Privacy and Personal Information Protection Amendment Bill 2021

Factsheet

The *Privacy and Personal Information Protection Act 1998* regulates how New South Wales public sector agencies manage personal information and the functions of the NSW Privacy Commissioner.

The Privacy and Personal Information Protection Amendment Bill 2021 proposes the creation of a mandatory notification of data breach scheme, and would extend the Act to include NSW State-Owned Corporations that are not already regulated by the *Privacy Act 1988* (Cth).

Overview of the proposed reforms

The *Privacy and Personal Information Protection Amendment Bill 2021* (PPIP Amendment Bill) proposes to strengthen the protection of Privacy in NSW through the following reforms:

- Creating a Mandatory Notification of Data Breach Scheme (**MNDB scheme**) to require public sector agencies bound by the *Privacy and Personal Information Protection Act 1998* (**PPIP Act**) to notify the Privacy Commissioner and affected individuals of data breaches of personal or health information likely to result in serious harm,
- Applying the PPIP Act to all NSW State-Owned Corporations (**SOCs**) that are not regulated by the Commonwealth *Privacy Act 1988* (**Privacy Act**), and
- Repealing s117C of the *Fines Act 1996*, to ensure that all NSW public sector agencies are regulated by the same mandatory notification scheme.

Background

In July 2019, the Department of Communities and Justice (DCJ) released a discussion paper '[Mandatory Notification of data breaches by NSW Public Sector Agencies]' seeking community views about how government agencies should respond to data breaches. DCJ received 23 submissions, including from six Government agencies, six members of the public, three local councils, two universities or educational facilities and various advocacy groups and professional associations.

The submissions indicated overwhelming support for the introduction of a mandatory notification of data breach scheme. That view is shared by the NSW Government and the NSW Privacy Commissioner.

This exposure bill has been developed by the Department of Communities and Justice and the Department of Customer Service, in close consultation with the Information and Privacy Commission (**IPC**) and the Ministry of Health.

Proposed Model for MNDB scheme

Overview: What will the MNDB scheme do?

The MNDB scheme will require public sector agencies to notify the Privacy Commissioner and affected individuals if a data breach affecting personal or health information that is likely to result in serious harm occurs.

The MNDB scheme will require agencies to satisfy other data management requirements, including to maintain an internal data breach incident register, and have a publicly accessible data breach policy.

Under the PPIP Act, the Privacy Commissioner already has regulatory powers and functions, which can be used in relation to the MNDB scheme. The MNDB scheme will also confer on the Privacy Commissioner additional regulatory powers in relation to the MNDB scheme, including the power of entry.

Why is the MNDB scheme being proposed?

Depending on the size and nature of a data breach, the consequences for individuals can be significant. These consequences can include financial fraud, identity theft and even violence.

Data breaches can also have serious consequences for government agencies. A breach may create commercial risk through the disclosure of commercially sensitive information, or otherwise impact an agency's reputation, finances, interests or operations. Ultimately, data breaches can lead to a loss of trust and confidence in an agency and the services it provides.

A mandatory scheme is being proposed to improve agency data management, reduce underreporting and reduce the occurrence of data breaches that cause serious harm. Mandatory schemes enable individuals to take action to protect themselves in the event of breaches, and can increase public trust in government.

Mandatory notification schemes are considered best practice, and many models have been introduced in other jurisdictions, including the Commonwealth,[1] New Zealand,[2] the European Union[3] and Canada.[4]

When will the MNDB scheme commence?

Following public consultation, it is anticipated that a bill will be introduced in the NSW Parliament in 2021. If passed, the MNDB scheme will commence 12 months following the passage of legislation. This will allow enough time for NSW public sector agencies and the IPC to put in place a range of mechanisms to ensure compliance.

How would the MNDB scheme improve privacy protections in NSW?

It is expected that the MNDB scheme will improve privacy protections in the following ways:

- provide certainty for the public and government agencies regarding rights and obligations around the handling of personal information and the actions that should be taken if a data breach occurs,
- increase agency capability to properly respond to data breaches that are likely to result in serious harm,
- provide individuals with information needed to reduce their risk of harm following a serious data breach,
- encourage agencies to improve their policies and practices to better prevent, mitigate and manage the risk of data breaches, and
- increase public trust in government and agency handling of personal information and data breach incidents.

