information and privacy commission
new south wales

Statutory Guidelines

NSW Mandatory Notification of Data Breach Scheme

Guidelines on the exemption for compromised cyber security under section 59X

September 2023

Who is this information for?	NSW privacy practitioners seeking information about an exemption for compromised cyber security under section 59X
Why is this information important to them?	This Guideline is intended to provide agencies with guidance on the operation of the exemption under section 59X. This provision provides that the head of a public sector agency may decide to exempt the agency from notifying affected individuals if the head of the agency reasonably believes that notification would worsen the agency's cyber security or lead to further data breaches.

Contents

Guidelines on the exemption for compromised cyber security under section 59X

Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act), establishes the Mandatory Notification of Data Breach scheme. Under the scheme, all public sector agencies bound by the PPIP Act must notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information that are likely to result in serious harm unless an exemption applies.

The Privacy Commissioner is empowered under section 59ZI to make guidelines for the purpose of exercising the Commissioner's functions under Part 6A.

These Guidelines, made in accordance with that section of the PPIP Act, are intended to provide agencies with guidance on the operation of the exemption under section 59X. This provision provides that the head of a public sector agency may decide to exempt the agency from notifying affected individuals if the head of the agency reasonably believes that notification would worsen the agency's cyber security or lead to further data breaches.

These Guidelines supplement the provisions of the PPIP Act. Agencies must have regard to them in accordance with section 59I of the PPIP Act.

Sonia Minutillo

A/Privacy Commissioner

Information and Privacy Commission NSW

September 2023

1. Introduction

1.1 Background

Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIP Act**), establishes a scheme for the mandatory notification of data breaches by NSW public sector agencies.

Under the Mandatory Notification of Data Breach (**MNDB**) scheme all public sector agencies (**agencies**) bound by the PPIP Act must notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information ("personal information") likely to result in serious harm.[1]

The MNDB scheme requires agencies to have regard to any guidelines issued by the Commissioner when assessing a data breach.[2]

These *Guidelines on the Exemption for compromised cyber security under section 59X* (**Guidelines**) have been made under section 59ZI of the PPIP Act.

These guidelines are not legal advice. Agencies are encouraged to seek professional advice tailored to their own circumstances where required.

Examples are provided throughout the guidelines. These examples are not exhaustive and should be considered as illustrative only.

1.2 Other resources

These Guidelines are part of a suite of guidelines and resources the IPC has developed to help agencies ensure they have the required systems, processes and capability in place, and should be used in conjunction with the following additional materials which can be found on the IPC website:[3]

- Guide to Preparing a Data Breach Policy
- Guide to managing data breaches in accordance with the Privacy and Personal Information Protection Act 1998 (NSW)
- Guidelines on the assessment of data breaches under Part 6A of the PPIP Act
- Guidelines on the exemption for risk of serious harm to health or safety under section 59W

2. Exemption for compromised cyber security

2.1 Overview

When an eligible breach has occurred, the head of the agency or their delegate[4] must take all reasonably practicable steps to notify the individuals to whom the information relates or who may be affected by the breach (affected individuals).[5]

[1] Section 59B of the PPIP Act provides that, for the purpose of Part 6A, personal information includes health information within the meaning of the *Health Records and Information Privacy Act 2002*.

[2] *Privacy and Personal Information Protection Act 1998* s 59I

[3] https://www.ipc.nsw.gov.au/privacy/MNDB-scheme.

[4] Any reference in the Guidelines to the head of an agency also includes their delegate. Section 59ZJ provides that the head of an agency may delegate the exercise of a function under Part 6A to a person employed in or by the agency or a class of person prescribed by the regulations.

[5] *Privacy and Personal Information Protection Act 1998* s 59N

Under Section 59X, where the head of an agency reasonably believes that notification of an eligible data breach would worsen the agency's cyber security or lead to further data breaches, the head of the agency may decide to exempt the agency from the requirement to notify affected individuals or make a public notification for a period of time.

When applying this exemption, the head of the agency must:

- have regard to these guidelines,
- notify the Privacy Commissioner by written notice of the exemption period and the method the agency will use to review the exemption, and
- review the exemption each month and provide an update to the Privacy Commissioner.

