LSC LEGAL SERVICES COUNCIL | COMMISSIONER FOR UNIFORM LEGAL SERVICES REGULATION

Data Breach Policy

February 2024

LEGAL PROFESSION Uniform Law

Contents

Purpose

The purpose of this Policy is to set out the approach of the Legal Services Council (**Council**) and the Commissioner for Uniform Legal Services Regulation (**Commissioner**) to containing, assessing, managing, notifying, and reporting on eligible data breaches in accordance with the Mandatory Notification of Data Breach Scheme (**MNDB Scheme**) established by Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIP Act**).

This Policy has been prepared in accordance with section 59ZD of the PPIP Act and should be read in conjunction with the Privacy Management Plan (**PMP**) of the Council and Commissioner, which provides further information about how the Council and the Commissioner manage personal information in line with the PPIP Act.

Who we are

The Council and Commissioner are created by the Legal Profession Uniform Law (**Uniform Law**) which applies in New South Wales by virtue of the *Legal Profession Uniform Law Application Act 2014* (NSW) (**NSW Application Act**). The Commissioner is also the CEO of the Council.

The Uniform Law commenced operation in New South Wales and Victoria on 1 July 2015 and in Western Australia on 1 July 2022.

Application of the PPIP Act

The Council and Commissioner are subject to the PPIP Act by virtue of section 416 of the Uniform Law and section 6(1)(2) of the NSW Application Act, as modified by clause 5(1)(a) of the Legal Profession Uniform Regulations 2015 (**Uniform Law Regulations**). Clause 5(1)(a) of the Uniform Law Regulations provides that the Council and Commissioner "are taken to be public sector agencies" for the purposes of the PPIP Act. The Council and Commissioner are therefore subject to the requirement to prepare and implement a Data Breach Policy.

Definitions

Authorised User	Ongoing, temporary and casual staff, graduates, and volunteers, contracted service providers, consultants, members of the Council and the Council's Admissions Committee and Audit and Risk Committee, the Chief Executive Officer and Commissioner and any other authorised individuals who access IT systems, networks, information assets and office premises of the Council and Commissioner.
CEO	Chief Executive Officer of the Council. For the purpose of the PPIP Act, the Chief Executive Officer is the Council's agency head.[1] The CEO may delegate functions in relation to this policy, and where a delegation has been made, a reference to the CEO includes the CEO's delegate.[2]
Commissioner	Commissioner for Uniform Legal Services Regulation. The Commissioner is also the CEO of the Council and agency head.
Council	Refers to the members of the Legal Services Council, including the Chair.

[1] *Privacy and Personal Information Protection Act 1998* (NSW), s 59A.

[2] *Privacy and Personal Information Protection Act 1998* (NSW), s 59ZJ.

Eligible Data Breach	Has the same meaning it has in the PPIP Act.[3]
Health Information	Has the same meaning it has in the *Health Records and Information Privacy Act 2002* (NSW).
MNDB Scheme	Mandatory Notification of Data Breach Scheme, established in Part 6A of the PPIP Act.
Personal Information	Has the same meaning as it has in the PPIP Act and, for the purposes of the MNDB Scheme, includes Health Information.[4]

Scope

This Policy applies to all Authorised Users.

The Council and the Commissioner are responsible for information held if:
(a) the Council or the Commissioner are in possession or control of the information, or
(b) the information is contained in a State record in respect of which the Council or the Commissioner are responsible under the *State Records Act 1998* (NSW).[5]

Information in the hands of a service provider may still be "held" by an agency if the agency retains a legal or practical power to deal with the personal information – whether or not the agency physically possesses or owns the medium on which the personal information is stored.[6]

Policy details

The MNDB Scheme commenced on 28 November 2023 and requires all public sector agencies, including Council and Commissioner, to take various steps in relation to assessing, containing, managing, notifying, and reporting on Eligible Data Breaches. This Policy provides a framework for the Council and Commissioner's compliance with the MNDB Scheme.

