information and privacy commission
new south wales

Enquiries: [redacted]
Telephone: [redacted]
Our reference: 20/861/DJ

25 June 2021

NSW Privacy Laws - Project Team
Courts, Access to Justice and Regulatory
Policy, Reform and Legislation
NSW Department of Communities and Justice
GPO Box 31
Sydney NSW 2001

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

Dear Sir/Madam

PROPOSED CHANGES TO NSW PRIVACY LAWS: MANDATORY NOTIFICATION OF DATA BREACH SCHEME AND OTHER PRIVACY REFORM

The Information and Privacy Commission (IPC) welcomes the opportunity to provide a submission to the Department of Communities and Justice (DCJ) on the exposure draft of the *Privacy and Personal Information Protection Amendment Bill 2021* (the draft Bill) which would introduce a mandatory notification of data breach (MNDB) scheme in NSW and other important privacy reforms.

The Privacy Commissioner supports the establishment of a MNDB scheme for NSW and expects that establishing the scheme will:

- increase public trust in how government handles personal information and responds to data breach incidents
- increase agency awareness of and responses to data breach incidents
- improve transparency and accountability of agencies in the way they respond to serious data breaches
- encourage agencies to elevate capability to mitigate and manage the risk of data breaches, and
- provide members of the public with the information they need to reduce their risk of harm following a serious data breach.

Scheme design

The design of the model for the MNDB scheme has been developed by a working group comprising representatives from DCJ, the Department of Customer Service, NSW Ministry of Health and the IPC.

The MNDB scheme will complement the information protection principles (IPPs) in the *Privacy and Personal Information Protection Act 1998* (PPIP Act) and the health privacy principles (HPPs) in the *Health Records and Information Privacy Act 2002* (HRIP Act) that currently apply to NSW agencies that hold personal and health information. The notifications to the Privacy Commissioner and affected individuals under the MNDB scheme will operate in addition to any investigation of conduct that might contravene an IPP or HPP.

In designing the scheme, the working group was informed by the Commonwealth's Notifiable Data Breach (NDB) scheme in the *Privacy Act 1988* (Cth) (Privacy Act) which requires certain organisations and agencies to report eligible data breaches to the Office of the Australian Information Commissioner (OAIC). Some NSW public sector agencies are captured by the Commonwealth NDB scheme; for example, state and local government bodies that are tax file number (TFN) recipients are covered by the Commonwealth scheme if TFN information is involved in a data breach. Adopting a harmonious approach will make it easier for NSW agencies to comply with the MNDB scheme. In recognition of this interplay, the threshold for notification to the IPC, features of the draft legislation and operational considerations are highlighted below.

Threshold for notification to the IPC

Careful consideration has been given to the threshold for an eligible data breach that would require notification to the Privacy Commissioner and to persons affected by a data breach. Under the proposed MNDB scheme, an eligible data breach occurs if there is unauthorised access, disclosure or loss of personal information and a reasonable person would conclude that this breach would be likely to result in serious harm to an affected individual.

This threshold for notification is consistent with the Australian legislative framework. It is well understood by NSW agencies that also share information with the Commonwealth. A consistent approach will assist agencies in complying with their statutory obligations and promote streamlined processes.

The Privacy Commissioner supports the proposed threshold for notification for the MNDB scheme. It is important that notification occurs where a data breach is likely to result in serious harm for an individual but not otherwise. The threshold needs to ensure that members of the public are effectively protected without leading to 'notification fatigue' in individuals which may be counterproductive in the longer term. It should be set at a level that is manageable in terms of resourcing for agencies and the regulator.

In the European Union, notification of personal data breaches is provided for in Article 33 of the *General Data Protection Regulation*. Notification is required unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. In practical terms, the threshold proposed for the MNDB scheme is similar to the EU threshold, in that agencies must alert members of the public of a serious data breach that may affect them.

Assessment of data breaches

Under the proposed scheme the Privacy Commissioner will be required to issue guidelines to assist agencies in complying with the scheme. One set of guidelines will address the factors an agency may consider when assessing a data breach and deciding whether it is likely to result in serious harm. A non-exhaustive list of the factors for consideration is included in proposed section 59G of the draft Bill. The IPC's guidance will build on these factors and will address considerations relating to:

- the type, sensitivity and amount of the personal information involved in the breach
- the data context, including whether the personal information is protected by security measures
- the circumstances of the breach, for example, whether it was caused by human error or by a malicious actor, and
- the nature of the harm that has or may occur as a result of the breach.

