information and privacy commission
new south wales

Statutory guidelines

NSW Mandatory Notification of Data Breaches Scheme

Guidelines on the exemption if a public sector agency has taken certain actions under section 59U

Consultation Draft - March 2026

Contents

Guidelines on the exemption if a public sector agency has taken certain actions under section 59U

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 59U. This provision provides that the head of a public sector agency may decide to exempt the agency from notifying affected individuals if the agency has taken certain actions under s59U to mitigate the harm arising from an eligible data breach.

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

Privacy Commissioner

Information and Privacy Commission NSW

March 2026

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]

The *Guidelines on the exemption if public sector agency has taken certain actions under section 59U* (**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.

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:

- *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 Exemption if public sector agency has taken certain action

2.1 Overview

When an eligible data 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.[2]

Under Section 59U, the head of a public sector agency is exempt from notifying affected individuals if:

a) for an eligible data breach involving unauthorised access to, or disclosure of, personal information held by the agency—
   i. the agency the subject of the breach takes action to mitigate the harm done by the breach, and
   ii. the action is taken before the access to or disclosure of information results in serious harm to an individual, and
   iii. because of the action taken, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to an individual, or
b) for an eligible data breach involving the loss of personal information held by the agency
   i. the agency the subject of the breach takes action to mitigate the loss, and
   ii. the action is taken before there is unauthorised access to, or unauthorised disclosure of, the information, and
   iii. because of the action taken, there is no unauthorised access to, or unauthorised disclosure of, the information.

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 detailed information about the circumstances of the breach, including its scope and severity
- clearly identify the serious harm that the agency has identified as being likely to arise from the breach
- demonstrate how the risk of harm has been mitigated
- engage with the vulnerability of the persons affected.

These factors are discussed in detail within this Guideline.

Agencies must notify the Privacy Commissioner of their use of the exemption as soon as practicable after the agency head (or their delegate) has made the decision that the exemption is applicable.

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

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

exemptions under this section will be applied in limited situations, justified thoroughly and recorded in writing.

2.2 Key terms

Many of the key terms in this exemption are used in assessing whether or not a data breach is eligible under the Scheme and are therefore defined in Guidelines on the assessment of data breaches under Part 6A of the PPIP Act.

Selected key terms from Guidelines under Part 6A are provided in Section 3 for ease of reference.

2.2.1 Exemption Part (a)

To rely on the exemption under s59U(a) agencies must be able to demonstrate that they have taken actions such that the risk of serious harm has been removed or adequately mitigated.

2.2.1.1 Mitigate harm

In responding to a data breach, agencies will take a range of mitigating and remediating measures. Some of these measures will address the impacts of the breach for affected individuals, and some will relate to future organisational processes or prevention measures.

When applying this exemption, agencies must consider that the actions that are taken must mitigate the harm *before* it occurs.

While it is possible that some remediation actions may decrease the risk of harm to affected individuals, this exemption is primarily focussed on mitigation actions.

Remediation actions that decrease the impacts of the harm after it has occurred (such as paying for the replacement of proof of identity documents) do not fulfil the requirements of this exemption.

2.2.1.2 Demonstrate how the action has mitigated serious harm

To rely on this exemption, agencies must be able to demonstrate and explain how the actions they have taken have adequately mitigated the risk of serious harm. When informing the Privacy Commissioner of their reliance on this exemption, agencies must be able to explain how the action/s taken has mitigated the harm.

> ***Example:*** *where an agency has taken action to mitigate harm*
>
> *An agency experienced a data breach involving the unauthorised disclosure of customer passwords. The agency determined that the incident was an eligible data breach as there was a likelihood of serious harm to individuals whose information was affected by the data breach.*
>
> *The agency took the following actions:*
>
> - *swiftly undertake a mass password reset for all affected accounts, and*
> - *use technical tools to confirm that non-sensitive website use history has been exposed but no financial or sensitive information had been accessed between the time of the breach and the time of the reset.*

The level of certainty that the harm has been mitigated must be proportional to the potential seriousness of the harm (see section 2.2.1.6 below).

2.2.1.3 'Reasonable person'

To rely on section 59U where these has been unauthorised access to or disclosure of personal information, the mitigation action must be such that "a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to an individual."

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.

Similarly, a reasonable person is a person who is properly informed of the circumstances and can exercise sound judgement.[3]

2.2.1.4 Not likely to

In assessing whether a data breach is 'likely' to cause serious harm, agencies must assess whether the outcome is more likely than not, rather than merely possible.

