Framework' may not be appropriate in making decisions to release data publicly; they should only be used for data sharing decisions.
3. Relying on de-identification of personal information carries with it significant challenges and risks and is unlikely to be appropriate in a data release context.
4. Certain elements of the Victorian data sharing model, as described in the *Victorian Data Sharing Act 2017* (Vic) (**VDS Act**), seek to address these issues and may be appropriate for inclusion in the scheme.

The need for community trust

OVIC acknowledges the need for a simple and effective mechanism for sharing government data and is supportive of using government data for evidence-based policy design.

[1] Under s 8C(1)(f) of the PDP Act.

However, such a scheme must be established in a way that accords with community expectations. If a data sharing scheme does not align with the manner in which members of the public expect their personal information to be used, it will not be met with community acceptance. Without this, the existing social license that data users such as researchers and government rely on in carrying out their current activities will be compromised. The Productivity Commission correctly stated that building community trust is a critical part of enhancing data sharing and release.[2] A data sharing and release scheme must be consistent with community expectations in order for it to be successful.

Existing privacy law seeks to reconcile the interests of data subjects and data users. Privacy has developed mechanisms and principles to handle the tension between these potentially diverging interests. For example, the objects of the PDP Act expressly acknowledge the need to balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information.[3] I suggest that the proposed scheme should consider and incorporate similar principles where appropriate, including notions of necessity, proportionality, and transparency.

The proposed framework may not be suitable for public release decisions

My office acknowledges the benefits of encouraging proactive data release schemes, rather than relying solely on the formal mechanisms under freedom of information legislation, to access data held by government. However, the model proposed for the Data Sharing and Release Bill (**DS&R Bill**) appears to have largely been designed to deal with proposals for data sharing.

There is a fundamental difference between sharing of public sector data with trusted third parties (data sharing), and open release of data to the world at large (data release). In a data sharing context, the purpose of data use can be identified and measured against the proposed purposes test that will be defined within the DS&R Bill, and protections can be applied in accordance with the Five-Safes Framework.

However, it is unclear how this model can reliably and effectively be applied to a data release proposal. None of the purposes listed in the purposes test on page 14 of the Issues Paper appear relevant to a public release scenario. This is because the purposes for which publicly available data will be used cannot be known; by definition, anyone can use open data for any purpose.

Similarly, the Five-Safes Framework is not well suited to assess and treat the risks associated with the public release of data. Security measures that relate to 'safe projects,' 'safe people,' 'safe settings,' and 'safe outputs' cannot be applied in a public release context, again, due to the inability for data custodians to know how the data will be handled once it is released. The only measure that can be applied to public release is 'safe data.'

As such, I suggest that the DS&R Bill clearly distinguish between data sharing and data release, outlining the appropriate decision-making steps for each, independently of the other, and that any future draft of the Bill provide an alternative governance model for public release. By conflating data sharing and data release, there is a risk that poor data governance will result, and that community confidence in the scheme as a whole could be undermined.

De-identification

Relying exclusively on 'safe data' to guide public release decisions is a risky proposition for data derived from personal information. Ensuring that personal information is 'safe' for public release relies on the successful

---

[2] Productivity Commission, *Data Availability and Use: Productivity Commissioner Inquiry Report, Overview and Recommendations,* No. 82, 31 March 2017, p. 2, available at: https://www.pc.gov.au/inquiries/completed/data-access/report/data-access-overview.pdf.

[3] Under s 5(a) of the PDP Act. See also s 5(b).

de-identification of that information. Section 4 of the Issues Paper notes that '(p)ublic release of data may occur when data is appropriately de-identified.'[4]

Successfully de-identifying personal information to the point where it cannot be re-identified, particularly unit-record level data, is likely to be impossible.[5] It is very difficult to determine the likelihood of re-identification for any given data set, for example, through matching information with other open or proprietary data sets that may be available to a given individual. The inability to know what other data might be available to adverse actors, and in what circumstances, means that it is impossible to develop an effective governance framework for release of unit-level data. OVIC's work in this area has identified the very real risks that can result from publicly releasing unit-record level data sets,[6] and we strongly encourage the Department of the Prime Minister and Cabinet (**DPMC**) to consider the implications of de-identification in a public release context in drafting the DS&R Bill.

Given the limitation in the application of the Five-Safes Framework and the purposes test in an open data context, OVIC suggests that DPMC reconsider its approach to data release under the proposed DS&R Bill, including whether data release (as opposed to data sharing) should be a component of this scheme at all.

Victorian data sharing model under the *Victorian Data Sharing Act 2017*

The VDS Act was enacted to promote the sharing and use of public sector data to support government policy making, service planning and design.[7] The VDS Act establishes the role of the Chief Data Officer, who leads the Victorian Centre for Data Insights (**VCDI**).

The VCDI employs a number of privacy-enhancing techniques that the DPMC may wish to consider incorporating into the proposed data sharing model under the DS&R Bill, including:

- express privacy and data security safeguards under the VDS Act, including mandatory breach notification and annual reporting requirements to OVIC;[8]
- an additional layer of protection for data analytics conducted in a controlled environment, ensuring that reasonable steps have been taken to ensure that data no longer relates to an identifiable individual or an individual who can reasonably be identified before data analytics work commences;[9]
- the provision of a clear legislative framework for the **sharing** of public sector data only, as distinct from the **release** of public sector data; and
- the employment of the Five-Safes Framework in the context of a secure environment to conduct data analytics.

