



information
and privacy
commission
new south wales

Statutory guidelines

NSW Mandatory Notification of Data Breaches Scheme

Guidelines on the exemption for investigations and legal proceedings under section 59T

Consultation Draft - October 2025

CONSULTATION DRAFT

Contents

1	Introduction	3
2	Exemption for investigations and legal proceedings	4
3	Factors to consider	6
4	When agencies should choose not to rely on the exemption	7
5	Notification and review	7

CONSULTATION DRAFT

1 Introduction

1.1 Background

Part 6A to 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 likely to result in serious harm.

The MNDB scheme requires agencies to have regard to any guidelines issued by the Commissioner when assessing a data breach.¹

These *Guidelines on the exemption for investigations and legal proceedings under section 59T* (**Guidelines**) have been made under section 59ZI of the PPIP Act.

These Guidelines are designed to help agencies recognise circumstances that trigger obligations under the MNDB scheme. They also aim to provide further clarification on what constitutes an eligible data breach.

These guidelines are not legal advice. Agencies have flexibility to apply the processes and definitions outlined below in the way that is most appropriate for their size, resources, and privacy risks. Agencies are encouraged to seek professional advice tailored to their own circumstances where required.

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:²

- *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*
- *Guidelines on the exemption for risk of serious harm to health and safety section 59W*
- *Guidelines on the exemption for compromised cyber security under section 59X*

¹ *Privacy and Personal Information Protection Act 1998* s 59I

² <https://www.ipc.nsw.gov.au/privacy/MNDB-scheme>.

2 Exemption for investigations and legal proceedings

2.1 Overview

When an eligible breach has occurred, the head of the agency must take all steps that are reasonably practicable to notify the individuals to whom the information relates or who may be affected by the breach.³

Under Section 59T, where the head of an agency reasonably believes notification of the eligible data breach under the Subdivision would be likely to prejudice--

- a) an investigation that could lead to the prosecution of an offence, or
- b) proceedings before a court or a tribunal, or
- c) another matter prescribed by the regulations for the purposes of this section,

the head of the agency may decide that the agency is exempt from the requirement to notify affected individuals.

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

- have regard to these guidelines,
- notify the Privacy Commissioner by written notice that the exemption will be relied upon.

It is the Privacy Commissioner's expectation that this notice should include advice concerning:

- the period of time for which the exemption will be applied and
- the method and frequency by which the agency will review the exemption.

Exemptions granted under section 59T should be temporary and reviewed regularly. Agencies must notify the Privacy Commissioner of their use of the exemption as soon as practicable after deciding to rely on the exemption and should provide an update upon each review.

The exemption only applies so long as the agency head reasonably believes that the notification to the affected individuals would prejudice an investigation, or proceedings before a court or tribunal or another matter prescribed by the regulations.

If an agency seeks to apply more than one exemption to notifying of a breach, the agency head must be satisfied the breach meets the requirements of both exemptions in full. Agencies should be conscious that the requirements vary, and one exemption may cease to apply before the other.

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 a data breach can be assumed to be beneficial, as it empowers and enables those individuals to take steps to protect themselves from potential harm. Exemptions to notification are intended to apply only in exceptional circumstances. The Privacy Commissioner expects that exemptions under this section will be applied in limited situations, justified thoroughly and in writing, and apply for a minimal period of time before review.

2.1.1 Matters arising from the data breach

Data breaches may give rise to legal action, however, the exemption under section 59T is not intended to apply to **anticipated** matters arising from the data breach itself. An agency may not use this exemption to avoid notifying if they **anticipate** actions arising from the breach, such as:

- that they may be the focus of a class-action lawsuit, or

³ *Privacy and Personal Information Protection Act 1998* s 59N

- commencing proceedings against or being a party to legal action against a hacker or other malicious actor or other person that caused or contributed to the data breach

if the broader criteria of the exemption (such as an active investigation) are not otherwise met.

There may be circumstances where a law enforcement body asks an agency not to notify due to an investigation that they are undertaking. In this instance, the agency should take steps to satisfy itself that this would meet the broader criteria of the exemption, as outlined throughout this guidance.