Who would the MNDB scheme apply to?

The MNDB scheme would apply to all 'public sector agencies' as defined by the PPIP Act. This includes all NSW agencies and departments, statutory authorities, local councils, bodies whose accounts are subject to the Auditor General and some universities.

If the proposal to extend the application of the PPIP Act to SOCs is enacted, then the MNDB scheme would also apply to SOCs.

Which breaches would the MNDB scheme apply to?

The MNDB scheme would capture data breaches of personal information or health information that are likely to result in serious harm.

---

[1] Part IIIC of the *Privacy Act 1988 (Cth)* commenced on 22 February 2018.
[2] Part 6 of the *Privacy Act 2020* commenced on 1 December 2020.
[3] The European Union General Data Protection Regulation 2016/679 commenced on 25 May 2018.
[4] Division 1.1 of the *Personal Information Protection and Electronic Documents Act 2000* and related Regulations commenced on 1 November 2018.

What is serious harm?

Serious harm can include financial, psychological, physical and reputational harm.

What constitutes serious harm will depend on the circumstances of each breach. The legislation will prescribe a number of factors to consider when assessing whether an eligible breach is likely to cause serious harm. This ensures both flexibility to suit a variety of breaches, and consistency in that important factors will necessarily be considered during assessment.

It is intended that the judicial and academic consideration of the Commonwealth Notifiable Data Breaches scheme (**NDB scheme**) threshold will also be used.

The IPC will also publish guidance and resources to assist NSW public sector agencies in making this assessment.

What is a breach?

A data breach can include unauthorised access, disclosure and loss of information (where the loss is likely to result in unauthorised access or disclosure). The breaches can occur between agencies, within an agency and external to an agency.

What is personal information?

'Personal information' is defined in s4 of the PPIP Act as information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. Personal information can include photos, contact details, fingerprints, body samples and genetic characteristics.

What is health information?

'Health information' is defined in s6 of the *Health Records and Information Privacy Act 2002* (HRIP Act) and includes personal information about an individual's physical or mental health, disability, and information connected to the provision of a health service.

Why would the MNDB scheme regulate health information, when information regulated by the HRIP Act is otherwise expressly excluded from PPIP Act?

If the bill is enacted, health information as defined by the HRIP Act will remain excluded from the PPIP Act generally, except in relation to the MNDB scheme.

As there is no mandatory reporting scheme for breaches involving health information under the HRIP Act, it is important that these breaches are captured by the MNDB scheme. Otherwise, there would be no obligation for NSW public sector agencies to report data breaches involving health information, which is a particularly sensitive subset of personal information.

Notably, the Commonwealth Privacy Act regulates the management of both personal and health information held by Commonwealth public sector agencies, and many private entities, including those with a turnover of greater than $3 million.

What obligations will an agency have under the MNDB scheme?

The proposed MNDB scheme requires an agency to contain and assess a suspected data breach to determine whether it is an eligible breach under the MNDB scheme, and, if so, to notify the Privacy Commissioner and any affected individuals.

The MNDB scheme specifies several timeframes – the timeframes in which an agency must assess a data breach, notify the Privacy Commissioner, and notify affected individual(s) of the breach.

In nominating these timeframes, a range of factors have been considered, including:

- the need to expeditiously notify individuals so that they can take precautionary action
- the average time in which a malicious breach can lead to misuse of information
- the need to create a workable scheme, including creating timeframes that agencies can comply with, and
- the need to ensure that the Privacy Commissioner has oversight where agencies cannot comply expeditiously with the timeframes (particularly when notifying individuals).

Agencies will also have other information handling requirements, including maintenance of an internal data breach incident register and creation of a publicly accessible data breach policy.

Assessment of Breach

When an agency reasonably suspects that a data breach has occurred, it will be required to immediately

- attempt to contain the breach, and
- assess whether it meets the threshold for notifying the Privacy Commissioner and affected individuals. This assessment must be completed within 30 days from the date the agency first held the reasonable suspicion about the data breach, unless the head of the agency, or their delegate, approves an extension and notifies the Privacy Commissioner.