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 ● GPO Box 7011, Sydney NSW 2001
T 1800 IPC NSW (1800 472 679) ● **E** ipcinfo@ipc.nsw.gov.au ● **W** www.ipc.nsw.gov.au

Depending on the circumstances of the data breach, serious harm to an individual may include serious physical, psychological, emotional, financial or reputational harm. The IPC guidance will assist agencies in identifying the types of harm that may result from different kinds of data breaches, allowing for a response that is context specific for each agency.

Timeframe for assessment of data breaches

Under the proposed MNDB scheme, the initial assessment of the data breach is to occur within 30 days of the agency first holding a reasonable suspicion that a breach has occurred, unless the head of the agency is satisfied the assessment cannot reasonably be conducted within this timeframe, and gives written notice to the Privacy Commissioner of an extension of time. By requiring an agency head to make this assessment, the MNDB scheme ensures that agencies and agency heads take responsibility for managing the risk of potential data breaches and for detecting and responding to breaches when they occur. This feature will promote compliance through accountability and responsibility for the cultural change that is required to support the introduction of the scheme.

In supporting an initial assessment period of 30 days, the Privacy Commissioner acknowledges the need to notify affected individuals expeditiously so that they can take precautionary action but also recognises the practicalities that agencies experience in responding to increasingly complex cybersecurity threats. It allows sufficient time for agencies to assess the impact of the data breach and provide accurate information about the breach to the Privacy Commissioner, including the number of individuals likely to have been affected and the remedial action that the agency will implement to mitigate further risk to individuals. Within this context, the Privacy Commissioner expects agencies to carry out their assessment as expeditiously as possible, given the imperative to inform and support individuals whose personal information may have been breached.

Notification of data breaches

If an agency decides that an eligible data breach has occurred, the proposed MNDB scheme would require notification to occur:

- to the Privacy Commissioner immediately, in an approved form to be developed by the Privacy Commissioner and published on the IPC website
- to each affected individual as soon as practicable, or if that is not reasonably practicable, by public notification that is publicised and included on the agency's website for at least 12 months, and
- to the Privacy Commissioner following individual or public notification, of any information that was not given as part of the immediate notification.

These notification requirements allow the Privacy Commissioner to exercise oversight of the data breach response, from initial notification through to additional learnings that arise in notifying members of the public.

Exemptions to notification obligations

There is a clear public interest in agencies notifying the Privacy Commissioner of a data breach that is likely to result in serious harm, including where an agency has taken remedial action to mitigate the harm, or where another exemption applies. In this way the Privacy Commissioner will be able to provide a more comprehensive report to government and Parliament on the data breaches experienced across the NSW public sector. The exposure draft of the Bill contains six exemptions where an agency is not required to notify an affected individual but is required to notify the Privacy Commissioner:

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 ● GPO Box 7011, Sydney NSW 2001
T 1800 IPC NSW (1800 472 679) ● **E** ipcinfo@ipc.nsw.gov.au ● **W** www.ipc.nsw.gov.au

- *Multiple agencies*: if a breach affects multiple agencies, an agency is exempt from compliance if another agency provides the notifications required under the MNDB scheme

- *Prejudice an investigation or proceedings*: if notification would prejudice an investigation that could lead to prosecution of an offence, or prejudice court or tribunal proceedings

- *Mitigation of harm*: if an agency has taken action to mitigate the harm done by the breach and as a result there is not likely to be a risk of serious harm to an individual

- *Secrecy provision*: if notification is inconsistent with a secrecy provision

- *Health and safety*: if notification would create a serious risk of harm to an individual's health or safety, and

- *Cybersecurity*: if notification would worsen the agency's cybersecurity or lead to further data breaches

The IPC will be developing guidelines to assist agencies in applying these exemptions.

The mitigation of harm exemption encourages an agency to take remedial action at an early stage to contain the breach, and to prevent or reduce the harm that an affected individual may otherwise experience. Its inclusion is consistent with the intent of the scheme to alert members of the public to breaches that are likely result in serious harm.

The health and safety exemption will only apply if the harm in notifying an individual of the breach is greater than the harm of not notifying, and where the decision is made on information that is current and known to the agency, without conducting searches. The exemption may be permanent or temporary. The Privacy Commissioner must be notified of an agency's reliance on the exemption and whether it will be permanent or temporary.

In including the health and safety exemption, the working group took into account that it is state agencies that are primarily responsible for health care in NSW, and this exemption may be necessary in some clinical settings. The Privacy Commissioner notes the risk assessment that is built into this exemption, that requires consideration of the harm of not notifying, and this assessment will be particularly applicable where identity information is compromised. It is important that members of the public are provided with the information they need to take steps to protect themselves and reduce their risk of harm that may result from a data breach.