What is a data breach

A data breach occurs when there is unauthorised access to or unauthorised disclosure of personal information or it is lost in circumstances where the loss is likely to result in unauthorised access or disclosure.

A data breach can be accidental or intentional and may arise as a consequence of a cyber-attack, inadvertent disclosure, over-provisioning of access to sensitive systems, or as a result of loss or theft of a physical device.

Types of data breaches include, but are not limited to:
1. loss or theft of a physical device containing information (for example, a work-issued portable computer, a USB stick, or a file)
2. an information repository being compromised or accessed without authorisation (for example, the sharing of user login details with a third party, hacking, or malware infection), or
3. an employee or contractor mistakenly providing personal information to an unauthorised person or entity (for example, by sending an email containing personal information to the wrong recipient).

---

[3] *Privacy and Personal Information Protection Act 1998* (NSW), s 59D.
[4] *Privacy and Personal Information Protection Act 1998* (NSW), ss 4, 59B.
[5] *Privacy and Personal Information Protection Act 1998* (NSW), s 59C.
[6] Information and Privacy Commission of NSW, *Introduction to the Mandatory Notification of Data Breach Scheme: Ensuring your agency is prepared* <https://www.ipc.nsw.gov.au/sites/default/files/2023-08/IPC_Presentation_by_PC_Samantha_Gavel_IPC_MNDB_Scheme_Webinar_17_August_2023.pdf>.

What is an Eligible Data Breach

The MNDB Scheme applies where an Eligible Data Breach has occurred.

A data breach will be an Eligible Data Breach if:

(a) there is unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency and 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, or

(b) personal information held by a public sector agency is lost in circumstances where

  (i) unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and

  (ii) if the unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to an individual to whom the information relates.[7]

Serious harm is not defined in the PPIP Act, however guidance from the NSW Privacy Commissioner (**Privacy Commissioner**) sets out that:

> Serious harm occurs where the harm arising from the eligible data breach has, or may, result in real and substantial detrimental effect to the individual. That is, the effect on the individual must be more than mere irritation, annoyance or inconvenience.
>
> Harm to an individual includes physical harm; economic, financial, or material harm; emotional or psychological harm; reputational harm; and other forms of serious harm that a reasonable person in the agency's position would identify as a possible outcome of the data breach.
>
> While mere irritation or annoyance does not in itself amount to serious harm, emotional or psychological impacts of a data breach can amount to serious harm if they are severe.[8]

Assessment of the likelihood of serious harm arising from a data breach is an objective test, to be determined from the perspective of a reasonable person and on the facts of the specific breach in question.[9] The phrase "likely to result" means that the risk of serious harm to an individual is more probable than not, rather than merely possible.[10] The NSW Privacy Commissioner's statutory guidelines will be considered in any assessment of a data breach.[11]

Preparation for a data breach

The Council and Commissioner are committed to the protection of all personal information they handle. This Policy outlines the steps the Council and the Commissioner have taken to prepare for, assess and manage any data breaches.

---

[7] *Privacy and Personal Information Protection Act 1998* (NSW), s 59D(1).

[8] Information and Privacy Commission of New South Wales, *Guidelines on the assessment of data breaches under Part 6A of the PPIP Act* <https://www.ipc.nsw.gov.au/guidelines-assessment-data-breaches-under-part-6a-ppip-act> [3.2].

[9] Information and Privacy Commission of New South Wales, *Guidelines on the assessment of data breaches under Part 6A of the PPIP Act* <https://www.ipc.nsw.gov.au/guidelines-assessment-data-breaches-under-part-6a-ppip-act> [3.3].

[10] Information and Privacy Commission of New South Wales, *Guidelines on the assessment of data breaches under Part 6A of the PPIP Act* <https://www.ipc.nsw.gov.au/guidelines-assessment-data-breaches-under-part-6a-ppip-act> [3.3].

[11] *Privacy and Personal Information Protection Act 1998* (NSW), s 59H(g).

Training and awareness

All Council staff are required to complete mandatory online training on the MNDB Scheme provided by the NSW Department of Communities and Justice (**NSW Department**).