Agencies may not open an investigation as a shield against notifying – investigations must be genuine and active (see further below).

2.2 'Reasonable Belief'

To invoke section 59T, an agency head must '*reasonably believe*' that notification to affected individuals would prejudice an investigation, proceeding or other prescribed matter.

A 'reasonable belief' is a belief that results from the exercise of sound judgement. To justify a reasonable belief the agency head must be able to explain, based on their experience and the information available to them at the time of the decision, the basis on which the belief was formed. This means being able to articulate specifically how the notification would be prejudicial (see additional information under 2.4 Prejudice).

2.3 'Likely to'

In this context, '*likely to*' means more probable than not, not merely possible. The assessment of whether a notification is 'likely to' cause prejudice must be read in conjunction with 'prejudice', as reliance on this exemption requires demonstration of the causal relationship between notification and prejudice.

2.4 'Prejudice'

Prejudice holds its ordinary meaning: that the notification will be harmful to or have an adverse effect on the outcome of the investigation, court case or proceeding.

To rely on this exemption, agencies must demonstrate *how* notification is likely to prejudice the outcome – it is not adequate to state that it may do so, causality must be shown.

The agency must be able to describe the specific impact that notification would have. For example, that it would expose confidential information from an investigation that would then undermine that investigation or would be in contempt of court.

Note that this exemption is reliant on the prejudice, not the investigation or proceeding, and only applies for as long as the likely risk of prejudice applies.

2.5 'Investigation'

An *investigation* is any active investigatory activity that could lead to the prosecution of an offence (see 2.6 below). The investigation may be at any stage but must have formally been commenced or recorded and must not have been finalised.

An agency may have investigations that are open but that are not being pursued or actively investigated. It is very unlikely that an agency would be able to demonstrate that a notification would prejudice an inactive investigation.

There may arise a situation where an internal investigation has been completed and referred to a law enforcement body. In this instance the investigation would remain 'active', in that it is being investigated by the law enforcement body. However, it does not automatically follow that the prejudice would still apply.

The relevant investigation does not have to be undertaken by the notifying agency; it is sufficient that notification is likely to prejudice a formal investigation being undertaken by another agency or entity.

2.6 'Could lead to the prosecution of an offence'

2.6.1 'Could lead to'

The agency head must have reasonable belief that the investigation *could lead to* prosecution. 'Could lead to' does not have to be more probable than not, it is sufficient that an investigation is being undertaken where prosecution is a possible result.

2.6.2 'Prosecution of an offence'

This exemption is not confined to criminal proceedings.

Prosecution of an offence includes (but is not limited to):

- Criminal offences,
- Breaches of environmental or planning law,
- Breaches of administrative law, and
- Serious professional misconduct that may result in prosecution (e.g. fraud).

Examples of situations that would not be considered an 'offence' within this exemption include (but are not limited to):

- Civil proceedings,
- Disciplinary actions or code of conduct investigations that may lead to termination or performance management but not to prosecution.

2.7 'Proceedings before a court or tribunal'

'*Proceedings before a court or tribunal*' means an issue or case has been officially listed to be heard by a court or tribunal.

Court or tribunal proceedings do not need to be being undertaken in New South Wales; they may be before any state, territory or federal court (at any level) or any tribunal within Australia.

3 Factors to consider

The following are questions and considerations that will help you answer whether you can or should rely on this exemption. These factors are provided as examples to assist with decision-making — this is not a comprehensive list of factors that you may need to consider.

3.1 Prejudice

- What are the factors that make you believe notifying would prejudice the investigation or proceeding? (You may find it valuable to list the factors and the corresponding expected impact.)

3.2 Investigation

- Is there a formal investigation on foot that involves an affected party?
- What is the status of that investigation — is it open but inactive or active?

3.3 Could lead to the prosecution of an offence

- Has a matter involving the affected individual been referred to a law enforcement body?
- How serious is the matter being investigated/prosecuted? Is it a criminal offence, does it involve serious misconduct, and/or does it involve significant penalties?

