Agency Update to existing Data Breach Notification

Agencies who have made a formal notification to the Privacy Commissioner using the approved webform are able to provide an update or new information regarding the breach to the IPC using this form.

You do not need to complete all fields within the form, only the content that you wish to update from your original notification. However, the form **must** include the case number that was provided to you by the IPC.

This is form is to be used for updates to existing data breach notifications only. To notify the IPC about a new data breach, please use the webform available via the IPC website.

Agency providing notification update

Agency name:

Agency address:

Telephone number:

Contact name:

Contact telephone:

Contact email:

Contact role/title in organisation:

IPC MNDB reference number:

Please ensure you include the IPC reference number in the above field that this update relates to. The reference number can be found in correspondence from the IPC and will begin with IPCYY/MNDB.

Type of personal information that was the subject of the breach

Select the option(s) that best apply:

- ☐ Contact details
- ☐ Identity documents/credentials
- ☐ Financial information
- ☐ Health information
- ☐ Under review (agency is still conducting its assessment at time of notification)
- ☐ Other sensitive information:

Description of eligible data breach

Discovery of the breach

When the data breach occurred:

When the data breach was discovered:

Where the data breach was discovered:

How the data breach was discovered:

By whom was the data breach discovered:

Amount of time the personal information was exposed:

Type of breach

Select the **type(s) of data breach** as applicable:

- ☐ Unauthorised disclosure
- ☐ Unauthorised access
- ☐ Loss of information
- ☐ Other:

How the breach occurred

Provide a brief explanation as to how the breach occurred:

Cause of breach

- ☐ Cyber Incident

If the breach was caused by a Cyber Incident, select the type of Cyber Incident below:

- ☐ Ransomware
- ☐ Malware
- ☐ Phishing (compromised credentials)
- ☐ Compromised credentials (method unknown)
- ☐ Hacking
- ☐ Brute Force Attack (compromised credential)
- ☐ Other:.

- ☐ Human Error
- ☐ Loss/theft of data/equipment
- ☐ System fault
- ☐ Other:

Remedial action taken to date (including description of action and when)

Remedial action to be taken

Notification to affected persons

Total number of individuals affected, or likely to be affected by the breach (provide best estimate if exact figure is unknown):

Total number of individuals notified of the breach at this stage:

Total number of individuals yet to be notified of the breach:

Provide details of how and when individuals were notified:

Have individuals been advised of the complaints and internal review procedures under the PPIP Act?

Recommendations made to affected individuals about the steps they should take to mitigate the effects of the breach

Estimated cost

Estimated cost of the breach to the agency:

Other bodies notified

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