Privacy Commissioner Update

Sonia Minutillo
Privacy Commissioner

information and
privacy commission
new south wales

Privacy Awareness Week NSW 2025

Privacy is

my business...

your business...

our business...

it's everyone's business

ipc

information and privacy commission

new south wales

16 – 22 June 2025

www.ipc.nsw.gov.au/PAWNSW2025

PAW Re-cap

Overview

- IPC PAW 2025 Event – *Privacy in the World of AI*
- Participated in OVIC Panel Discussion
- Released updated MNDB Self-assessment Tool
- Guidance – You have been told your information has been breached released
- Champion program

IPC PAW 2025 Event

Everyone’s Privacy in the World of AI

- The event discussed the evolving relationship between AI and privacy, with a key focus on AI use within NSW public sector agencies.
- Keynote speakers:
  - Dr Katharine Kemp, Associate Professor, UNSW
  - Sam Mackay, CISO, DCS
- Katharine’s presentation focused on AI in its evolving landscape and its broader intersection with human rights.
- Sam’s presentation offered an understanding about the opportunities and challenges the use of AI presents for cyber breach incidents, cyber management and response.

Speakers

Sonia Minutillo
NSW Privacy Commissioner
Information and Privacy Commission

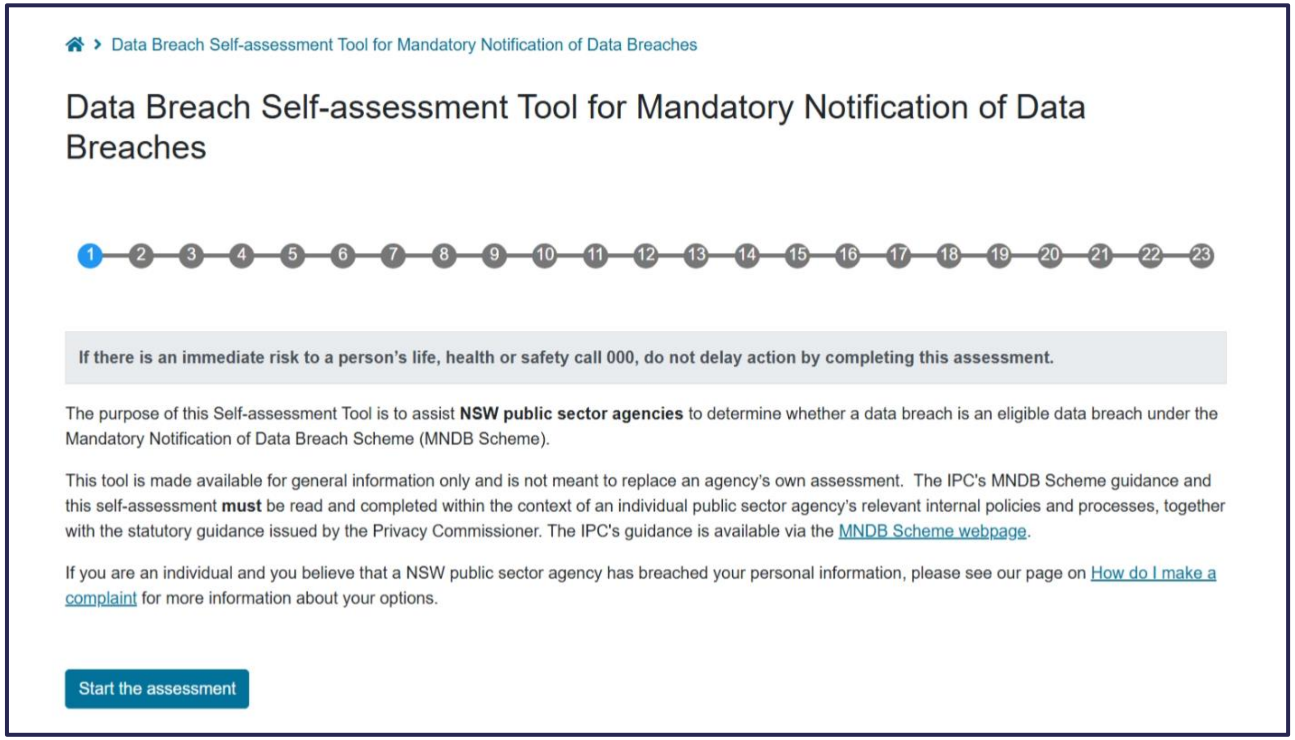
Dr Katharine Kemp
Associate Professor
Faculty of Law & Justice
University of New South Wales

Sam Mackay
Chief Information Security Officer
Department of Customer Service

New Resources

Updated MNDB Self-assessment Tool

- Updated Tool designed to assist public sector agencies to determine whether a data breach is an eligible data breach under the MNDB Scheme.