In this context, the assessment is that 'the access or disclosure would *not be likely* to result in serious harm to an individual', specifically because of the mitigation actions taken.

In assessing the mitigation actions that have been taken, agencies must find that the balance of probability has reversed such that serious harm *not* occurring is the most likely outcome.

In this instance, as in any assessment of the risk of serious harm, agencies must also take into account:

- the extent to which affected individuals may be particularly vulnerable to harm,
- the ease with which information can be accessed and individuals identified
- whether the circumstances of the breach increase the likelihood of deliberate harm.[4]

2.2.1.5 Individual

An "affected individual" is defined under s59D of the PPIP Act as an individual:

- to whom the information subject to unauthorised access, unauthorised disclosure or loss relates, and
- who a reasonable person would conclude is likely to suffer serious harm as a result of the data breach.

In assessing harm for this exemption, the assessment should consider the potential harm to an individual, rather than a cohort of individuals. That is, it is not adequate to say that the harm is 'not likely to' cause serious harm to a group of people when considered as a whole – the assessment of harm should be specific to the individual/s affected by the breach. Due to individuals' differing circumstances, there may be individuals for whom it is possible to mitigate harm and others for whom it is not, within the same cohort.

2.2.1.6 Proportionality

The actions that have been taken to mitigate harm must be proportionate to the level of potential harm. This relates to:

- the inherent risk of the type of information – e.g. more sensitive information, or more exploitable information
- the vulnerability of the affected individuals, where the agency might be reasonably expected to have this information (see more at 2.2.1.7 below)
- the specific circumstances of the breach – e.g. was it the result of a cyber-attack versus accidental disclosure; was it a disclosure to another Government agency versus disclosure to a person outside the agency who may have reason to exploit it.

Agencies should ensure they have considered that their mitigation actions are responsive to the specific harm that is likely to ensue.

---

[3] See Guidelines on the assessment of data breaches under Part 6A of the PPIP Act section 2.7

[4] See Guidelines on the assessment of data breaches under Part 6A of the PPIP Act section 3.4

Agencies should consider the information on 'serious harm' provided in Guidelines on the assessment of data breaches under Part 6A of the PPIP Act (set out in section 3 of this guideline for convenience).

2.2.1.7 Vulnerability

Before relying on this exemption the agency must take into account the vulnerability of affected individuals.

Agencies must consider any factors affecting vulnerability:

- Is this person inherently vulnerable (financial, socially etc)?
- Does the service provided by the agency inherently disclose sensitive information or make the person vulnerable to social stigma or disadvantage (for example, a drug treatment clinic)?
- Has this person previously been affected by a data breach (particularly a data breach of the same agency), which increases their vulnerability to risks such as identity theft?

If the breach affects vulnerable people (or even one vulnerable person), this will impact the likely seriousness of the breach and consequently increase the threshold for both proportionality and certainty that harm has been mitigated.[5]

2.2.2 Exemption Part (b)

To rely on exemption at s59U(b) agencies must be able to demonstrate that, as a result of the mitigation action taken, no unauthorised access or disclosure has taken place.

2.2.2.1 Demonstrate how the action has prevented access/disclosure

To rely on this exemption, agencies must be able to demonstrate and explain how the actions they have taken have adequately prevented unauthorised access or disclosure of personal information.

In case of loss of personal information, actions must be taken to mitigate loss *before* there is unauthorised access/disclosure of information.

> ***Example:*** *where an agency has taken steps to mitigate harm*
>
> *An agency may be confident that a mis-sent email has not been accessed as;*
>
> - *it was sent to an unrelated Government agency (not a related individual),*
> - *the incorrect recipient proactively and immediately notified the agency that the email had been sent in error and,*
> - *the recipient has confirmed that the email had been deleted.*
>
> *Here, the agency's confidence that the loss has been mitigated comes from all of these factors: the proactive notification, that it was not sent to an individual with a reason to access the information or seek to harm the individual, and the written confirmation of deletion from a government agency.*

The level of certainty that the access/disclosure has been prevented must be proportional to the potential seriousness of the harm (outlined further below).

2.2.2.2 No unauthorised access or disclosure

Part (b) of this exemption requires that: "because of the action taken, there is no unauthorised access to, or unauthorised disclosure of, the information."

[5] See also Guidelines on the assessment of data breaches under Part 6A of the PPIP Act section 3.4.7

The threshold for relying on Part (b) is higher than that of relying on Part (a) because this exemption requires that unauthorised access or disclosure has not occurred – an assessment of likelihood is not required, as the agency must be able to confidently assert that the access/disclosure has *not* occurred. If the agency cannot determine with confidence that the access or disclosure has not occurred, they may not rely on Part (b).

