Consultation Document: Data Breach Policy Procedure

Requirements

Introduction

On 28 November 2023 amendments to the Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act) will come into effect. The amendments impact the responsibilities of agencies under the PPIP Act, and require agencies to provide notifications to affected individuals in the event of an ‘eligible data breach’ of their personal or health information by a NSW public sector agency or state-owned corporation subject to the PPIP Act.

An ‘eligible data breach’ occurs where:

1. there is an unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency or there is a loss of personal information held by a public sector agency in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information, and
2. a reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates.

The key changes to the PPIP Act include:

- creating a Mandatory Notification of Data Breach (MNDB) Scheme that will require public sector agencies bound by the PPIP Act to notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information likely to result in serious harm
- applying the PPIP Act to all NSW state-owned corporations that are not regulated by the Commonwealth Privacy Act 1988
- repealing s117C of the Fines Act 1996 to ensure that all NSW public sector agencies are regulated by the same mandatory notification scheme.

As an agency that falls under the PPIP Act, UNSW must in accordance with these obligations, revise and review its Data Breach Policy and the Data Breach Procedure. Authority to amend the Data Breach Policy and Data Breach Procedure was approved by the Chief Data and Insights Officer and the Head, Compliance and Controlled Entities Law.

---

1 ‘Serious harm’ is not defined in the legislation. The legislation provides a series of factors that an agency should consider when assessing the risk of serious harm occurring as a result of a data breach. They include the type of personal information accessed, disclosed or lost, and whether a combination of types of personal information might lead to increased risk; the level of sensitivity of the personal information accessed, disclosed or lost; the amount of time the information was exposed or accessible, including the amount of time information was exposed prior to the agency discovering the breach; the circumstances of the individuals affected and their vulnerability or susceptibility to harm (that is, if any individuals are at heightened risk of harm or have decreased capacity to protect themselves from harm) the circumstances in which the breach occurred, and actions taken by the agency to reduce the risk of harm following the breach.
The Mandatory Notification Data Breach Scheme

The purpose of the MNDB Scheme is ‘to ensure that both the Privacy Commissioner and affected individuals are notified when personal or health information is involved in a data breach, and there is a likelihood of serious harm to the affected individuals as a result. Notification allows people to take steps to reduce the risks of associated harms, for example by changing a password to online accounts, or monitoring for suspicious or fraudulent activity’. The MNDB Scheme is designed to ‘enhance transparency and accountability around privacy management within public sector agencies…[b]y holding agencies accountable and demonstrating that breaches of privacy are taken seriously and responded to appropriately, the MNDB Scheme builds trust in personal information handling across the NSW public sector’.

Under the MNDB Scheme agencies will have an obligation to:

- immediately make all reasonable efforts to contain a data breach and undertake an assessment within 30 days where there are reasonable grounds to suspect there may have been an eligible data breach. If the head of an agency is satisfied the assessment cannot reasonably be conducted within 30 days, they may approve an extension of time. The legislation provides a non-exhaustive list of factors an agency may consider when making an assessment
- during the assessment period, make all reasonable attempts to mitigate the harm done by the suspected breach, and
- decide whether a breach is an eligible data breach or there are reasonable grounds to believe the breach is an eligible data breach.

Where a data breach is assessed as an eligible data breach, agencies must:

- notify the Privacy Commissioner immediately using a prescribed form
- notify affected individuals as soon as practicable of the eligible data breach. (An agency is not required to notify individuals of an eligible data breach if an exemption applies. However, an agency must notify the Privacy Commissioner in the event of an eligible data breach.)

The obligations set out above require UNSW to have a robust Data Governance Framework and an effective data breach response plan to:

- establish clear roles and responsibilities for managing a data breach or suspected data breach
- review and update its Privacy Management Plan to include provisions relating to “the procedures and practices used by the agency to ensure compliance with the obligations and responsibilities set out in Part 6A for the mandatory notification of data breach scheme.” Agencies will be required to include in their plan reference to their data breach policy
- prepare and publish a Data Breach Policy that sets out how UNSW will respond to a data breach; the roles and responsibilities of UNSW staff in relation to managing a breach, and the steps UNSW will follow if a breach occurs
- review and update any relevant policies and procedures to comply with obligations under the MNDB Scheme
- establish and maintain an internal (incident) register of ‘eligible data breaches
- establish and maintain a public Notification Register on UNSW's website of any notifications made. The information recorded in the register must be publicly available for at least 12 months after the date of publication and include a link to the Privacy Commissioner and publication on the IPC website.

---

2 Guide – Mandatory Notification of Data Breach Scheme: Guide to managing data breaches in accordance with the PPIP Act.
3 Ibid.
4 The assessment must have regard to Guidelines (currently being developed) published by the IPC.
5 See Fact Sheet – Mandatory Notification of Data Breach Scheme: Exemptions from notification requirements, March 2023.