An exemption under section 59X must be temporary and must be reviewed on a monthly basis. Agencies must notify the Privacy Commissioner of their use of the exemption and provide an update on each monthly review. The exemption only applies to the extent that the head of the agency reasonably believes that the notification would worsen the agency's cyber security or lead to further data breaches.

The policy intent of the MNDB scheme is to empower individuals, provide transparency, and build trust in agency management of personal information. In most cases, notification of individuals affected by an eligible data breach can be presumed to be beneficial, as it empowers those individuals to take steps to protect themselves. Exemptions to notification are intended to only apply in exceptional circumstances. The Privacy Commissioner expects that exemptions under this section will be tightly framed and exercised for a minimal period of time.

2.2 Key terms

2.2.1 'Cyber security'

The PPIP Act does not define the term cyber security. The NSW Cyber Security Policy defines cyber security as "Measures used to protect the confidentiality, integrity and availability of systems and information".[6]

When determining whether the s59X exemption applies the head of the agency must have a reasonable belief that notification would have a detrimental impact on the measures used by the agency to protect information that it holds.

2.2.2 "Data breach"

The Guidelines on the assessment of data breaches provides that "a data breach occurs when personal or health information held by an agency is subject to unauthorised access, unauthorised disclosure or is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure." [7]

When determining whether the s59X exemption applies the head of the agency must have a reasonable belief that notification would lead to further unauthorised access, unauthorised disclosure or loss of information.

2.3 Seeking advice from Cyber Security NSW

Agencies should seek advice from Cyber Security NSW before exercising this exemption. Cyber Security NSW can provide advice on topics including cyber security best practice, threat assessments, and incident response to support agencies in coming to a view on the likely cyber security impacts of notification as well as any remedial actions required to mitigate the risk to the agency's cyber security and enable notification of affected individuals to take place.

---

[6] NSW Cyber Security Policy

[7] Guidelines on the assessment of data breaches under Part 6A of the PPIP Act

Agencies can contact Cyber Security NSW by email at: info@cyber.nsw.gov.au.

Agencies may also wish to consider seeking assistance or advice concerning implementation of mitigation actions recommended by Cyber Security NSW. This may include seeking assistance from ID Support or a private sector cyber security firm.

2.4 'Reasonable Belief'

In order to exercise the exemption under section 59X, the head of the agency must 'reasonably believe' that notification to affected individuals would worsen the agency's cyber security or lead to further data breaches.

A 'reasonable belief' is a belief that results from the exercise of sound judgement. The head of the agency must be able to explain the basis on which their reasonable belief was formed, based on the information available to them. This means being able to articulate specifically how notification would lead to the agency's cyber security being worsened, or lead to further data breaches.

2.5 Extent to which an agency's cyber security must be affected

There is no specific threshold for the degree to which an agency's cyber security must be affected to trigger section 59X, however the effect must be non-trivial. A mere possibility that the agency's cyber security *may* be worsened, or that a further data breach *may* occur is insufficient.

Before exercising the exemption, the head of the agency should be satisfied that there is a real risk that notification would worsen the agency's cyber security or lead to a further data breach.

Circumstances where notification would worsen an agency's cyber security or lead to further data breaches may include:

- Where notification would invite further unauthorised access to (or unauthorised use and disclosure of) affected personal information. For example, if personal information is accidentally published in an obscure online location and has not yet been taken down (and/or the information persists in search engine caches or web archives), notification may direct people to the location(s) resulting in further unauthorised access.
- Where the method used to cause the breach could be replicated by an interested party. For example, if a cyber attacker exploited a particular software vulnerability or used particular methods to exfiltrate data from the agency's network without being detected, and these gaps have not yet been remediated, notification including these details may both worsen the agency's cyber security posture and lead to further breaches by other attackers replicating those methods.

The impact on another agency of making a notification to affected individuals is not a relevant factor to consider when making a decision to exercise the exemption under s59X.