Data Breach Self-assessment Tool for Mandatory Notification of Data Breaches

If there is an immediate risk to a person's life, health or safety call 000, do not delay action by completing this assessment.

The purpose of this Self-assessment Tool is to assist **NSW public sector agencies** to determine whether a data breach is an eligible data breach under the Mandatory Notification of Data Breach Scheme (MNDB Scheme).

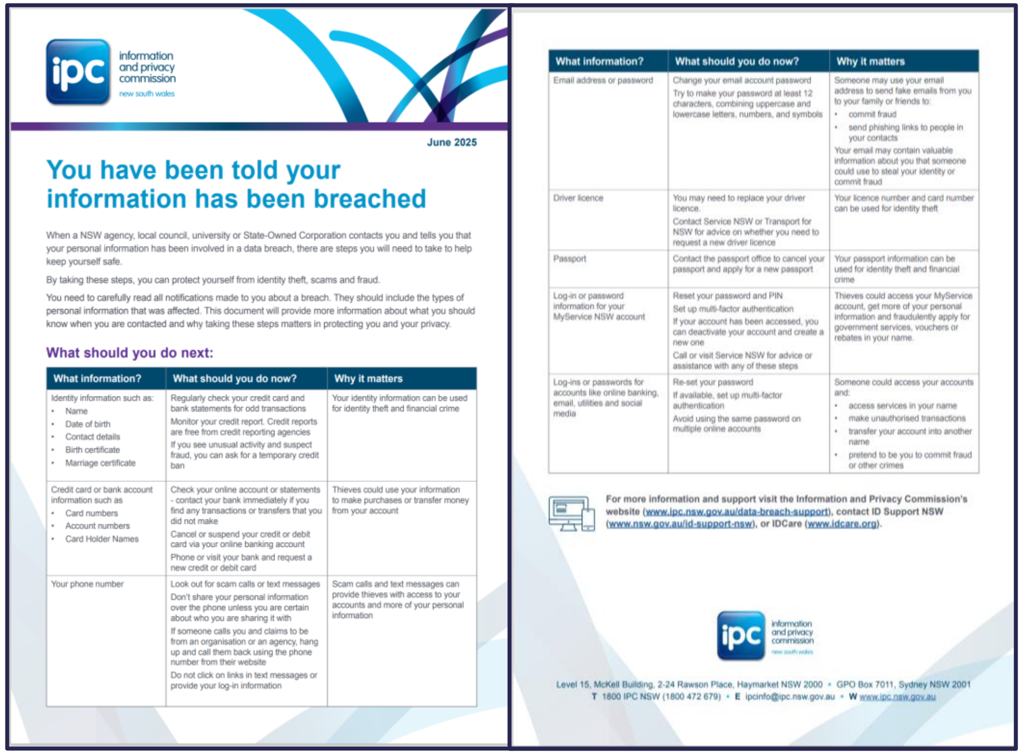
This tool is made available for general information only and is not meant to replace an agency's own assessment. The IPC's MNDB Scheme guidance and this self-assessment **must** be read and completed within the context of an individual public sector agency's relevant internal policies and processes, together with the statutory guidance issued by the Privacy Commissioner. The IPC's guidance is available via the MNDB Scheme webpage.

If you are an individual and you believe that a NSW public sector agency has breached your personal information, please see our page on How do I make a complaint for more information about your options.

New Resources

Guidance: You have been told your information has been breached

- Developed and released supporting guidance for individuals and for agencies to supply alongside their notifications to individuals affected by a data breach.



ipc information and privacy commission new south wales

June 2025

You have been told your information has been breached

When a NSW agency, local council, university or State-Owned Corporation contacts you and tells you that your personal information has been involved in a data breach, there are steps you will need to take to help keep yourself safe.

By taking these steps, you can protect yourself from identity theft, scams and fraud.

You need to carefully read all notifications made to you about a breach. They should include the types of personal information that was affected. This document will provide more information about what you should know when you are contacted and why taking these steps matters in protecting you and your privacy.