The cybersecurity exemption was included in consultation with Cyber Security NSW and applies only if notification would worsen the agency's cybersecurity or lead to further data breaches. This exemption may be relevant if a data breach is caused by a malicious actor. An agency must follow guidelines, to be prepared by the Privacy Commissioner, in making a decision about an exemption under this section.

Powers of the Privacy Commissioner

The Privacy Commissioner will have powers under the MNDB scheme to make directions and recommendations, to investigate, monitor, audit and report on the exercise of agency functions, and may enter and inspect agency premises for this purpose. The Privacy Commissioner will also have the power to make a written report and recommendations.

The exercise of these powers by the Privacy Commissioner as regulator will support agency compliance and promote public trust in the handling of personal information by government.

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 ● GPO Box 7011, Sydney NSW 2001
T 1800 IPC NSW (1800 472 679) ● **E** ipcinfo@ipc.nsw.gov.au ● **W** www.ipc.nsw.gov.au

Publication of statistical information

In implementing the MNDB scheme, the Privacy Commissioner intends to publish statistical information about its operation. Making statistical information publicly available is important for government transparency and for building public trust in the scheme. The Privacy Commissioner currently publishes quarterly statistics in relation to the operation of the voluntary data breach notification scheme.

As currently drafted, proposed section 59ZF requires information given to the Privacy Commissioner to be kept confidential and only released in limited circumstances. The Privacy Commissioner requests that consideration be given to clarifying the effect of the confidentiality provision to confirm that statistical information may be published periodically.

Resource impacts on the IPC

To successfully implement the MNDB scheme, the Information Commissioner as CEO of the IPC provided input into the development of the proposal from an operational perspective. This input was informed by the operation of both the voluntary scheme and schemes operating elsewhere. Within the IPC context the introduction of a MNDB scheme must be associated with additional funding as confirmed by the May 2021 independent review of IPC efficiency and effectiveness.

Previous advice is confirmed regarding the requirements for:

- Initial funding to develop the IPC guidelines and approved forms that will underpin the scheme
- The requirement for capital funding to acquire and implement appropriate technology to capture data and effectively report on the operation of the scheme
- Ongoing operational funding to carry out scheme functions including review of notifications, auditing and reporting functions, as well as an anticipated increase in the Privacy Commissioner's complaints jurisdiction arising from agency handling of data breach incidents.

A business case to support the implementation of the MNDB scheme was provided in September 2020. The scheme as currently designed reflects a significant reliance upon guidelines developed and issued by the Privacy Commissioner. That reliance upon regulatory guidance was not canvassed within the IPC business case to the degree now envisaged. The funding provided to the IPC should reflect its role as the expert regulator responsible for the development of the guidance.

In light of the dependence of the MNDB scheme upon Privacy Commissioner guidelines, the need for operational changes within agencies and the promotion of the scheme to the public, the proposal to commence 12 months after assent is supported.

State owned corporations

The draft Bill would also amend the definition of public sector agency in the PPIP Act to include State owned corporations (SOCs) that are not covered by the Commonwealth's Privacy Act.

The IPC welcomes the inclusion of these SOCs in the PPIP Act and recognises the need for the preparation period of 12 months for SOCs to put in place processes to support compliance with their privacy obligations. The IPC has a range of resources available to assist SOCs to meet their compliance obligations under the PPIP Act.

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 ● GPO Box 7011, Sydney NSW 2001
T 1800 IPC NSW (1800 472 679) ● **E** ipcinfo@ipc.nsw.gov.au ● **W** www.ipc.nsw.gov.au

Contracted service providers

In its current form, the proposed MNDB scheme would not apply to contracted service providers who hold information as a result of a NSW public sector partnership or contract. The Privacy Commissioner notes the potential complexity in extending the MNDB scheme to cover contracted service providers but would consider supporting this extension once consideration has been given to how this might be achieved and following consultation with the OAIC.

Proposed amendment to the *Government Information (Public Access) Act 2009* (GIPA Act)

The Information Commissioner suggests reconsideration of the extension of Schedule 2 "Excluded information of particular agencies" of the GIPA Act in circumstances where audit reports produced by the IPC currently serve an educational regulatory purpose. Any extension of the categories of excluded information under the GIPA Act curtails the public's right to access information and the presumption in favour of disclosure and would require a robust articulation of public benefit. Further consultation regarding this aspect of the legislative proposal is welcome.

We hope these comments will be of assistance. Please do not hesitate to contact us if you have any queries. Alternatively, your officers may contact [redacted], Director, Legal Counsel and Regulatory Advice on [redacted] or by email at [redacted].

Yours sincerely

[redacted]

CEO, Information and Privacy Commission NSW
Information Commissioner
NSW Open Data Advocate

[redacted]

Privacy Commissioner

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 IPC NSW (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au