information and privacy commission new south wales

Guide to Regulatory Action under the MNDB Scheme

August 2023

Administration of the Mandatory Notification of Data Breaches Scheme

The NSW Privacy Commissioner administers the Mandatory Notification of Data Breach (MNDB) Scheme established under Part 6A of the *Privacy and Personal Information Protection Act 1998* (PPIP Act).

The provisions of Part 6A impose obligations on NSW public sector agencies to:

- assess suspected data breaches to determine whether an eligible data breach has or is likely to have occurred
- undertake steps to contain an eligible data breach
- undertake steps to mitigate the effects of an eligible data breach in order to reduce the risk of serious harm to affected individuals
- notify the Privacy Commissioner that an eligible data breach has occurred
- notify affected individuals that an eligible data breach has occurred
- prepare and publish a data breach policy
- keep and maintain a register of eligible data breaches.

In oversighting the MNDB Scheme the Privacy Commissioner will adopt a range of regulatory approaches as relevant to achieve the objects and intent of the MNDB Scheme. This guide outlines the Privacy Commissioner's regulatory approach to receiving and responding to mandatory notifications made under the MNDB Scheme and aims to provide clarity and transparency about the Privacy Commissioner's regulatory approach and intent.

The Privacy Commissioner's compliance approach is underpinned by the principles established in the IPC Regulatory Framework:

- **Constructiveness:** We engage with agencies and provide advice and guidance to assist compliance.
- **Consistency:** Similar circumstances lead to similar regulatory responses and outcomes.
- **Targeted:** Regulatory activities are focused on the areas of highest regulatory risk.
- **Proportionality:** Regulatory activities are proportionate to the seriousness of the regulatory risk.
- **Accountability:** We explain our decisions and make available avenues of complaint review.
- **Transparency:** We demonstrate our values of independence and integrity in all our dealings with agencies and citizens of NSW.

Status of the Voluntary Data Breach Scheme

The former Voluntary Data Breach Scheme (VDB Scheme) operated by the Privacy Commissioner ceased on the commencement of the MNDB Scheme. As of 28 November 2023, all notifications are to be made in accordance with the MNDB Scheme.

Privacy Commissioner's Functions under the MNDB Scheme

Under section 36(2)(m) of the PPIP Act, the Privacy Commissioner has the following functions in relation to Part 6A:

> *'to investigate, monitor, audit and report on a public sector agency's compliance with Part 6A, including the agency's data handling systems, policies and practices.'*

In undertaking these functions, the Privacy Commissioner will:

- encourage and promote agency compliance with the MNDB Scheme
- receive eligible data breach notifications from agencies under section 59M
- assess information provided via a notification in order to satisfy themself that the agency has complied with its obligations under Part 6A
- provide agencies with advice on best practice data breach response and remediation, and
- publish guidelines and other resources to build agency capacity and knowledge, and provide information to citizens about the operation of the MNDB Scheme and their rights under the PPIP Act.

The Privacy Commissioner may also:

- undertake an own motion investigation or audit of the systems, policies and practices of an agency
- undertake monitoring activities with respect to an agency's response to an eligible data breach
- direct an agency to prepare and provide the Privacy Commissioner with a statement containing information about a suspected eligible data breach, and
- make recommendations to agencies with respect to the notification of individuals affected by the suspected eligible data breach.

Notifications under the MNDB Scheme

Agencies must assess all suspected eligible data breaches and take appropriate action to contain, evaluate and remediate the data breach. Once the head of an agency has determined that a data breach is an eligible data breach under Part 6A, the agency must, in the approved form, immediately notify the Privacy Commissioner of the eligible data breach (section 59M).

Under the MNDB Scheme the Privacy Commissioner receives a data breach notification which meets the threshold of an 'eligible data breach' established under Part 6A. Only those which satisfy the threshold test under Part 6A are required to be notified to the Privacy Commissioner under the MNDB Scheme.

Receiving notifications

When receiving notification of an eligible data breach under section 59M, the Privacy Commissioner will only accept written notifications provided in the approved form submitted available on the IPC website and submitted to the IPC. Verbal notifications or written notifications not made via the approved form will not be accepted.

The Privacy Commissioner will acknowledge receipt of all eligible data breach notifications made under the MNDB Scheme. The Privacy Commissioner may also seek further information from an agency in relation to the notification if required.

Most notifications will be dealt with by making an assessment and/or preliminary inquiries and providing information to the agency to ensure privacy obligations are met. Following an assessment of the notification, the Privacy Commissioner may decide not to take further regulatory action.

