Fact Sheet May 2023

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* for NSW public sector agencies ('agencies') in the event of an 'eligible data breach'.

From 28 November 2023, an agency must notify the affected individuals and the Privacy Commissioner when there has been an eligible data breach.

What is 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.

How can an eligible data breach occur?

What is unauthorised access and unauthorised disclosure?

Unauthorised access to personal information can occur when someone accesses information without permission. For example:

- a cyber attack on a database containing personal information, or
- an agency employee intentionally opens an electronic or paper file containing personal information when they do not have permission to access that information.

Unauthorised disclosure of personal information can occur if information is provided to or accessible by people outside the agency. This could be the result of:

- simple human or technical errors without malicious intent, for example where an agency accidentally publishes a data set containing personal information on its website
- a third party downloading data from an unsecured computer system or platform
- emails containing personal information being sent to the wrong person.

Personal information held by an agency can also be accidentally lost (including where it is stolen) in circumstances where it is likely to result in unauthorised access to or disclosure of that information. For example:

- a file containing personal information is accidently left in a public place
- a laptop containing the personal information of an agency's clients is stolen from the agency's office.

What is personal information?

Personal information is any information that identifies you and includes:

- a written record which may include your name, address and other details about you
- photographs, images, video or audio footage
- fingerprints, blood, or DNA samples.

Health information is a specific type of 'personal information' which may include information about your physical or mental health or disability.

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.

Who decides if you've suffered serious harm?

Whether the unauthorised access, disclosure or loss of your personal information is likely to result in serious harm to you, will be assessed by the agency as part of its response to the data breach. This requires an objective assessment determined from the viewpoint of a reasonable person.

An agency will consider the circumstances of the breach, how likely it is that the breach will cause harm, and the consequences and severity of that harm. In making this determination, the agency may consider the following:

- the types of personal information involved, for example, an email address is likely to be considered less likely to result in serious harm than credit card details
- the sensitivity of the personal information, for example, if it relates to a person's finances, health, or sexual orientation
- whether the personal information is or was protected by security measures such as encryption and therefore unlikely to be accessed or misused
- who has access to the personal information
- whether the person/s who accessed the personal information may have a malicious intent and whether they may be able to circumvent security measures
- the nature of the likely harm
- any other matter specified in the Privacy Commissioner's guidelines.

Your right to be notified of a breach of your personal information

When a data breach occurs, an agency must immediately make all reasonable efforts to contain the breach and try to reduce the likelihood that an individual will experience serious harm.

Agencies then have 30 days from the date they become aware of a possible data breach to assess whether that data breach is likely to result in serious harm. Whilst making this assessment, all reasonable attempts must be made to mitigate any harm already done.

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:

- 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 make a privacy complaint to the Privacy Commissioner.

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.

See the IPC Fact Sheet – Notification to affected individuals of a data breach for further information on the notification process and tips on how to protect your personal information.

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.

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.