Other Authorised Users may be encouraged to complete privacy and cyber security training where appropriate.

Process for identifying and reporting breaches

In the event of any data breach, all Authorised Users or concerned members of the public should contact the Privacy Contact Officer as soon as practicable once they become aware that a data breach has occurred, at lsc@legalservicescouncil.org.au.

In the event of a data breach relating to the NSW Department systems, NSW Department Legal and Information and Digital Services will be contacted.

Plan for managing data breaches

All data breaches will be managed in accordance with guidance provided by the Privacy Commissioner.

Contain data breaches

If a data breach occurs, Authorised Users are immediately required to take all reasonable steps to contain harm and prevent further loss or compromise of Personal Information and minimise potential harm to affected individuals. In the event of a data breach, Authorised Users should advise the CEO.

Assessment of a potential Eligible Data Breach

Where an Authorised User is aware that there are reasonable grounds to suspect there may have been an Eligible Data Breach, they must report the data breach to the CEO.[12] The CEO must immediately make all efforts to contain the data breach.[13]

The CEO must, within 30 days, carry out an assessment of whether the data breach is, or there are reasonable grounds to believe that the data breach is, an Eligible Data Breach.[14] If the CEO is satisfied that it is not reasonably possible to complete the assessment within 30 days, they may approve an extension of time to complete the assessment and give written notice of that extension to the Privacy Commissioner.[15]

During the assessment, the CEO must make all reasonable attempts to mitigate the harm done by the suspected breach.[16]

The CEO may direct one or more persons to carry out the assessment, but not a person who is reasonably suspected to have been involved in an action or omission that led to the data breach.[17] The person/s will advise the CEO whether the data breach is, or there are reasonable grounds to believe it is, an Eligible Data Breach.[18]

The following may be considered in assessing whether there has been an Eligible Data Breach:

---

[12] *Privacy and Personal Information Protection Act 1998* (NSW), s 59E(1).
[13] *Privacy and Personal Information Protection Act 1998* (NSW), s 59E(2)(a).
[14] *Privacy and Personal Information Protection Act 1998* (NSW), s 59E(2)(b).
[15] *Privacy and Personal Information Protection Act 1998* (NSW), s 59K(1). Section 59K provides additional guidance to the Commissioner in the event an extension of the assessment period has been approved.
[16] *Privacy and Personal Information Protection Act 1998* (NSW), s 59F.
[17] *Privacy and Personal Information Protection Act 1998* (NSW), s 59G.
[18] *Privacy and Personal Information Protection Act 1998* (NSW), s 59J(1).

- the types of Personal Information involved in the data breach
- the sensitivity of the Personal Information involved in the data breach
- whether the Personal Information is or was protected by security measures
- the persons to whom the unauthorised access to, or unauthorised disclosure of, the Personal Information involved in the data breach was, or could be, made or given and the likelihood that those persons
    - have or had the intention of causing harm, or
    - could or did circumvent security measures protecting the information
- the nature of the harm that has occurred, or may occur, and
- any other relevant matters, including those specified in guidelines issued by the Privacy Commissioner.[19]

Following the process of assessment, the CEO will make a decision as to whether the data breach is an Eligible Data Breach.[20]

Notifications and recordkeeping

The CEO will immediately notify the Privacy Commissioner of an Eligible Data Breach in the approved form.[21]

Where applicable and depending on the nature and severity of the data breach, the CEO may notify external assistance authorities or bodies, including but not limited to:

- Cyber Security NSW
- iCare
- IDCare
- ID Support NSW
- law enforcement agencies
- Privacy Commissioner, and
- other agencies affected by the data breach.

If the CEO decides that there has been an Eligible Data Breach or there are reasonable grounds to believe that the data breach is an Eligible Data Breach, they will consider exemptions to the notification of affected individuals, including any guidance issued by the Privacy Commissioner regarding such exemptions, and if none of the exemptions apply will notify affected individuals.[22]

In the event there is an Eligible Data Breach, the CEO will take all reasonably practicable steps to notify affected individuals.[23] In the event that the CEO is not able, or it is not reasonably practicable, to notify each affected individual, the CEO will prepare and publish a public notification register on the Council website.[24] The Council and Commissioner will also maintain an internal register of all Eligible Data Breaches.[25]

Once the incident is finalised and notifications are completed, the Council and the Commissioner will ensure that a "post incident review" is conducted to consider further measures to prevent such incidents from occurring again.