2.2.2.3 Proportionality and vulnerability

In assessing whether an action meets the requirements of Part (b), proportionality and vulnerability must be assessed, as outlined above.

However, an agency is not assessing mitigation actions, it is assessing whether the level of certainty that access or disclosure has been averted is adequate when weighed against the potential risk of harm.

> ***Example:*** *where mitigation action taken may not be sufficient*
>
> *If, instead of being sent to an unrelated Government agency, the mis-sent email was sent to a person listed as the individual's spouse, the assessment of proportionality and vulnerability (and thus certainty) may reach a different outcome.*
>
> *The agency may still consider the recipient's proactive communication as relevant, but must also consider other contextual factors, such as:*
>
> - *how sensitive is this information?*
> - *what is the role of this agency and does that add sensitivity to the information?*
> - *is there any history of legal disputes or family violence that should be taken into account?*
> - *do any of these factors decrease the believability of the recipient's assertion that the information was deleted before it was accessed?*

3 Key terms as defined in Guidelines on the assessment of data breaches under Part 6A of the PPIP Act

These terms are defined in the Guidelines on the assessment of data breaches under Part 6A of the PPIP Act and are provided for convenience. Additional information on the assessment of data breaches is provided in the Guideline under Part 6A, which should be read as part of the assessment of any data breach.

3.1 'Unauthorised access'

Unauthorised access to personal information occurs when personal information held by an agency is accessed by someone who is not permitted to do so.

Unauthorised access can occur:

- Internally within an agency – for example, an employee browses agency records relating to a family member or a celebrity without a legitimate purpose.
- Between agencies – for example, a team at one agency may be provided with access to systems and data at a second agency as part of a joint project. Unauthorised access may occur if a member of the team were to use that access beyond what is required for their role as part of that project.
- Externally outside an agency – for example, personal information is compromised during a cyberattack and accessed by a person external to the agency.

3.2 'Unauthorised disclosure'

Unauthorised disclosure occurs when an agency (intentionally or accidentally) discloses personal information in a way that is not permitted by the PPIP Act or HRIP Act.

For example, an unauthorised disclosure may occur where:

- A system update results in the unintended publication of customer records containing personal information on an agency's website.
- An agency intends to provide de-identified information to a researcher but accidently sends the data with personal identifiers included.
- An agency provides personal information to the wrong recipient regardless of whether the information was viewed or accessed by the recipient.
- A database hosted in a cloud environment or a web facing application containing personal information does not have appropriate access controls and personal information in the data set is visible and accessed by unauthorised individuals.

Unauthorised access and disclosure are not mutually exclusive and may occur as a result of the same breach or as part of a chain of events. For example, if a malicious external actor gains unauthorised access to agency records during a cyberattack, and steals information from those records, this may amount to unauthorised access to, and unauthorised disclosure of, the personal information held within those records.

3.3 'Loss

Loss refers to situations in which personal information is removed from the possession or control of the agency. Loss may occur because of a deliberate or accidental act or omission of the agency, or due to the deliberate action of a third party. For example, personal information might be lost when:

- An agency sells or disposes of a physical asset (such as a laptop or filing cabinet) that still contains personal information.
- An agency employee accidentally leaves a device containing personal information on the bus.
- A device containing personal information is stolen from agency premises or an employee's home.

The loss of personal information will only result in an eligible data breach where such loss is likely to result in unauthorised access or disclosure of this information. If the personal information is inaccessible due to security measures or because the information is retrieved before it is accessed or disclosed, then it is unlikely that an eligible data breach has occurred.

Examples of this may include where:

- A password protected laptop containing client files is left on a bus but is handed into the depot and the agency is able to retrieve the laptop which has not been accessed.
- A USB containing personal information is lost but is both encrypted and password protected.
- A tablet device containing client records is stolen from an employee's home, but it is only accessible via multifactor authentication.

As the loss of personal information in the above examples did not result in an unauthorised access or disclosure, no eligible data breach has occurred.

In some cases, a loss that results in serious harm to an individual may not necessarily amount to an eligible data breach. For example, where customer records are unintentionally deleted from a records management system, resulting in the denial of a particular service to those customers. Although this would not be an eligible data breach and notification is not mandatory in this scenario, it is nonetheless recommended that agencies consider voluntarily informing individuals of the loss of their information where there is a risk of serious harm.