In the case of notifications that indicate serious non-compliance with privacy obligations, the Privacy Commissioner may conduct a compliance audit or investigation or take other appropriate regulatory action.

Consistent with the approach outlined in the broader IPC Regulatory Framework, not all notifications will result in the taking of regulatory action. The IPC must work within its available resources to ensure that regulatory activities are targeted appropriately and proportionate to their risk. The factors to be considered when determining appropriate regulatory action are set out below in 'Factors informing regulatory action'.

The Privacy Commissioner's weighing of any particular factor in making a decision to conduct a compliance audit, investigation or other regulatory action will depend on the individual circumstances of each case.

Importantly, while not all notifications received by the Privacy Commissioner will result in regulatory action, all notifications are recorded so further action can be taken if a pattern of non-compliance is observed in the future in relation to the relevant agency.

Powers available to the Privacy Commissioner

In addition to the general powers of the Privacy Commissioner to conduct inquiries and investigations under sections 36-39 of the PPIP Act, Part 6A provides for the following specific powers to:

- direct an agency to prepare and give the Privacy Commissioner a statement about a suspected eligible data breach (section 59Y(2))
- recommend that an agency notify individuals about the suspected eligible data breach or publish a notification under section 59N(2) as if it were an eligible data breach (section 59Y(3))
- investigate, monitor, audit and report on the exercise of a function of one or more agencies, including the systems, policies and practices of an agency, that relate to Part 6A (section 59Z)
- make and publish written reports in relation to a function of the Privacy Commissioner under Part 6A (sections 59ZB and 59ZC).

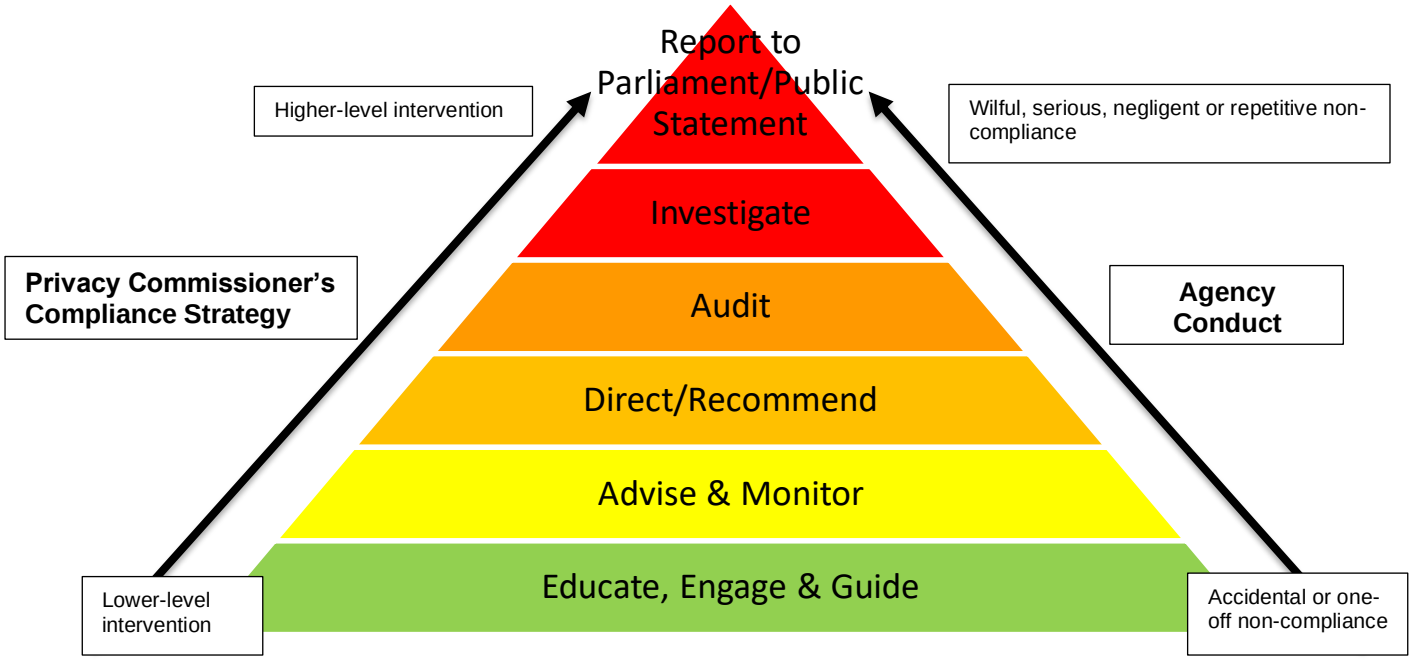
The Privacy Commissioner may also direct the head of an agency to provide access to its premises for the purpose of monitoring and reporting on the agency's compliance with the requirements under Part 6A (section 59ZA). If the Privacy Commissioner considers that it would be appropriate to enter an agency's premises to observe its systems, policies and/or procedures, the Privacy Commissioner will issue a notice setting out the direction and the day and time for compliance with the direction. Members of the IPC may, on behalf of the Privacy Commissioner, enter the premises on the specified day and time to observe a demonstration of the agency's data handling policies and procedures, and inspect documents relating to the agency's data handling policies and procedures. This information may be used to inform the Privacy Commissioner's investigation, monitoring, auditing and reporting functions with respect to the mandatory notification of data breaches scheme.