What should you do next:

What information?	What should you do now?	Why it matters
Identity information such as: • Name • Date of birth • Contact details • Birth certificate • Marriage certificate	Regularly check your credit card and bank statements for odd transactions Monitor your credit report. Credit reports are free from credit reporting agencies If you see unusual activity and suspect fraud, you can ask for a temporary credit ban	Your identity information can be used for identity theft and financial crime
Credit card or bank account information such as • Card numbers • Account numbers • Card Holder Names	Check your online account or statements - contact your bank immediately if you find any transactions or transfers that you did not make Cancel or suspend your credit or debit card via your online banking account Phone or visit your bank and request a new credit or debit card	Thieves could use your information to make purchases or transfer money from your account
Your phone number	Look out for scam calls or text messages 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, hang up and call them back using the phone number from their website Do not click on links in text messages or provide your log-in information	Scam calls and text messages can provide thieves with access to your accounts and more of your personal information
Email address or password	Change your email account password Try to make your password at least 12 characters, combining uppercase and lowercase letters, numbers, and symbols	Someone may use your email address to send fake emails from you to your family or friends to: • commit fraud • send phishing links to people in your contacts Your email may contain valuable information about you that someone could use to steal your identity or commit fraud
Driver licence	You may need to replace your driver licence. Contact Service NSW or Transport for NSW for advice on whether you need to request a new driver licence	Your licence number and card number can be used for identity theft
Passport	Contact the passport office to cancel your passport and apply for a new passport	Your passport information can be used for identity theft and financial crime
Log-in or password information for your MyService NSW account	Reset your password and PIN Set up multi-factor authentication If your account has been accessed, you can deactivate your account and create a new one Call or visit Service NSW for advice or assistance with any of these steps	Thieves could access your MyService account, get more of your personal information and fraudulently apply for government services, vouchers or rebates in your name.
Log-ins or passwords for accounts like online banking, email, utilities and social media	Re-set your password If available, set up multi-factor authentication Avoid using the same password on multiple online accounts	Someone could access your accounts and: • access services in your name • make unauthorised transactions • transfer your account into another name • pretend to be you to commit fraud or other crimes

For more information and support visit the Information and Privacy Commission's website (www.ipc.nsw.gov.au/data-breach-support), contact ID Support NSW (www.nsw.gov.au/id-support-nsw), or IDCare (www.idcare.org).

ipc information and privacy commission new south wales

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 IPC NSW (1800 472 679) • E ipcinfo@ipc.nsw.gov.au • W www.ipc.nsw.gov.au

Save the date!

Privacy Awareness Week 2026

4–10 May 2026

Smart Tech, Smarter Choices: Protecting Your Privacy in the Age of AI

MNDB Update

MNDB Spotlight series

- From the end of November, we will be commencing with a limited series of monthly MNDB Spotlights.
- These will be very short e-alerts with important reminders and updates about what is happening in this space. Make sure you are subscribed (via our website) and the **privacy area of interest** is selected to receive these.

MNDB Scheme Anniversary

- 28 November marks two years of operation of the MNDB Scheme. Along with the first MNDB Spotlight we will also be releasing some updated statistics.

Human Error

- From our data, we continue to see **human error** as the biggest contributor to breaches.
- Agencies are encouraged to remind staff and promote training to reduce this risk.

MNDB Takeaways

MNDB Guidelines

Guidelines on the exemption for investigations and legal proceedings under section 59T

- Thank you to those who provided feedback. Consultation closed on 18 November and consultation with the Attorney General and Minister of Customer Service and Digital Government will commence before publishing the Guidelines in early 2026.

Upcoming guidelines

- Use of the exemption under s59U where a public sector agency has taken action to mitigate the harm done by a breach.
- The guideline will assist agencies to assess when it may be appropriate to apply the exemption under s59U, what it means to “mitigate the harm” and the information that the agency should provide when notifying the Privacy Commissioner of its use of the exemption.

Follow up Data Breach Policy audit

- In October 2024, the Privacy Commissioner published an audit report on the level of compliance with the requirement to have a data breach policy by agencies.
- That audit report provided a base line understanding of the levels of compliance by agencies with their obligation to have a data breach policy publicly available.
- This subsequent audit, conducted twelve months after the initial report, is intended to assess ongoing compliance with these statutory obligations.
- This audit is scheduled to commence in January 2026.

Desktop Review of AI & ADM use in AIGs and PMPs

Report published on 17 November 2025 and looked at 119 agencies across the sector.

Privacy findings:

- **75%** of agencies **did not** reference the use of AI/ADM in their PMP
- The review suggests that most regulated agencies may **not yet formally recognise** the use of AI/ADM as part of their approach to privacy management, specifically about how PI is being used
- Agencies should ensure individuals are informed by documenting within their PMP when a decision that may significantly affect them is made using AI or ADM
- Agencies should review their data-handling practices that involve the use of AI/ADM to determine whether PI is involved and if applicable, update their PMP.

Questions on the Privacy Commissioner’s Update

- Please add any questions on the Privacy Commissioner’s Update using the Q&A function in teams.