Mandatory Notification of Data Breach (MNDB) Scheme – Quick Guide

Information Privacy Act 2009

What's happening?

As part of the reforms under the *Information Privacy and Other Legislation Amendment Act 2023* (IPOLA) a Mandatory Notification of Data Breach (MNDB) scheme will commence on 1 July 2025 for public sector agencies, with the exception of local councils where the scheme will commence on 1 July 2026.

The MNDB scheme requires agencies to:

- Contain the data breach and mitigate harm.
- Determine if the breach is an eligible data breach.
- If an eligible data breach, notify the Information Commissioner and particular individuals.
- Publish a data breach policy about how data breaches will be managed.
- Maintain an internal register of eligible data breaches.

When is a breach an eligible data breach?

An eligible data breach under the MNDB scheme applies when:

- There is unauthorised access to, or unauthorised disclosure of, personal information held by the agency, or there is a loss of personal information held by the agency in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur.

- The unauthorised access to, or disclosure of the information is likely to result in serious harm to an individual to whom the personal information relates (an 'affected individual').

How can agencies start preparing?

- **Develop a unified approach** to data breach management across a cross section of subject matter experts from privacy, information management and security, cyber, human resources, governance, records, legal and incident management.

- **Review your agency data breach framework (policies, procedures and systems)** and consider the appropriate roles and responsibilities required to identify if a breach includes personal information, and how to assess and manage the range of potential breaches that may occur in your agency. This will form part of your agency's data breach policy.

What is serious harm?

Serious harm can include serious physical, psychological, emotional, financial, or reputational harm to the individual.

Other types of harm may also meet the serious threshold. The effect on an individual must be more than irritation, annoyance, or inconvenience.

Factors to consider:

- the kind of personal information accessed, disclosed or lost
- the sensitivity of the personal information
- whether the personal information is protected by one or more security measures and the likelihood that any of those measures could be overcome
- the kind of person/s who have or could obtain the personal information
- the nature of the harm likely to result from the breach, and
- any other relevant matter.

How is OIC supporting you?

To support agencies prepare for the IPOLA reforms, the Office of the Information Commissioner is delivering Guidelines, other resources and a staged training program to build awareness and knowledge.

- Keep across the published Guidelines and training material available via the IPOLA webpage on OIC's website. Specific MNDB Guidelines include:
  - MNDB Scheme
  - MNDB Scheme Policy and Register, and
  - MNDB Scheme Exemptions.
- Keep updated by subscribing to OIC's newsletters.

This guide does not reflect the current law.
It highlights important changes to the *Information Privacy Act 2009.*
This guide does not constitute legal advice and is general in nature only. Additional factors may be relevant in specific circumstances.
For detailed guidance, legal advice should be sought.

The Queensland Audit Office has published a report on government agencies preparedness for mitigating and managing cyber-attacks: Responding to and Recovering from Cyber-attacks.

In November 2023, an MNDB scheme began in NSW. According to their most recent data:

Approximately two out of three breaches were caused by human error...

Personal information sent to wrong recipient email

+

Unauthorised disclosure or unintended release of publication

Approximately one out of three breaches were caused by malicious and criminal attack...

Phishing (compromised credentials), stolen and compromised credentials

+

Ransomware, hacking, malware, and brute-force attack

Office of the Information Commissioner
Queensland

IPOLA

To contact us or for more information visit www.oic.qld.gov.au/ipola