Circular to Councils

Subject/title	Mandatory Notification of Data Breach Scheme Trends Report 2023-2024
Circular Details	Circular No 24-22 / 22 September 2024 / A935874
Previous Circular	*Circular 24-06 Privacy and the Mandatory Notification of Data Breach Scheme*
Who should read this	Councillors / General Managers / All council staff
Contact	Information and Privacy Commission / 1800 472 679
Action required	Information / Council to Implement

What's new or changing?

- The Acting Privacy Commissioner has released the first Mandatory Notification of Data Breach Scheme (MNDB Scheme) Trends Report (the Report) for November 2023 to June 2024.
- The Report provides preliminary insights into the operation of the MNDB Scheme following its commencement in November 2023.
- It draws from the statistical data from notifications received and the Information and Privacy Commission's (IPC) broader engagement with agencies.

What will this mean for council?

- The Report provides useful insights that councils may draw from to uplift their data breach preparedness and understanding.
- Council staff can be its most valuable asset in ensuring that personal information is safely and securely handled. Councils should build a pro-privacy culture, invest in training on end-to-end information management, document security and privacy awareness, and embed robust privacy practices into the design of systems and processes.

Key points

- The MNDB Scheme requires NSW public sector agencies, including councils, to notify the Privacy Commissioner and provide notifications to affected individuals in the event of an eligible data breach subject to the *Privacy and Personal Information Protection Act 1998*.
- The MNDB Scheme also requires the local government sector to satisfy other data management requirements, including to maintain an internal data breach incident register, and have a publicly accessible data breach policy.
- The Report shows that:
    - 78% of notifications from the local government sector were attributable to human error. Human error was the dominant cause of data breaches across all sectors
    - 22% of notifications for the local government sector involved a criminal or malicious attack
    - 11% of all notifications from the local government sector involved a systems fault
    - 7,054 individuals were affected by a council data breach.
- Cyber security for local government is an area requiring attention, having regard to the total number of cyber incidents notified during the reporting period.
- Data breach readiness is key to responding to data breaches in a timely, effective and efficient manner.
- Delegations should be made to officers with the appropriate level of seniority and necessary expertise to respond to a data breach.
- Notifications to affected individuals are most effective when they provide clear advice on what happened and what steps an individual should take. Provision of assistance should be meaningful and comprehensive. Councils should recognise that the nature of assistance may differ in individual circumstances.
- Councils should consider their data breach response plans and service contracts to ensure that they adequately address their data breach requirements under the MNDB Scheme.

Where to go for further information

- The Report can be accessed at MNDB Scheme Trends Report.
- For resources to support councils with their MNDB responsibilities, go to Mandatory Notification of Data Breach Scheme on the IPC's website.
- For more information, contact the IPC at 1800 472 679.

Danny Lester
A/Deputy Secretary
Office of Local Government