3.4 Serious harm

The term 'serious harm' is not defined in the PPIP Act. Harms that can arise as the result of a data breach are context-specific and will vary based on:

- the type of personal information accessed, disclosed or lost, and whether a combination of types of personal information might lead to increased risk,
- the level of sensitivity of the personal information accessed, disclosed or lost,
- the amount of time the information was exposed or accessible, including the amount of time information was exposed prior to the agency discovering the breach,
- the circumstances of the individuals affected and their vulnerability or susceptibility to harm (that is, if any individuals are at heightened risk of harm or have decreased capacity to protect themselves from harm),
- the circumstances in which the breach occurred, and
- actions taken by the agency to reduce the risk of harm following the breach.

Serious harm occurs where the harm arising from the eligible data breach has, or may, result in a real and substantial detrimental effect to the individual. That is, the effect on the individual must be more than mere irritation, annoyance or inconvenience.

Harm to an individual includes physical harm; economic, financial or material harm; emotional or psychological harm; reputational harm; and other forms of serious harm that a reasonable person in the agency's position would identify as a possible outcome of the data breach.

While mere irritation or annoyance does not in itself amount to serious harm, emotional or psychological impacts of a data breach can amount to serious harm if they are severe.

4 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.

Questions	Factors to consider
Have there yet been any impacts of the breach?	If there have already been any impacts of the breach, then the agency will not be able to rely on this exemption.
How did you find out about the breach?	A data breach that was notified to you by an external body (such as by media or an affected individual) is unlikely to be able to mitigate impacts before they are experienced. A small-scale accidental disclosure, like an email that is sent only to one person, is one of the few examples where the exemption may still be relied upon despite external identification. A breach that was notified by the affected individual does not necessarily mean that harm has not occurred.
How long did it take to become aware of the breach?	The longer a breach has gone undetected, the less likely it is that satisfactory mitigation of harm will be possible.
How severe would the impacts of the breach have been on affected individuals?	The severity of the likely impacts of the breach should be considered in assessing whether mitigation measure have been adequate to apply the exemption.
How are you balancing certainty against sensitivity?	Agencies should systematically consider the sensitivity of the information involved in the breach when asserting certainty that harm has been mitigated or access/disclosure has been avoided. The more sensitive the information, the higher the degree of certainty that is required.

5 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
- whether there is benefit to individuals in receiving notification notwithstanding the exemption.

For example, where the serious harm that may arise from an eligible data breach has been mitigated, but the surrounding circumstances mean that the breach will become known and publicised, individuals may benefit from a breach notification giving them information and reassurance.

In a circumstance where the potential impacts of a data breach were substantial or extremely harmful, an agency might choose to notify despite being confident that they have mitigated these impacts, to add an additional layer of protection to the individuals impacted and build trust.

6 Notification and recordkeeping

6.1 Notifying the Privacy Commissioner

When relying upon this exemption the agency head (or delegate) must notify the Privacy Commissioner in writing that the exemption is being relied upon, as soon as is practicable after they have made the decision that the exemption is applicable.

The notification should include:

- the number of people who are affected by the exemption
- the types of harm/s that have been identified as potentially arising from the breach
- detailed information about the steps taken to mitigate the harm
- an explanation of how and why the agency believes that the likelihood of serious harm has been mitigated, including detailed information about how the steps taken are appropriate and proportionate for the specific harm.

6.1.1 Delegation

The decision to rely on this exemption is a significant one, and it is important to ensure that any delegations that are in place are appropriate for the circumstances.

Any delegated decision-maker should have adequate skills and experience to apply the PPIP Act and the statutory guidelines and hold sufficient seniority to be able to justify the decision to apply a notification exemption. Consideration should be given to the higher risk or sensitivity of choosing to apply an exemption, which may require a more senior decision-making delegation.

The Agency Head and senior leadership should retain visibility of decisions made, as, notwithstanding any delegations, the Agency Head remains accountable for all decisions made under the Mandatory Notification of Data Breach scheme.

6.2 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.

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

Document information

Identifier/Title:	Guidelines on the exemption if public sector agency has taken certain actions under section 59U
Business Unit:	IPC
Author:	Assistant Commissioner (Reviews & Compliance)
Approver:	Privacy Commissioner
Date of Effect:	Day Month 20XX
Next Review Date:	Day Month 20XX+ 1 year
EDRMS File Reference:	D26/007694/DJ
Key Words:	Eligible data breach, exemption, notification, assessment, mitigation of harm