When regulatory action will be taken

The Privacy Commissioner will exercise their powers to undertake regulatory action that is proportionate to the circumstances of each case. The Privacy Commissioner will apply an escalation model to determine the appropriate regulatory action in response to non-compliance by agencies with respect to their obligations under Part 6A. The type of regulatory response taken by the Privacy Commissioner will be risk-based and proportionate to the circumstances of the eligible data breach. This approach to regulatory action is consistent with the IPC's overall approach to risk-based regulation overseen by the IPC's Regulatory Compliance Committee.

The IPC's Regulatory Compliance Committee will continue to play a role in providing advice on proposed regulatory action consistent with the approach outlined below to ensure actions remain guided by a risk-based and intelligence-informed approach to regulation, with focused attention and activity on emerging issues, entities and sectors that pose the greatest risk.

The following diagram sets out the escalation levels and the corresponding regulatory action that may be taken.



Types of regulatory action that may be taken by the Privacy Commissioner

Educate, Engage and Guide

The Privacy Commissioner encourages and supports compliance through guidance, education and promoting good practice. The IPC provides agencies with guidance and tools to promote best practice and to identify and address privacy concerns as they arise. This includes the publication of guidelines, guidance material, self-assessment tools and training via e-learning modules.

Advise and Monitor

The IPC works with agencies to improve privacy compliance and best practice through the provision of tailored advice on agency practices, policies and systems. The IPC encourages agencies to seek guidance, advice or comment from our office after accessing our published resource materials.

In circumstances where the Privacy Commissioner considers that an agency has taken active steps to address and remediate the eligible data breach, but may benefit from further engagement on the issue, the Privacy Commissioner may also decide to monitor an agency's response to a data breach event. This may include requesting periodic updates from the agency concerning its notification processes, assistance provided to affected individuals, updates to systems, policies and procedures, and any other remediation activities being implemented to prevent future breaches. Intelligence from monitoring activity may also inform the development of the IPC's audit program or inform decisions on future regulatory action.

Directions and Recommendations

Where the Privacy Commissioner becomes aware that there are reasonable grounds to believe an eligible data breach has occurred that has not been notified to the Privacy Commissioner, the Privacy Commissioner may by written notice direct the agency to prepare a statement and give it to the Privacy Commissioner (section 59Y(2)).

The information required by the notice will include the following details:

- the name and contact details of the agency
- a description of the suspected eligible data breach
- the kind of information involved in the suspected eligible data breach
- the recommendations about the steps that a notifiable individual should take in response to the breach
- the name and contact details of any other agencies involved in the suspected eligible data breach, and
- any other information that the Privacy Commissioner considers relevant to the suspected eligible data breach.

Similarly, the Privacy Commissioner may recommend that an agency notify affected individuals or publish a notification as if the suspected breach were an eligible data breach (section 59Y(3)).

Before making a direction or recommendation, the Privacy Commissioner will invite the agency to make a submission (section 59Y(4)). When deciding whether to make a direction or recommendation, the Privacy Commissioner will take into consideration:

- any advice given to the Privacy Commissioner by a law enforcement agency
- any submission made by the agency
- any other matters the Privacy Commissioner considers relevant.

Audit

The Privacy Commissioner may decide to undertake an audit in response to a complaint or series of complaints (whether from the public, a public interest disclosure or another agency) about any issue(s) concerning an agency's compliance with their obligations under Part 6A. In undertaking the audit, the Privacy Commissioner may examine the practices of an agency to assess compliance with Part 6A and provide recommendations on actions to uplift agency practices, policies and systems.

Following completion of the compliance audit, the findings and outcome may be included in a written report.

If the Privacy Commissioner considers it appropriate to make an adverse comment about a person and/or a public sector agency in a report, the Privacy Commissioner will inform the person and/or agency of the substance of the grounds for the adverse comment and provide them with the opportunity to provide a submission in response to the adverse comment (section 59ZC).

