Ombudsman
New South Wales

Data breach policy

21 November 2023

Version 1

Document information

Document name:	Data breach policy	**Type of document:**	Policy
Status:	Active	**Version number:**	1
Date originally created:	21 November 2023	**File reference:**	ADM/2023/744
Superseded policy:	N/A	**Compliance:**	All staff
Related policies/ documents:	• Business Continuity Plan • Cyber Security Policy • Privacy and Information Management Framework	**Publication date:**	21 November 2023
Review date:	Every 3 years	**Policy owner:**	Chief Operating Officer
Distribution:	Public – this Policy must be publicly available on Ombudsman's website: *Privacy and Personal Information Protection Act 1998* s59ZD	**Feedback:**	Legal, Governance and Risk Branch

NSW Ombudsman
Level 24, 580 George Street
Sydney NSW 2000

Phone: (02) 9286 1000
Toll free (outside Sydney Metro Area): 1800 451 524

Website: ombo.nsw.gov.au
Email: info@ombo.nsw.gov.au

Contents

1. Purpose 1

2. Application 1

3. Related legislation and policies 1

4. Policy statement 1

5. Information to which the MNDB scheme applies 2

6. What is a data breach? 2

6.1 What is an 'eligible data breach'? 2

7. Data Breach Response Plan (DBRP) 3

7.1 Reporting actual or suspected data breaches 3

7.2 Triage breach reports 3

7.3 Contain the breach and minimise harm 3

7.4 Assess and manage the breach 4

7.5 Notify relevant stakeholders 4

8. Preventing a data breach 5

8.1 Strategies for preventing data breaches 5

8.2 Post-breach reviews and reporting on compliance 6

9. Records management 6

10. Breaches of the policy 6

11. Roles and responsibilities 6

11.1 All Ombudsman officers 6

11.2 Ombudsman 7

11.3 Chief Operating Officer 7

11.4 Data Breach Response Team 7

11.5 Manager Governance and Risk 7

12. Ombudsman approval 8

1. Purpose

This is the Ombudsman's Data Breach Policy (**DBP**).[1] It explains the Ombudsman Office's (**Office**) obligations and expectations relating to the Mandatory Notification of Data Breach (**MNDB**) scheme administered by the Privacy Commissioner.

The MNDB scheme is in Part 6A of the *Privacy and Personal Information Protection Act 1998* (**PPIPA**). All section numbers referred to in this Policy are sections of PPIPA unless the contrary is indicated.

2. Application

The policy applies to:

- statutory officers appointed under the *Ombudsman Act 1974*
- ongoing, temporary, and casual employees of the Office, and employees on secondment to the Office
- contractors and agency staff engaged to perform work for or on behalf of the Office
- students, interns, and volunteers engaged with the Office for the purposes of work experience or in any other capacity, and
- consultants and others the Office has a business relationship with whose engagement requires adherence to the policy.

In the policy these people are referred to as '**officers**', and the Ombudsman's Office is referred to as 'Office', 'we' or 'our'.

3. Related legislation and policies

Privacy and Personal Information Protection Act 1998 (**PPIPA**)

Cyber Security Policy

Privacy and Information Management Framework

Guide - Mandatory Notification of Data Breach Scheme: Guide to Preparing a Data Breach Policy May 2023 (**IPC**).

4. Policy statement

We deal with many individuals' personal information, as well as confidential and sensitive information about government and non-government entities.

Data breaches are a serious risk for our Office. A data breach may have serious consequences for the person or entity to whom the data relates, and result in a loss of trust and confidence in the Office.

[1] We are required to have a DBP: *Privacy and Personal Information Protection Act 1998* s59ZD.

Compliance with the MNDB scheme, and with this policy, is mandatory. A contravention of the MNDB scheme, or breach of this policy, may amount to misconduct.

The MNDB scheme does not affect our other obligations under PPIPA or our non-disclosure obligations under the Ombudsman Act.

This policy will be tested annually in conjunction with the Business Continuity Plan (**BCP**).

5. Information to which the MNDB scheme applies

The MNDB scheme applies to breaches of 'personal information'.

'Personal information', for the purposes of the MNDB scheme, means both:

1. 'personal information' as defined in section 4, meaning information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion, and
2. 'health information' as defined in section 6 of the *Health Records and Information Privacy Act 2002* (**HRIPA**), meaning personal information about an individual's physical or mental health or disability, or information connected to the provision of a health service.