In practice, the de-identification of personal information, in accordance with the 'safe data' element of the Five-Safes Framework, is just one of the security measures applied to the data under the Victorian model, as this model provides that all of the elements of the Framework, including 'safe people' 'safe settings' 'safe outputs' and 'safe projects,' can likely be assured in a secure environment. This is not true for data that is released to environments where these elements cannot be determined.

---

[4] On page 16 of the Issues Paper.

[5] See for example, Office of the Australian Information Commissioner, *Publication of MBS/PBS data: Commissioner initiated investigation report*, March 2018, p. 4, available at: https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/publication-of-mbs-pbs-data.

[6] See Office of the Victorian Information Commissioner, *Protecting unit-record level personal information*, May 2018, p. 7, available at: https://www.cpdp.vic.gov.au/images/content/pdf/privacy_papers/20180503-De-identification-report-OVIC-V1.pdf.

[7] See s 1(b) of the VDS Act.

[8] Under ss 24 and 29 of the VDS Act, respectively.

[9] Under s 18 of the VDS Act.

Key principles of the Data Sharing and Release Bill

In response to **Question 1** of the Issues Paper, OVIC notes that one of the overall aims of the DS&R Bill will be to 'safeguard data sharing and release in a consistent and appropriate way.'[10] OVIC suggests including an express provision to this effect within the DS&R Bill. A similar approach has been taken in Victoria, under s 1(d) of the VDS Act, which outlines the protections provided for under the VDS Act, including the purpose limitations, express circumstances in which the sharing of identifiable data is permitted and the offences for the unauthorised access, use or disclosure of data. Such a provision would signal that it is the intention for these reforms to promote the sharing of identifiable data in a secure and responsible way.

There may also be potential limitations in the proposed 'alternative authority' to share under the DS&R Bill. The Issues Paper outlines the intention for the DS&R Bill to introduce a new 'easier' alternative to share data, to operate alongside existing legislative authorisations for information sharing. In response to **Question 2** of the Issues Paper, OVIC notes that providing an alternative authority to share under this model may result in Commonwealth entities and Commonwealth companies failing to share information under the most appropriate authority, instead relying on the DS&R Bill because it allows for 'easier' sharing.

Further, OVIC notes that the alternative authority to share under the DS&R Bill needs to be drafted in such a way to give public sector decision-makers confidence that any other relevant legislative obligations have been displaced, to the extent appropriate to implement these reforms. The broad overriding of secrecy and confidentiality provisions should only be done in consultation with the parties responsible for administering the relevant legislation. While in some cases historical secrecy provisions may no longer be required, there will be others that exist for legitimate and necessary reasons.

Given that the threshold for easier sharing is unclear from the Issues Paper, as well as the associated privacy and data security risks associated with the potential public release of data, decision-makers may be less inclined to rely on the alternative authority in practice.

Role of the National Data Commissioner

In response to **Question 3** of the Issues Paper, OVIC queries how the scope of the DS&R Bill and the role of the National Data Commissioner (**NDC**) will interact with the existing privacy and security protections under the Privacy Act 1988 (**the Privacy Act**), administered by the Office of the Australian Information Commissioner (**OAIC**). Further, OVIC questions whether it is the intention that the OAIC will have an oversight role within the model or a more collaborative role in practice. From a Victorian perspective, OVIC plays an express oversight role over the VCDI and the interaction between the VDS Act and the PDP Act is clearly outlined under s 24 of the VDS Act. This is a model that DPMC may wish to consider, to enhance the accountability and governance of the scheme.

While OVIC appreciates that this relationship will presumably be further clarified under the DS&R Bill, we recommend ensuring that there is no ambiguity between the roles of the Australian Information Commissioner and NDC when drafting the DS&R Bill.

In terms of the proposed reporting function of the NDC, it is unclear to whom the NDC will be reporting when providing 'statistics or reports on the data system, and on progress in sharing and release of data through the DS&R Bill'.[11] In response to **Question 32**, OVIC sees the reporting function of the NDC as an essential mechanism to ensure transparency and accountability within the model. OVIC recommends ensuring it is clear within the DS&R Bill to whom the NDC will be reporting, the frequency of reporting requirements and the matters to be contained within the reports.

[10] On page 8 of the Issues Paper.
[11] On page 20 of the Issues Paper.

In terms of what the NDC should be reporting on, OVIC welcomes the suggestion that the NDC should report on cases of non-compliance with the DS&R Bill.[12] OVIC recommends that the NDC be required to provide, at a minimum:

- detailed statistics about the use of the model;
- information regarding individual uses of the model (if the model is used at an individual intervention level, for example, to administer or enforce compliance requirements);
- the number of data sharing agreements made under the DS&R Bill; and
- the purposes for which the model has been used (by reference to the purposes test under the DS&R Bill).

