Office of the Victorian Information Commissioner

t 1300 006 842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D21/11464

18 June 2021

Mr Michael Coutts-Trotter
Secretary
NSW Department of Communities and Justice

By email only: policy@justice.nsw.gov.au

Dear Mr Coutts-Trotter

Exposure Draft of the Privacy and Personal Information Protection Amendment Bill 2021

Thank you for the opportunity to provide comment on the Exposure Draft of the *Privacy and Personal Information Protection Amendment Bill 2021* (**the Bill**) and related Factsheet (**the Factsheet**).

The Office of the Victorian Information Commissioner (**OVIC**) regulates privacy, freedom of information and information security in Victoria. My office administers both the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**) and the *Freedom of Information Act 1982* (Vic). One of my functions under the PDP Act is to make public statements on matters that affect individuals' personal privacy.

My office considers that the proposed introduction in New South Wales (**NSW**) of a Mandatory Notification of Data Breach (**MNDB**) scheme and mandating the creation of publicly accessible data breach policies under the Bill has the potential to improve privacy and data security outcomes in the state. It is also positive to see the Bill proposes to extend the application of the *Privacy and Personal Information Protection Act 1998*, including the MNDB scheme, to State-Owned Corporations (**SOCs**) not regulated under the *Privacy Act 1998* (Cth).

General comments

Meaning of 'serious harm'

1. Due to the circumstantial and varied nature of assessing the level of harm that has or will likely result from a data breach, OVIC supports the inclusion of factors for considering whether 'serious harm' has or would likely occur under section 59G of the Bill, in place of an explicit definition (consistent with the Commonwealth Notifiable Data Breaches (**the Commonwealth NDB scheme**)).

2. The Factsheet[1] notes that the NSW Information and Privacy Commission (**IPC**) will publish guidance and resources to assist NSW agencies assess whether serious harm has or will likely occur. Based on our experience in Victoria, OVIC strongly encourages this approach, as awareness within the NSW public sector as to what constitutes serious harm is a crucial element to the uptake and success of the MNDB scheme.

[1] Factsheet, Privacy and Personal Information Protection Amendment Bill 2021 (NSW).

Consistency with Commonwealth law

3. Legislative clarity is imperative for the successful implementation of the MNDB scheme. To that end, it is pleasing to see general consistency with legislative definitions, the threshold for notification, and response processes across the Commonwealth NDB scheme and the MNDB scheme. This will allow for easier interpretation in practice.

4. While consistency with the Commonwealth NDB scheme will aid implementation of the MNDB scheme (due to existing familiarity with terminology under the NDB scheme), OVIC sees the introduction of the MNDB scheme as an opportunity to optimise data breach reporting. To that end, it is pleasing to see that under the MNDB scheme, an agency must report a data breach to the NSW IPC even where the risk of serious harm has been mitigated by actions of the agency. This distinction from the Commonwealth NDB scheme incorporates best practice in privacy law.[2]

General clarity

5. OVIC suggests amending title of section 59G to 'Assessment of whether data breach would be likely to result in serious harm' for clarity around the purpose of the provision. This would also promote consistency with the Commonwealth NDB scheme.[3]

6. Experience suggests that guidance and resources that are accessible, drafted in plain English and include recent best-practice examples are most effective. To that end, OVIC recommends that guidance be issued on assessing data beaches include any best practice examples from other jurisdictions, such as the management and assessment of data breaches in jurisdictions subject to the Europeans Union's General Data Protection Regulation.

Operational matters

Resources and funding

7. Overall, OVIC views the MNDB scheme as a sophisticated way to manage data breaches involving personal or health information.

8. To be effective, the MNDB scheme needs to be appropriately resourced to allow the NSW IPC to fulfill its expanded functions under the Bill. New investigation and monitoring functions,[4] permitting the Privacy Commissioner to investigate, monitor, audit and report on the functions, policies and practices of NSW agencies will likely require additional resourcing to effectively carry out these assurance and monitoring activities.

9. In addition, to aid the successful implementation of the MNBD scheme, the NSW IPC will need to dedicate resourcing to communications and guidance, to raise initial awareness and understanding of the MNDB scheme once introduced.[5]

Transparency

10. It is pleasing to see the introduction of a requirement for NSW agencies to prepare and publish a data breach policy under section 59ZC of the Bill. OVIC suggests the processes for reporting suspected eligible data breaches to agency heads form part of an agency's publicly accessible data breach policy. This will aid government transparency and foster public trust in government.

[2] See, Articles 33 and 34 of the General Data Protection Regulation.
[3] *Privacy Act* 1998 (Cth) section 26WG.
[4] See, section 59Y of the Bill.
[5] For example, providing support and guidance to NSW agencies to devise streamlined processes for reporting data breaches to agency heads to fulfill their obligations under section 59D of the Bill.

Interaction with the Commonwealth MDB scheme

11. The Factsheet identified that there are limited circumstances where a data breach within an agency or SOC may be captured under both the Commonwealth NDB scheme and the MNDB scheme. An example is where the data breach involves tax file number (**TFN**) information.[6] OVIC notes that the NSW IPC will need to update existing guidance, such as the guidance relating to the obligations of NSW public sector agencies under the Commonwealth NDB scheme in relation to TFN information,[7] and guidance for reporting obligations under the MNDB scheme.

12. Given that the MNDB scheme will operate concurrently with the Commonwealth NDB scheme, the NSW IPC will need to provide clear guidance to individuals regarding which regulator (NSW IPC or the Office of the Australian Information Commissioner) they should approach to exercise their information rights. It may also wish to develop communication protocols with the OAIC for specifically this situation.

Exemptions

13. OVIC shares NSW's position that agencies should be exempt from notification requirements if the notification would create a serious risk of harm to an individual's health or safety. Agencies should be provided guidance and examples of such situations, to aid decision-making before notifying affected individuals.

Information security

14. While it is understandable the term 'cyber security' is not defined under the reforms, to allow for evolving interpretations in practice, it is currently unclear what cyber security framework(s) may apply to establish a collective understanding of what is considered a cyber incident. NSW agencies will require a baseline level of understanding of cyber security for relevant provisions under the Bill to be interpreted in practice.

15. Accordingly, any guidance issued by the Privacy Commissioner under section 59ZH in relation to exemptions for cyber security reasons should reflect current standards and frameworks for assessing and managing cyber security risks, such as OVIC's Victorian Protective Data Security Framework or the Commonwealth Protective Data Security Framework.

Thank you for the opportunity to comment on the Bill. I have no objection to this submission being published without further reference to me. I also propose to publish a copy of this submission on OVIC's website and would be happy to adjust the timing of this to allow you to collate and publish submissions proactively.

If you would like to discuss this submission, please do not hesitate to contact me or my colleague [redacted], at [redacted].

Yours sincerely

[redacted]

[6] *Privacy Act* 1998 (Cth) section 5.
[7] See, https://www.ipc.nsw.gov.au/fact-sheet-nsw-public-sector-agencies-and-notifiable-data-breaches.