information and privacy commission new south wales

Fact Sheet **November 2023**

MNDB Scheme Frequently Asked Questions

Who is this information for?	NSW citizens seeking information about the Mandatory Notification of Data Breach Scheme.
Why is this information important to them?	This Fact Sheet will help citizens to understand more about the Scheme and what their rights are when a data breach involving their personal information occurs.

What is the Mandatory Notification of Data Breach Scheme?

The Mandatory Notification of Data Breach Scheme (MNDB Scheme) is a mandatory notification requirement under the *Privacy and Personal Information Protection Act 1998* (PPIP Act) for NSW public sector agencies in the event of an 'eligible data breach'.

When did the MNDB Scheme commence?

The MNDB Scheme commenced on 28 November 2023.

Who does the MNDB Scheme apply to?

The MNDB Scheme applies to NSW public sector agencies, Ministers, Universities, Councils and State-Owned Corporations that are not covered by Commonwealth privacy legislation.

What is a Data Breach Policy?

A Data Breach Policy (or DBP) is a documented policy or plan setting out how an agency will respond to a data breach. Agencies are required to have a DBP under the legislation. A DBP should establish the roles and responsibilities of agency staff in relation to managing a breach, and the steps the agency will follow when a breach occurs.

Agencies are required to ensure their DBP is publicly accessible which means agencies should publish their DBP on their website.

What is an 'eligible data breach'?

Under the MNDB Scheme, an agency must notify the affected individuals and the Privacy Commissioner when there has been an eligible data breach.

An 'eligible data breach' occurs when there is:

- unauthorised access to, or unauthorised disclosure of, personal information held by an agency that would be likely to result in **serious harm** to an individual to whom the information relates
- the loss of personal information held by an agency in circumstances where unauthorised access or disclosure is likely to occur, and which would be likely to result in **serious harm** to an individual to whom the information relates.

What is serious harm?

Serious harm can include physical, financial, or material harm, emotional or psychological harm, or reputational harm. The impact of the harm can vary from person to person, but may include:

- financial loss through fraud
- a likely risk of physical or psychological harm, such as by an abusive ex-partner
- identity theft, which can affect your finances and/or credit record
- serious harm to an individual's reputation.

How might a data breach occur?

Broadly, a data breach can occur because of human error, systems failure or a malicious or cyber breach.

What are examples of data breaches?

Some examples of data breaches are:

Human error:

- A Letter or email is sent to the wrong recipient.
- System access is incorrectly granted to someone without authorisation or there is inadequate password protection.
- Physical assets with Personal Information are lost/misplaced e.g., records, laptop, USB, phone.

System failure :

- A coding error allowing system access without authentication, or automatically generating notices.

- Systems are not maintained through the application of known and supported patches.

Malicious or criminal attack:

- Cyber incidents e.g., ransomware, malware, hacking, phishing, brute force access attempts.
- Social engineering/impersonation meaning inappropriate disclosure of personal information.
- Insider threats (employees) using valid credentials to access/disclose personal information outside the scope of their duties or permissions.

Does the agency need to notify the Privacy Commissioner?

Where a data breach is assessed as an eligible data breach, agencies must notify the Privacy Commissioner immediately, using the form on the IPC website.

Will I be notified if I am affected by an eligible data breach?

If an agency decides there has been an eligible data breach in relation to your personal information, it must notify you as soon as practicable about that breach. This means that an agency must notify you in writing and provide you with information about the eligible data breach, including the:

- actions the agency has taken or plans to take to control or mitigate the harm done to you
- steps you should consider taking following an eligible data breach
- information about how to seek an internal review of the agency's conduct or how to make a privacy complaint to the Privacy Commissioner.

How long after a data breach can I expect to be notified?

When an agency has reasonable grounds to suspect that an eligible data breach may have occurred, agencies must take a number of steps:

- Make all reasonable efforts to contain the breach.
- Assess whether there has been unauthorised access, disclosure or loss of personal information held by an agency within 30 days.
- Assess if there is a likelihood of serious harm to any affected individual within 30 days.
- Make all reasonable attempts to mitigate the harm done by the suspected breach.

If, after undertaking the above steps, an agency decides there has been an eligible data breach in relation to your personal information, it must notify you as soon as practicable about that breach.

What if the agency no longer has my details to notify me about a data breach?

Agencies have information sharing powers under the MNDB Scheme to enable them to request relevant personal information from another public sector agency. The information an agency can request is limited to information that is reasonably necessary to confirm the name and contact details of an individual affected by a data breach.

However, if the agency is unable to notify you directly it must publish a notification on its website and take reasonable steps to publicise the notification. The notification must remain on the agency's public notification register for at least 12 months.

Are there reasons why an agency might not notify me?

Yes. There are certain exemptions to the requirement that agencies notify affected individuals of a data breach. For example, if an agency acts quickly to mitigate a data breach, and because of this action the data breach is not likely to result in serious harm, there is no requirement to notify any affected individuals.

Will the agency provide me with any assistance after a notification?

The type of assistance or support an agency may provide following a notification will depend on the specific circumstances of the data breach. Examples may include:

- assistance to replace compromised government issued identity documents or credentials – such as a driver licence
- advice on how to protect your personal information
- providing links to additional support and counselling services.

What should I do if I receive a notification?

There are practical steps you can take to protect your personal information and reduce the risk that you will be harmed by a data breach. The types of actions you can take will depend on the circumstances of the data breach and the type of information involved. The notification you receive should recommend actions you can take in response to the type of breach identified in the notice.

If you want more information about the data breach or how to protect your personal information, you should contact the agency that sent you the notification.

Where can I find more information?

The Information and Privacy Commission (IPC) has further information and additional resources available via its website. Alternatively, you can contact the IPC using the contact details below.

For more information

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au

NOTE: The information in this fact sheet is to be used as a guide only. Legal advice should be sought in relation to individual circumstances.