In relation to the role of the National Data Advisory Council (**the Council**), it is unclear whether the NDC will have an obligation to follow the advice of the Council under the DS&R Bill, or whether the role of the Council will be purely consultative. OVIC would suggest clarifying the advisory role of the Council within the DS&R Bill.

Data security considerations

In response to **Question 25** I recommend ensuring that the DS&R Bill provides for the necessary data security assurance mechanisms under the proposed data sharing agreements. I note that the proposed data sharing agreements will 'make clear the rights, responsibilities and safeguards for data sharing between the data custodian and the trusted user.'[13]

To that end, I recommend that the template data sharing agreements to be provided by the NDC account for appropriate privacy and data security safeguards required of both parties to the agreement, such as:

- providing the data custodian with the ability to review or audit the trusted user's adherence to the terms of the data sharing agreement;
- clearly defined accountabilities and responsibilities in relation to the handling of the data under the data sharing agreement (for instance, clarifying roles and responsibilities in the event of a data breach); and
- requirements for the trusted user to report regularly to the data custodian on the effectiveness of the agreed assurance mechanisms and any incidents that may compromise the privacy or security of the data under the agreement.

The data sharing agreements should operate to ensure that, in essence, interagency risks are identified and managed carefully. In practice, this will involve collaboration between data custodians and trusted users to manage the shared risks effectively, efficiently and economically. This should be supported by an appropriate governance structure to ensure clear accountability and oversight.

Further, it is unclear from the Issues Paper what role, if any, the NDC or the OAIC would have in reviewing or auditing any data sharing agreements established under the DS&R Bill. Given that it is unlikely that all data sharing agreements would be appropriate to be made publicly available, I recommend clarifying whether these data sharing agreements will be subject to independent oversight, as a means to ensure transparency. I note that if the NDC is to have a role in advising data custodians on the development of data sharing agreements, it may be inappropriate for the NDC to also have a review or audit function.

As a general observation, Page 15 of the Issues Paper discusses the compatibility of the Five-Safes Framework with Australian Privacy Principle 11 and the Protective Security Policy Framework (**PSPF**). The PSPF and associated controls scale up and down according to the value of the information, including unclassified information. Security risks may arise in a public release context, given the increased value of disparate data

[12] On page 20 of the Issues Paper.
[13] On page 16 of the Issues Paper.

sets being combined to form more sensitive data holdings, that will in turn require increased security controls. For instance, the potential linking of various unclassified data sets, deemed to be appropriate for public release, could mean the aggregated value is substantially higher.

Security measures are also critical in a public release context, to ensure that the original source of the information is protected. For example, if the website of a data custodian is the source of access to a data set deemed appropriate for public release, the security of the source website is critical, as users of the released data are relying on the integrity and availability of the data set.

I also note that Commonwealth entities already have requirements to apply the PSPF and the related Information Security Manual. The Issues Paper states that the safeguards legislated in the DS&R Bill would exist alongside current safeguards under various other requirements, including the PSPF.[14] I recommend that the DS&R Bill clarify entities' obligations under the proposed model in relation to data security, as there is potential for confusion with many co-existing standards in place.

Accredited Data Authorities

The Issues Paper notes that the NDC could develop the criteria and process for the accreditation of Accredited Data Authorities (**ADAs**) under the model.[15] In response to **Question 29**, I recommend that the accreditation of ADAs be subject to periodic review, to ensure that they are performing their duties in accordance with the DS&R Bill and accreditation criteria, as well as their obligations under relevant privacy law and the PSPF (where applicable). Further, the model should provide a mechanism for the suspension of ADAs that do not perform in accordance with the DS&R Bill and accreditation criteria. Given that the NDC will play a role in the accreditation of the ADAs, it would be inappropriate for the NDC to perform any review or audit functions with respect to the accreditation of ADAs. As such, I recommend that the periodic review of ADAs be conducted by an independent third party.

In response to **Question 30**, OVIC raises concerns regarding the proposed ability for ADAs to pay to become accredited. Instead, it would be desirable to see strict criteria around the accreditation of ADAs under the model.

I also suggest that the DS&R Bill clarify the relationship between data custodians and ADAs when ADAs are authorised to manage some or all of the steps in the data sharing or release process on behalf of the data custodian, as there is a lack of clarity around the allocation of risk and responsibility between the data custodian and ADAs in Section 5 of the Issues Paper.

Thank you for the opportunity to provide a submission to this Issues Paper. OVIC notes that further consultation will occur through a Privacy Impact Assessment (**PIA**) and Exposure Draft Bill processes. We would be pleased to review and provide comment on the PIA and Exposure Draft of the Bill and will watch with interest as these reforms progress.

I have no objection to this letter being published by DPMC without further reference to me. I also propose to publish a copy of this letter on the OVIC website but would be happy to adjust the timing of this to allow DPMC to collate and publish submissions proactively.

[14] On page 10 of the Issues Paper.
[15] On page 18 of the Issues Paper.

If you have any questions regarding the above, please contact Emily Arians, Senior Policy Analyst at emily.arians@ovic.vic.gov.au.

Yours sincerely

Sven Bluemmel
Information Commissioner