2.6 When agencies should choose not to rely on the exemption

Exercise of the exemption is at the discretion of the head of the agency, even when the criteria under section 59X have been met. In deciding whether to exercise their discretion, agency heads should consider whether it is in the public interest to do so. For example, where the impact on an agency's cyber security is limited, but the anticipated risk or impact of delaying notification to affected individuals is significant, it may be appropriate for the head of an agency to choose to notify, notwithstanding that the exemption may be available.

As delay in making notifications can have significant impacts for affected individuals, agencies should consider whether it is possible to make a notification, even where the criteria to exercise the exemption has been met. The key information in a notification that is likely to result in risk to an agency's cyber security is information about:

- how the breach occurred

- actions that have been taken or are planned to ensure the personal information is secure, or to control or mitigate the harm done to the individual.

Agencies should consider whether information can be provided in a way that will not increase risk to the agency. For example, a notification could include a high-level statement that the breach occurred due to a cyber-attack on agency systems but without providing detailed information on the methods used or vulnerabilities within a specified system. If an agency takes this approach, it may be appropriate to advise affected individuals that further information will be provided as investigation and remedial action is undertaken by the agency.

2.7 Resolving weaknesses giving rise to the exemption

Section 59X permits agencies to delay notification of an eligible data breach to individuals, but not to withhold notification permanently. Agencies are expected to respond quickly to mitigate any weaknesses in their cyber security arrangements and therefore reduce the risks which have led to a decision to apply the exemption under s59X. If disclosure of the types of information required by section 59O presents a cyber security risk,[8] agencies should take prompt action to mitigate that risk and enable disclosure.

2.8 Documenting decision-making

Agencies should keep appropriate records of any assessment and decision-making process leading to reliance on an exemption, including accurate records of information and evidence used to support their decision.

2.9 Notifying the Commissioner

When relying upon this exemption the head of the agency must, by written notice, notify the Privacy Commissioner of the following:

- The fact that the exemption is relied on,
- When the exemption is expected to end, and
- The process that will be used to review this exemption.

The Privacy Commissioner also expects agency heads to provide, if practicable, the following information with any notice of reliance on the exemption:

- The number of people to whom the exemption is applied.
- An explanation of why notification is believed to worsen the agency's cyber security or lead to further breaches.
- Confirm whether the agency has consulted with Cyber Security NSW in relation to the decision to exercise the exemption.
- An explanation of the works planned and timelines to remedy the cyber security issue to enable notification.

2.10 Review

An agency that has applied the exemption under s59X, must review the exemption monthly.

The review should consider:

- Whether the risks identified during the initial assessment remain valid.

[8] Section 59O sets out the information that must be notified to affected individuals after an eligible data breach. It requires agencies to provide a high-level description of the data breach, how it occurred and the information involved, but does not require detailed technical information about cyber security arrangements and how they may be circumvented to be disclosed.

- Whether mitigation actions taken by the agency have reduced the risks identified in the initial assessment.
- Whether there remain reasonable grounds to believe that notification to affected individuals would worsen the agency's cyber security or lead to further data breaches.
- Whether mitigation activities can be completed within the estimated timeframe.
- Whether the timeframe of the exemption should be amended.

As required under s59X(4), the agency must provide an update to the Privacy Commissioner on the review of the exemption.

2.11 Extension of the exemption period

An exemption under s59X applies for the period of time that the head of the agency reasonably believes notification would worsen cyber security or lead to further data breaches. When notifying the Privacy Commissioner that the agency is exercising this exemption, the head of the agency is required to provide advice concerning the anticipated timeframe during which the exemption will apply and how the agency will review the exemption.

As part of the monthly review of the exemption the agency should consider whether mitigation activities can be completed within the estimated timeframe notified to the privacy Commissioner. This should include consideration of whether the period for the exemption should be extended or amended. This information should be notified to the Privacy Commissioner as part of the monthly update under s59X(4).

Document information

Identifier/Title:	Guidelines on the exemption for compromised cyber security under section 59X
Business Unit:	IPC
Author:	Legal Counsel & Regulatory Advice
Approver:	Privacy Commissioner
Date of Effect:	26 September 2023
Next Review Date:	26 September 2024
EDRMS File Reference:	D23/028456/DJ
Key Words:	MNDB Scheme, data breach, exemption, cyber security