Fact Sheet May 2023

Notification to affected individuals of a Data Breach

This fact sheet has been developed to help you understand NSW public sector agencies' notification obligations to you in the event of an eligible data breach.

The Mandatory Notification of Data Breach Scheme ('MNDB Scheme') was created by amendments to the *Privacy and Personal Information Protection Act 1998* (NSW) and **will commence on 28 November 2023**.

The MNDB Scheme requires that NSW public sector agencies ('agencies') notify affected individuals and the Privacy Commissioner when there has been an 'eligible data breach'.

You can find more information about the MNDB Scheme here.

When will you be notified about an eligible data breach?

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 an eligible data breach. Whilst making this assessment, all reasonable attempts must be made to mitigate any harm already done.

Once an agency decides there has been an eligible data breach, the agency must notify you as soon as practicable about that breach, with limited exceptions. This means that an agency must notify you as soon as it can, taking into consideration the facts and circumstances associated with the breach.

When would an agency not be required to notify an affected individual?

An agency will will not be required to notify you of an eligible data breach if:

- the breach involves more than one public sector agency and another agency involved in the same breach notifies you
- the notification would likely prejudice any investigation or legal proceedings
- the agency successfully contains the breach and limits the likelihood that you will experience serious harm
- there are overriding secrecy provisions in other laws that prohibit or regulate the use or disclosure of the relevant information
- notification would create a serious risk of harm to an individual's health or safety
- notification would worsen the agency's cybersecurity or lead to further data breaches.

In these circumstances the agency must still notify the Privacy Commissioner.

What must the notice include?

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

- the date the breach occurred
- a description of the breach, how the breach occurred and the type of breach that occurred
- the personal information that was the subject of the breach and the amount of time the information was disclosed for
- any actions taken or planned to ensure personal information is secure, or to control or mitigate the harm done to the individual
- recommendations about the steps the individual should take in response to the eligible data breach
- information about how to make a complaint or seek an interval review
- the name of the agency or agencies involved and their contact details.

If the agency is unable to notify or it is not reasonably practicable for any or all of the affected individuals to be notified, then the agency must publish a notification and take reasonable steps to publicise this notification. The notification must remain on the agency's public notification register for at least 12 months.

What assistance will the agency provide 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.

How to reduce your risk of harm if you are notified of an eligible data breach

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.

What can you do if you are unsatisifed with the agency's actions in relation to an eligible data breach?

If you are not satisifed with the way in which an agency has handled your personal information, you may ask that agency to conduct an 'internal review' of your privacy complaint.

An internal review is a fact-finding investigation into your privacy complaint. It gives the agency the opportunity to deal with and resolve your privacy issues.

The Privacy Commissioner has an oversight role in relation to internal reviews.

For more information about the complaints process and your right to internal review see the IPC Fact Sheet - Privacy complaints: Your review rights.

Where can you seek further assistance or information?

If you want more information about a specific data breach notification, contact the agency that sent you the notification.

For more information about creating strong passwords and multi-factor authentication, visit cyber.gov.au.

If your NSW Government proof of identity credentials have been stolen or fraudulently used you can contact ID Support NSW for assistance.

More information about the nature of identity theft and how to protect yourself can be found here, and by visiting IDCARE, NSW Police Force or the Australian Federal Police.

Identity theft can be a distressing experience. If you want to speak to a specialist identity and cyber security counsellor, you can contact IDCARE, Australia's national identity and cyber support service.

Tips to protect your personal information after a data breach notification

Change your online passwords

It is a good idea to change your password regularly, but after a data breach, it's especially important to change your passwords to something strong, secure, and unique. Do not use the same password for all your online accounts. You may want to consider using a password manager to help generate and keep track of your passwords.

Enable multi-factor authentication for your accounts

Multi-factor authentication makes it more difficult for someone else to gain access to your online accounts by asking you to confirm your identity with two or more methods such as a password and a security code sent to your mobile phone.

Take care with emails and text messages

Know how to spot a scam. If your name and contact details were involved in a data breach, you may receive a personalised email or text message. Don't open attachments or click on links in emails, texts or social media messages from strangers or if you are unsure whether the sender is genuine.

Take care on phone calls

Don't share your personal information over the phone unless you are certain about who you are sharing it with. If someone calls you and claims to be from an organisation or an agency, you can hang up and verify the information by checking their website and then calling the organisation or agency back.

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