Notification of Breach

In most instances, the MNDB scheme will require the agency to notify both the Privacy Commissioner and the affected individuals.

Notification to the Privacy Commissioner

Once an agency knows, or has reasonable grounds to believe, that an eligible breach has occurred, the agency must immediately notify the eligible breach to the Privacy Commissioner, with as many details as possible. A subsequent notification to the Privacy Commissioner with further detail may be required.

Notification to the affected individual(s)

The agency must also notify the affected individual(s) as soon as practicable after an agency knows or has reasonable grounds to believe that an eligible breach has occurred. There are three options for notifying individuals:

1. notify all individuals to whom the information relates,
2. notify only those individuals at risk of serious harm, or
3. publish a notification on the agency's website (if any) and take reasonable steps to publicise it.

The MNDB scheme will permit limited information sharing between agencies for the purpose of notifying affected individual(s) of an eligible data breach. This will include contact details and dates of birth and death of the affected individual(s), so that an agency can verify that they have the correct contact details, and can confirm that the individual is not deceased.

What information will be included in the notifications to individuals and the Privacy Commissioner?

Under the proposed MNDB scheme, notifications to individuals will generally include:

- a description of the breach, including when the breach occurred, how it occurred, what data was affected, how long the data was affected, and what type of breach, e.g. loss, disclosure or unauthorised access, and
- what the agency is doing (or has already done) to control or reduce the harm
- recommendations to affected individuals about the steps they should take to minimise the impact of the breach, as well as their right to seek an internal review, and
- the identity and contact details of the agency (or agencies if more than one).

In addition to the above information, notifications to the Privacy Commissioner will include, where practicable:

- whether the data breach is limited to the one agency or more than one agency, and whether the agency is reporting on behalf of multiple affected agencies (including the details of the other affected agencies)
- whether it was a cyber incident
- the estimated cost of the breach to the agency,
- the total number, or estimated total number, of individuals affected or likely to be affected by the breach, and whether they have been notified, and
- whether affected individuals have already been advised of their right to seek internal review.

Are there any exceptions to the MNDB scheme requirements under the proposed scheme?

Exceptions to the requirement to notify individuals may apply in circumstances where:

- notification would prejudice law enforcement activities
- the exception would prevent or reduce a serious risk to an individual's health or safety

- the notification is likely to result in more breaches or deteriorate the agency's cyber security and
- the agency has remedied the harm of the breach successfully, e.g. an email was sent to the incorrect recipient, but was recalled successfully and deleted prior to the recipient opening the email.

Exceptions to the requirement to notify the Privacy Commissioner and affected individuals may apply where:

- one agency reports the data breach that affects multiple agencies (i.e. the other affected agencies do not also need to notify)
- notification would contravene a secrecy provision contained in other legislation.

How would the MNDB scheme relate to the IPC's existing voluntary data breach reporting policy?

Currently, the IPC's voluntary data breach reporting policy (voluntary scheme) encourages public sector agencies to voluntarily report data breaches to the Privacy Commissioner. The voluntary scheme will be replaced by the MNDB scheme. This approach will focus the IPC's resources on breaches that are most likely to cause serious harm to affected individuals, as opposed to facilitating notification of all breaches.

Will agencies still be able to request advice and assistance from the Privacy Commissioner with respect to other, non-eligible data breaches?

Yes. Nothing in the bill prevents agencies from requesting advice and assistance from the Privacy Commissioner in relation to data breaches generally.

Is the proposed MNDB scheme the same as the Commonwealth Notifiable Data Breaches scheme?

The Commonwealth NDB scheme commenced in February 2018, and requires organisations governed by the Commonwealth *Privacy Act*, to assess and notify the Office of the Australian Information Commission (OAIC) and affected individuals of data breaches likely to result in serious harm.

The proposed NSW MNDB scheme shares the same notification threshold as the NDB scheme, but differs in application and enforcement. The two schemes also apply to different entities and data holdings; the NDB scheme primarily regulates Australian Government agencies and private entities with an annual turnover of more than $3 million, and other organisations including health services providers and credit reporting bodies, while the MNDB scheme will only apply to NSW public sector entities regulated by the PPIP Act.

Why is the proposed MNDB scheme so similar to the NDB scheme?