The Privacy Commissioner will take into consideration any submission provided by the person and/or agency prior to finalising the report.

Once the report has been finalised, the Privacy Commissioner may do any of the following:

- publish the report
- give a copy of the report to the Minister
- give a copy of the report to the head of the agency.

If the Privacy Commissioner proposes to publish a report that makes adverse comment about an agency, before publishing the report, the Privacy Commissioner will inform the responsible Minister and, if requested by the Minister, undertake a consultation with the Minister.

Investigation

An own-motion investigation may be undertaken where the Privacy Commissioner identifies serious cases of non-compliance with Part 6A. This includes circumstances where the Privacy Commissioner believes that:

- an agency has failed to implement appropriate practices, policies or systems despite engagement with the IPC
- there are potential systemic issues with the agency's compliance under Part 6A such as repeated and deliberate breaches of its obligations
- the data breach has resulted in significant risks of harm to an individual or group of individuals
- the data breach has impacted a significant number of individuals.

Other factors that may be relevant are set out below in 'Factors informing regulatory action'.

The results of the investigation will be reported to the agency, relevant Ministers and the public. The findings and outcome of the investigations may also be included in a written report under section 59ZB and reported to and tabled in Parliament (see 'Special Report to Parliament/Public Statement' below).

Similar to audit reports, if the Privacy Commissioner intends on making an adverse comment about a person and/or a public sector agency in a report, the Privacy Commissioner will provide the person and/or agency with procedural fairness by allowing them the opportunity to provide a submission in response to the adverse comment. The Privacy Commissioner will take into account any submission provided by the person and/or agency prior to finalising the report.

If the Privacy Commissioner proposes to publish a report that makes adverse comment about an agency, before publishing the report, the Privacy Commissioner will also inform the responsible Minister and, if requested by the Minister, undertake a consultation with the Minister.

Special Report to Parliament/Public Statement

Where the Privacy Commissioner has identified serious, flagrant, or repeated breaches of an agency's obligations under Part 6A, the Privacy Commissioner may:

- make a special report to Parliament under section 61C of the PPIP Act and/or
- issue a public statement concerning the relevant conduct consistent with the Privacy Commissioner's functions under section 36(2)(h) of the PPIP Act.

Where a special report is made to Parliament under section 61C, a copy of the report will also be provided to the responsible Minister.

Factors informing regulatory action

When deciding whether to undertake appropriate regulatory action following an agency's assessment of a notification under the MNDB Scheme, the Privacy Commissioner will take into account a range of factors including:

- the nature and seriousness of the data breach, including:
    - the number of persons affected or potentially affected
    - the categories of personal information affected
    - the sensitivity of the personal information exposed and the potential for adverse consequences to one or more individuals arising from the breach
    - the type and level of harm resulting from or likely to be caused by the data breach
    - whether disadvantaged or vulnerable groups may have been or may be particularly adversely affected or targeted
- whether the agency has been the subject of prior regulatory action, and the outcome of that action
- whether the breach raises new or repeated systemic issues, or concerns that technological security measures are not protecting the personal information held by the agency
- the manner in which the data breach became known to the Privacy Commissioner and, if relevant, any failure or delay by the relevant agency to notify the Privacy Commissioner of the breach
- the regulatory response, including action or inaction by the agency to any previous advice or assistance provided by the Privacy Commissioner
- any action taken by the agency to remedy and address the consequences of the data breach
- the cost and time to the IPC in order to achieve an appropriate outcome
- any advice given by a law enforcement agency (if any)
- any submission made by the head of the agency in accordance with section 59Y(4) (if any), and
- any other factors which the Privacy Commissioner considers relevant in the circumstances.

Working with other regulators or agencies

Where appropriate the Privacy Commissioner may collaborate, share information with, or refer notifications to, other privacy regulators, law enforcement bodies or NSW public sector agencies with relevant responsibilities (sections 47 and 67(2)). This may include where notifications raise potential contravention of other NSW legislation or where they concern matters arising under a law of another State, Territory or the Commonwealth.

This may include engagement with:

- Cyber Security NSW
- NSW Police Force
- NSW Auditor General
- ID Support NSW
- Privacy regulators in other Australian jurisdictions.

Document information

Identifier/Title:	Guide to Regulatory Action under the MNDB Scheme
Business Unit:	IPC
Author:	Director Investigation and Reporting
Approver:	Privacy Commissioner
Date of Effect:	August 2023
Next Review Date:	August 2024
EDRMS File Reference:	D22/011953/DJ
Key Words:	Regulatory action, MNDB, privacy, notification, investigation, audit, direction, recommendation, monitoring