3.4 Proceedings before a court or tribunal

- How would notifying affect proceedings?
 - Would it influence the testimony of a witness?
 - Would it introduce a risk of contempt of court?
 - Could it damage a party's claim that documents are protected by LLP (or otherwise disclose confidential matters)?

3.5 Other factors

- What are the likely impacts of the data breach?
- How severe are the impacts likely to be on affected individuals?
- To what degree will notification help affected individuals mitigate the likely impacts of the breach?
- To what extent is the data breach publicly known? Has there been any media coverage of the breach and if so, how much detail has been publicised?
- Does the prejudice apply to notification to any (or all) affected individuals, or only if notification is provided to a specific individual? Can notification be provided to some people without causing prejudice?
- Can the prejudice be mitigated through partial notification? (such as providing summary information about the breach, rather than detailed information)
- Can the impacts of the breach be lessened through partial notification? (such as providing summary information about the breach, rather than detailed information)

4 When agencies should choose not to rely on the exemption

Exercise of the exemption is at the discretion of the agency head, provided that all elements are met.

In deciding whether to exercise their discretion, agency heads should:

- consider whether it is in the public interest to do so, and
- weigh the severity of the breach and the impact for affected individuals against the seriousness of the offence being investigated or prosecuted.

For example, where the impact of notifying is likely to make a case or investigation considerably harder to prove, or add considerable complexity to obtaining evidence, but the anticipated impact of delaying notification to affected individuals is significant, it may be appropriate for an agency head to choose to notify, notwithstanding that the exemption may be available.

Where a notification will undermine an investigation or proceeding, or cause it to fail, but the offence being investigated is minor, and the impacts of the breach are significant, an agency may choose to notify of a serious data breach, notwithstanding the exemption.

5 Notification and review

5.1 Notifying the commissioner

When relying upon this exemption the head of the agency must notify the Privacy Commissioner in writing that the exemption is being relied upon.

The notification should include:

- The number of people who are affected by the exemption.
- An explanation of why and how notification is likely to be prejudicial.
- An expected timeframe of when the prejudice is likely to be resolved.
- The process that will be used to review this exemption.

5.2 Documenting decision-making

Good recordkeeping is an essential responsibility of agencies, as it enables transparency, accountability and ensures the agency is meeting legislative and regulatory requirements.

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. This includes any review that results in a further decision to rely on the exemption for another period.

Further information on good administrative recordkeeping for NSW agencies can be found in [Good conduct and administrative practice: guidelines for state and local government](#).

5.3 Review

An agency that has applied the exemption under s59T should nominate a time period that they reasonably think the exemption will apply. This nominated time period should be as short as reasonable in the circumstances, that is, limited to only the period in which the elements of this exemption are anticipated to apply.

Once this period has passed, the agency should review whether the exemption still applies. The review should consider:

- whether the investigation or proceeding is still active
- whether the risk of prejudice remains
- whether the scope of the prejudice remains unchanged (e.g. it may now be possible to notify some individuals or all individuals of some information)
- whether the initial assessment of 'likely to' still meets the threshold
- whether it is possible to reassess the timeframe for when the exemption should apply.

If the review finds the exemption is still required, the agency head should set a timeframe to reassess the exemption. This timeframe should be based on known factors and again, be as short as reasonable in the circumstances. If a known timeframe exists, this can be used for the re-review period. If a known timeframe does not exist, the exemption should be reviewed after no more than a month.

The agency should provide an update to the Privacy Commissioner on the review of the exemption. Any further reliance or extension should be advised to the Privacy Commissioner in advance of the expiry of the current exemption in place.

Further, agencies should establish a mechanism to ensure regular and structured internal information sharing between any department that might be undertaking an investigation and the area that is responsible for data breach notification and communication with the Privacy Commissioner.

The Privacy Commissioner will consider the matter open until they receive information that notification has been provided.

Document information

Identifier/Title:	Guideline - Guidelines on the exemption under section 59T
Business Unit:	IPC
Author:	Assistant Commissioner
Approver:	Privacy Commissioner
Date of Effect:	TBC
Next Review Date:	TBC
EDRMS File Reference:	D25/037457/DJ
Key Words:	MNDB Scheme, Exemptions, Investigation, Legal Proceedings