The development of the MNDB scheme was informed by the experiences of the NDB scheme, which has now been in operation for over two years. New South Wales frequently shares information with the Commonwealth and would benefit from similar data breach notification schemes.

In some limited instances, breaches may be captured by both schemes. Breaches of tax file numbers are reportable under the NDB scheme. They may also be notifiable under the MNDB scheme if the breach occurred within a NSW public sector agency and was likely to result in serious harm. Importantly, data breaches affect agencies broadly; a breach that compromises tax file numbers will often compromise other personal and health information. The MNDB scheme has been designed to adopt, as far as possible, key features of the NDB scheme to limit the impact of this overlap.

What is the Privacy Commissioner's role in the proposed MNDB scheme?

The Privacy Commissioner's role in the MNDB scheme is to:

- receive notifications of eligible data breaches
- encourage and support scheme compliance through advice and education
- investigate and enforce compliance as necessary
- report to the public and Government, and
- make recommendations to Government about the operation of the MNDB scheme.

What enforcement powers will the Privacy Commissioner have regarding the MNDB scheme?

The Privacy Commissioner has existing powers which are proposed to extend to the MNDB scheme, including to:

- investigate agency systems, policies, practices, which:
    - may include investigating compliance with legislative requirements of MNDB scheme and adequacy of data handling systems, policies and practices, and
    - allow the Privacy Commissioner to require documents or information regarding the agency's compliance with the MNDB scheme.
    - make recommendations to agencies to remedy, elevate and improve compliance and practice with privacy legislation.

The proposed MNDB scheme would grant the Privacy Commissioner new powers regarding the MNDB scheme, including to:

- enter premises and inspect anything that may relate to compliance with the MNDB scheme
    - this will enable examination of the physical space, processes and systems, and will only be used after providing notice in writing, and in the unlikely event that an agency unreasonably refuses a premises inspection
- conduct audits in relation to the MNDB scheme, and
- furnish a report to the head of agency and responsible minister.

As with current practice, the Privacy Commissioner will exercise the regulatory powers in an escalating model of engagement with agencies, as appropriate in each circumstance.

Will the proposed MNDB scheme be monitored?

If enacted, the Privacy Commissioner will monitor agency compliance with the MNDB scheme. The Privacy Commissioner will furnish annual statistical reports on a range of matters, including notification statistics, compliance with assessment and notification timeframes and use of exceptions.

Why does the bill propose the repeal of s117C of the *Fines Act 1996*?

Section 117C of the Fines Act currently requires Revenue NSW to notify unlawful disclosures of personal information to individuals and the Privacy Commissioner in a manner that will be inconsistent with the MNDB scheme.

As a public sector agency, Revenue NSW would be subject to the MNDB scheme on its commencement. In order to ensure the whole public sector is regulated by the same scheme, it is proposed that s117C will be repealed upon commencement of the MNDB scheme.

Extension of the PPIP Act to State Owned Corporations

Currently, SOCs are expressly excluded from the definition of 'public sector agency' in s3(1) of the PPIP Act, meaning they are not required to comply with NSW privacy laws. SOCs are also excluded from the Commonwealth Privacy Act, unless the NSW Government requests that the SOC be prescribed as an organisation to which the Privacy Act applies.

The bill proposes to apply the PPIP Act to all SOCs that are currently not regulated by the Commonwealth Privacy Act, that is, all SOCs except Essential Energy. For simplicity, it is not proposed to alter that arrangement.

There are eight SOCs in NSW. It is proposed that the PPIP Act will apply to the following:

- Transport Asset Holding Entity of NSW
- Forestry Corporation of NSW
- Hunter Water
- Port Authority of NSW
- Sydney Water
- Landcom
- Water NSW.

When is the PPIP Act and MNDB scheme proposed to be applied to SOCs?

If enacted, the bill will commence 12 months after passage through the Parliament. This will allow SOCs and the IPC enough time to prepare appropriate systems and processes to fulfil PPIP Act and MNDB scheme requirements.

For more information

Visit the website at
https://www.justice.nsw.gov.au/justicepolicy/Pages/lpclrd/lpclrd_consultation/proposed-changes-to-nsw-privacy-laws.aspx