6. What is a data breach?

Data breaches can take many forms. For example:

- a data breach may result from accidental loss or theft of data or information (including a hard copy)
- transfer of sensitive or confidential information to those who are not authorised to receive that information, e.g. inadvertently emailing personal information to the wrong recipient
- unauthorised access to data, information systems or a computing device, e.g. cyber attack
- unauthorised use of a system by any person.

A data breach can occur within the Office, between the Office and another agency, or in circumstances external to the Office, e.g. at a third party vendor that holds our information.

6.1 What is an 'eligible data breach'?

An 'eligible data breach' occurs where:

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

[2] s59D.

The term 'serious harm' is not defined in PPIPA. The following circumstances are examples of where the harm may be considered 'serious':

- the harm might be costly – physically, personally or financially
- the harm would require sustained remedial action
- the harm is difficult to remedy
- the breach involves a combination of types of information
- the information is sensitive and confidential.

7. Data Breach Response Plan (DBRP)

7.1 Reporting actual or suspected data breaches

Officers must report as soon as possible, and no later than one business day, any actual or suspected data breaches to the Governance and Risk unit at governance@ombo.nsw.gov.au using the Data Breach Assessment Checklist. This is a legislative requirement.[3]

Members of the public may also report any actual or suspected data breaches to info@ombo.nsw.gov.au.

7.2 Triage breach reports

Once a data breach report is received, the Manager Governance and Risk is responsible for evaluating the risks and recommending to the Ombudsman what should be done, which include undertaking an assessment.[4]

The Manager Governance and Risk may engage the assistance of the Data Breach Response Team (**DBRT**) during the response process. The DBRT will generally comprise the relevant branch Executive, Chief Information Officer, ICT Security & Service Desk Manager, and the Manager Governance and Risk. Additional officers may form part of the DBRT depending on the nature of the data breach.

7.3 Contain the breach and minimise harm

The Office has a responsibility to immediately make 'all reasonable efforts' to contain the breach.[5] We also have an obligation to minimise any harm done by the suspected breach.[6] These steps are legislative requirements that must be performed before and during, any assessment period, and may include:

- recovering the personal information
- asking a recipient to delete the information without reading it
- shutting down the system that has been breached or device that has been involved in the breach
- suspending the activity that led to the breach, and
- revoking or changing access codes or passwords.

---

3 s59E(2).

4 s59E

5 s59F.

6 s59F

If a third party is in possession of the data and declines to return it, it may be necessary for the Office to seek legal or other advice on what action can be taken to recover the data. When recovering data, we will take steps to ensure that copies have not been made by a third party or that, if they have, that all copies are recovered or steps have been taken to destroy them.

Contracted service providers involved in an Office data breach have a responsibility to identify and assist with remediation of breaches under their contracts, memoranda of understanding, or confidentiality agreements with us. The DBRT may liaise with external subject matter experts where appropriate.

7.4 Assess and manage the breach

Each data breach is different and must be assessed on a case-by-case basis.

Assessment should be carried out as promptly as possible and must be completed within **30 days** from the date the Office was made aware of the possible data breach, unless an extension is granted.[7]

The assessment will be carried out having regard to the factors set out in section 59H, as well as the Privacy Commissioner's Guideline.[8]

Once completed, the assessment will be given to the Ombudsman for decision whether an eligible data breach occurred.

If the assessment is unable to be reasonably conducted in 30 days, the Ombudsman or Ombudsman's delegate can extend this time. If this occurs, the Privacy Commissioner must be informed of the extension.[9]

7.5 Notify relevant stakeholders

We must notify relevant stakeholders if an eligible data breach has occurred. The Manager Governance and Risk will lead this process with the assistance of the DBRT.

Communications must be performed quickly and effectively and demonstrates the Office's commitment to open and transparent governance.

7.5.1 Privacy Commissioner

The Office must notify the Privacy Commissioner immediately through the IPC's Data breach notification to the Privacy Commissioner form.[10]

7.5.2 Affected individuals/organisations

We must notify affected individuals and organisations in writing as soon as practicable. Those notices will be similar to the notices provided to the Privacy Commissioner, 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

7 s59E(3).

8 ss59I, 59Z.

9 s59K(3).

10 s59M.

- 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 breach
- information about how to make a complaint or seek an internal review
- the name of the agency or agencies involved and their contact details.[11]

Where impacted individuals cannot be identified, or individual notification is not reasonably practicable we must issue a public notification.[12]

7.5.3 Others

We may need to notify or engage with other stakeholders. This will depend on the circumstances of the data breach and the categories of data involved. For example, if the data breach is a result of a cyber incident, we will have to inform Cyber Security NSW and the Australian Cyber Security Centre.

