Fact Sheet March 2023

# Mandatory Notification of Data Breach Scheme: Exemptions from notification requirements

The Mandatory Notification of Data Breach Scheme ('MNDB Scheme') was created by amendments to the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) and will commence on 28 November 2023.

The MNDB Scheme requires that NSW public sector agencies ('agencies') notify affected individuals and the Privacy Commissioner when there has been an 'eligible data breach'.

You can find more information about the MNDB Scheme here.

## When does an agency need to notify individuals about an eligible data breach?

When a data breach occurs, an agency must immediately make all reasonable efforts to contain the breach and try to reduce the likelihood that an individual will experience serious harm.

Agencies then have 30 days from the date they become aware of a possible data breach to assess whether that data breach is an eligible data breach. This assessment should be carried out as expeditiously as possible. Whilst making this assessment, all reasonable attempts must be made to mitigate any harm already done.

Once an agency decides there has been an eligible data breach, the agency must notify the affected individuals as soon as practicable about that breach, with limited exceptions.

## When would an agency not be required to notify an affected individual?

Part 6A, Division 4 of the PPIP Act provides a limited number of exemptions from the requirement to notify affected individuals of an eligible data breach. An agency will not be required to notify where any of the following exemptions apply.

### Breaches involving multiple agencies

The exemption under section 59S will apply where:

- the data breach involves more than one agency,
- each agency has undertaken an assessment of the breach,
- the head of each agency has made a data breach notification to the Privacy Commissioner, and
- the other agency involved in the breach has undertaken to notify affected individuals of the eligible data breach.

Agencies should work together during the assessment process to ensure all affected individuals are identified.

The notification provided to the affected individuals should identify all agencies involved in the breach. The notification should also identify a central contact for further enquiries.

This exemption would not apply where multiple entities were involved in the breach but only one entity was an agency. In this instance, the agency would need to comply with the notification requirements even if another entity (including an agency of the Commonwealth or another state or territory) was also required to notify affected individuals under Commonwealth or other law.

### Investigations and legal proceedings

The exemption under section 59T will apply where the agency reasonably believes notification would likely prejudice:

- an investigation that could lead to the prosecution of an offence
- proceedings before a court or tribunal
- another matter prescribed by regulations.

### Mitigation of harm

The exemption under section 59U will apply where the agency:

- takes action to mitigate the harm done by the breach, and

- the action is taken before the breach results in serious harm to an individual, and
- because of the action taken, a reasonable person would conclude that the breach would not be likely to result in serious harm to the individual.

The time period for when this exemption could apply is *after* the agency has determined that the breach is an eligible data breach but *before* the breach results in serious harm to the individual.

### Secrecy provisions

The exemption under section 59V will apply where compliance by the agency with the notification requirements would be inconsistent with a secrecy provision.

For the purposes of the MNDB Scheme, a secrecy provision means a provision of an Act or statutory rule that prohibits or regulates the use or disclosure of information.

### Serious risk of harm to health or safety

The exemption under section 59W will apply where the agency reasonably believes that notification would create a serious risk of harm to an individual's health or safety.

When considering whether to apply this exemption the agency must have regard to the Privacy Commissioner's Guideline on the exemption under section 59W.

When making a decision to apply this exemption the agency must:

- consider the extent to which the harm that may be caused by notifying the individual is greater than the harm of not notifying the individual about the breach, and
- consider the currency of the information relied on in assessing the serious risk of harm to the individual, and
- must not search data held by the agency that was not affected by the data breach during the assessment of risk unless the agency knows, or reasonably believes, there is information in the data that is relevant to whether the exemption applies.

This exemption can be applied permanently, temporarily or until a particular event has occurred. The type of exemption applied will depend on the nature and context of the breach and the unique characteristics and circumstances of the affected individual.

The agency must provide a written notice to the Privacy Commissioner where this exemption is relied upon. The notice must include the information specified under section 59W(5).

### Cyber security

The exemption under section 59X will apply where the agency reasonably believes that notification would:

- worsen the agency's cyber security, or
- lead to further data breaches.

When considering whether to apply this exemption the agency must have regard the Privacy Commissioner's Guideline on the exemption under section 59X.

This exemption can only be applied on a temporary basis for the duration of the risk to the agency's cyber security.

The agency must provide a written notice to the Privacy Commissioner where this exemption is relied upon. The notice must include the information specified under section 59X(3).

The agency must review the use of this exemption each month and provide an update to the Privacy Commissioner.

## Notification to the Privacy Commissioner

The exemptions set out in Division 4 of the PPIP Act **do not** affect an agency's obligation to make a notification to the Privacy Commissioner under section 59M.

### For more information

Contact the Information and Privacy Commission NSW (IPC):

**Freecall:** 1800 472 679
**Email:** ipcinfo@ipc.nsw.gov.au
**Website:** www.ipc.nsw.gov.au