---

[19] *Privacy and Personal Information Protection Act 1998* (NSW), ss 59H, 59I.
[20] *Privacy and Personal Information Protection Act 1998* (NSW), s 59J(2).
[21] *Privacy and Personal Information Protection Act 1998* (NSW), ss 59M, 59Q.
[22] *Privacy and Personal Information Protection Act 1998* (NSW), ss 59N(1); 59S-59X. Section 59O specifies the information required to be included in the notification to the affected individuals.
[23] *Privacy and Personal Information Protection Act 1998* (NSW), ss 59N.
[24] *Privacy and Personal Information Protection Act 1998* (NSW), s 59P.
[25] *Privacy and Personal Information Protection Act 1998* (NSW), s 59ZE.

Roles and responsibilities

Who	Responsibility	How
CEO and Commissioner	The CEO and Commissioner is responsible for compliance with the requirements of the MNDB Scheme.	• Promote a culture that values privacy protection • Ensure that the appropriate policies, procedures and systems are in place to comply with the MNDB Scheme • Receive any reports of data breaches and lead assessment process • Receive advice from the Response Team and make decisions about whether an Eligible Data Breach has occurred • Ensure necessary notifications to individuals and the Privacy Commissioner are made in compliance with the requirements of the legislation • Liaise with other agencies about suspected data breaches as necessary • Delegate agency functions to members of staff as appropriate • Organise review and evaluation exercises following any Eligible Data Breach.
Staff	Report data breaches in accordance with this Policy	• Undertake mandatory privacy training • Report data breaches to the CEO as soon as practicable in accordance with this Policy • Assist in responding to any data breaches in accordance with this Policy
Privacy Contact Officer	Responsible for developing Data Breach Policy, promoting staff awareness of MNDB Scheme and privacy obligations.	• Assist the CEO with responding to any data breaches • Report data breaches relating to the NSW Department's systems

Who	Responsibility	How
	Maintain records of Eligible Data Breaches in the Eligible Data Breach Register and any Public Notification Register, where required	• Provide advice and guidance to stakeholders in the management of a data breach including on privacy issues, and the assessment and notification process • Develop, review and implement policy and procedures to facilitate compliance with MNDB Scheme and the PPIP Act. • Coordinate learning and other activities to promote staff awareness of MNDB Scheme and their obligations. • In the event of an Eligible Data Breach, ensure the breach is recorded in the relevant registers. • Coordinate provision of legal advice as required to support compliance with this Policy and the PPIP Act.
Person(s) appointed to undertake an assessment	Accountable for assessing a data breach	• Undertake activities to enable an assessment of a data breach and determine whether the data breach is an Eligible Data Breach. • Report to the CEO in a timely way, bearing in mind statutory timeframes
Council, Admissions Committee and Audit and Risk Committee	Be aware of and adhere to the terms of this Policy	• Be aware of the application of this policy when managing any personal information in their role as a member of the Council, Admissions Committee and/or the Audit and Risk Committee. • Report any suspected data breaches in accordance with this Policy.

Monitoring and review

In the event of an actual or suspected Eligible Data Breach, the Council and Commissioner will review what may have contributed to the breach and work to identify and remediate any processes or weaknesses in data handling. The CEO will be responsible for organising a post-response assessment of how the agency responded to the breach and the effectiveness of this Policy.

This Policy will be reviewed annually or earlier if required by changes to the relevant policy or legislation. The Privacy Contact Officer is responsible for monitoring and updating this Policy for review by the Audit and Risk Committee, the Council and Commissioner.

Version schedule

Revision	**Date**
Initial draft	8 February 2024
Document endorsed by the Council	29 February 2024

Date of review: February 2025