At times we will have notification obligations under both the MNDB scheme and under the Commonwealth Notifiable Data Breach (**NDB**) scheme. For example, a data breach that involves Tax File Numbers and is likely to result in serious harm would be reportable to both the Office of the Australian Information Commissioner (**OAIC**) under the Commonwealth NDB scheme, and the NSW Privacy Commissioner under the MNDB scheme.

7.5.4 Exemptions

In the following circumstances, we do not need to notify affected individuals of a breach where:

- notification is given by another affected agency
- notification will likely prejudice any investigation that could lead to the prosecution of an offence or legal proceedings
- mitigation steps taken mean serious harm is not likely to occur
- there are overriding secrecy provisions in other laws that prohibit or regulate the use or disclosure of the relevant information
- notification poses a serious risk of harm to an individual's health or safety
- notification would worsen the Office's cyber security or lead to further data breaches.[13]

8. Preventing a data breach

8.1 Strategies for preventing data breaches

Preventing a data breach is the best strategy.

Key measures the Office has in place to prevent and prepare for a data breach include:

- access control mechanisms to keep data within the ICT-managed infrastructure and restricted cloud service

[11] s59N(1).

[12] s59N(2).

[13] Division 4.

- monitoring services, e.g. dark web, web proxy control
- periodic audits and reviews of access controls
- confidentiality undertakings given by all officers
- not hold unnecessary data that could be the subject of a breach, e.g. not collect more personal information than is necessary and dispose of or archive records as soon as required per relevant requirements
- staff training and awareness, e.g. mandatory annual cyber security training, data breach or privacy.

8.2 Post-breach reviews and reporting on compliance

Where an eligible data breach occurs, the Manager Governance and Risk will perform a post-breach review to identify what contributed to the breach, how issues were addressed, and what short or long-term measures could be taken to prevent any recurrence.

The review will also consider whether changes are needed to policies and procedures, including an evaluation of the effectiveness of the DBRP.

The Manager Governance and Risk will prepare a report at least annually for the Executive summarising the Office's compliance with this policy.

9. Records management

The Governance and Risk unit is responsible for:

- receiving and processing reports of actual or suspected data breaches
- establishing and maintaining an internal register for eligible data breaches (section 59ZE)
- keeping complete records of eligible data breaches
- maintaining a public notification register on the Office's website for any notifications given under section 59N(2) for at least 12 months after date of publication (section 59P).

10. Breaches of the policy

Any suspected or actual non-compliance with this policy should be reported by officers to their manager in the first instance and copied to the Manager Governance and Risk.

Breaches will be evaluated by the Manager Governance and Risk for further action under the Office's Privacy and Information Management Framework and the Office's Code of Ethics and Conduct. A breach of this policy may amount to misconduct.

11. Roles and responsibilities

11.1 All Ombudsman officers

Officers are responsible for:

- understanding and abiding by the policy
- reporting suspected or actual data breaches to Governance and Risk, and
- undertaking applicable training when and as directed.

11.2 Ombudsman

The Ombudsman is responsible for:

- leading and promoting the policy within the Office, and
- approving assessments of eligible data breaches and notifying the Privacy Commissioner and other stakeholders where appropriate.

11.3 Chief Operating Officer

The Chief Operating Officer is responsible for:

- overseeing the implementation of systems and processes that support adherence to the policy, and
- through the Manager Governance and Risk, monitoring compliance with the policy.

11.4 Data Breach Response Team

The Data Breach Response Team is responsible for:

- liaising with external subject matter experts where appropriate, and
- supporting the Manager Governance and Risk in completing assessments, notifying relevant stakeholders, and performing post-breach reviews.

11.5 Manager Governance and Risk

The Manager Governance and Risk is responsible for:

- monitoring the implementation of and maintaining the policy in accordance with relevant compliance requirements
- receiving and triaging data breach reports expeditiously for the Ombudsman's review and approval
- escalating eligible data breaches to the Data Breach Response Team
- providing reports to the Executive regarding the Office's compliance with the policy
- maintaining the internal data breach register and the public notification register, and
- assisting in responding to enquiries made by the public and managing any complaints that may be received as a result of a data breach.

12. Ombudsman approval

Paul Miller
NSW Ombudsman