information and privacy commission
new south wales

Mandatory Notification of Data Breach Scheme: Guide to Preparing a Data Breach Policy

May 2023

Contents

1 Introduction 3
1.1 Who should use this Guide? 3
1.2 How to use this Guide 3
2 Background and terminology 3
2.1 What is an eligible data breach? 3
2.2 What is a DBP? 4
2.3 Why is a DBP necessary? 4
2.4 Why must agencies publish their DBP? 4
2.5 What if an agency is also required to notify the Commonwealth regulator? 4
3 What should be included in a DBP? 5
3.1 How the agency has prepared for a data breach 5
3.2 What a data breach is and how to identify one 6
3.3 Plan for managing data breaches 7
3.4 Roles and responsibilities 8
3.5 Record-keeping 9
3.6 Post-breach review and evaluation 9
Annexure A 10
Data Breach Policy quick checklist 10

1 Introduction

Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIP Act**) establishes the NSW Mandatory Notification of Data Breach (**MNDB**) scheme.

The MNDB Scheme requires every NSW public sector agency bound by the PPIP Act to notify the Privacy Commissioner and affected individuals of eligible data breaches.

Under the scheme, public sector agencies are required to prepare and publish a Data Breach Policy (**DBP**) for managing such breaches.

This Guide to Preparing a Data Breach Policy (**Guide**) is designed to assist NSW public sector agencies to understand the type of information expected to be included in a DBP under the MNDB scheme. It sets out the Privacy Commissioner's expectations in relation to what agencies should consider and document in their DBPs, to ensure compliance with section 59ZC of the PPIP Act.

More comprehensive guidance about your obligations under the MNDB Scheme is available on the Information and Privacy Commission's (IPC) website.[1]

1.1 Who should use this Guide?

All 'public sector agencies' as defined in section 3 of the PPIP Act are required to prepare and publish a DBP. This includes all NSW agencies and departments, statutory authorities, local councils, state-owned corporations, Ministers' offices, and some universities.

NSW public sector agencies should use this Guide to understand what should be included in a DBP.

1.2 How to use this Guide

This Guide is not prescriptive in nature and is not intended as a one-size-fits-all approach to managing data breaches. It is designed to be of general application to agencies of all sizes and in all sectors.

This Guide is not legal advice. It is published by the IPC to provide general information to help entities understand how to approach compliance with section 59ZD of the PPIP Act. Entities are encouraged to seek professional advice tailored to their own circumstances where required.

2 Background and terminology

2.1 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 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.

Breaches can occur between agencies, within an agency and external to an agency.

The MNDB scheme applies to breaches of 'personal information' as defined in section 4 of the PPIP Act, meaning information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

[1] See - https://www.ipc.nsw.gov.au/privacy/MNDB-scheme.

The scheme also applies to 'health information,' defined in section 6 of the *Health Records and Information Privacy Act 2002* (**HRIP Act**), covering personal information about an individual's physical or mental health, disability, and information connected to the provision of a health service.

The scheme does not apply to data breaches that do not involve personal information or health information, or to breaches that are not likely to result in serious harm to an individual. Where the scheme does not apply, agencies are not required to notify individuals or the Commissioner but should still take action to respond to the breach. Agencies may still provide voluntary notification to individuals where appropriate.

2.2 What is a DBP?

A DBP is a documented policy or plan setting out how an agency will respond to a data breach. Agencies are required to draft a DBP under section 59ZD of the PPIP Act. A DBP should establish the roles and responsibilities of agency staff in relation to managing a breach, and the steps the agency will follow when a breach occurs.

Agencies are required to ensure their DBP is publicly accessible.[2] In practice, this means agencies should publish their DBP on their website. Agencies should also consider including a link to the policy on their intranet or other central repository and should ensure staff know how to access the policy.

2.3 Why is a DBP necessary?

Depending on the size and nature of a data breach, the consequences for individuals can be significant. They can give rise to a range of actual or potential harm to individuals. These consequences can include financial fraud, identity theft, damage to reputation and even violence.

Data breaches can also have serious consequences for government agencies. A breach may create risk through the disclosure of sensitive information, or otherwise impact an agency's reputation, finances, interests, or operations. Ultimately, data breaches can lead to a loss of trust and confidence in an agency and the services it provides.

Responding quickly when a breach occurs can substantially reduce its impact on affected individuals, reduce the costs to agencies of dealing with a breach, and reduce the potential reputational damage that can result.

For these reasons, it is important that agencies have a documented and operationalised plan or framework for quickly and effectively responding to and managing data breaches.

2.4 Why must agencies publish their DBP?

Making a DBP publicly accessible enhances transparency and ensures agencies remain accountable for the way they respond to data breaches. It also enhances public trust and confidence in government and the services it provides.

2.5 What if an agency is also required to notify the Commonwealth regulator?

In some cases, agencies will have notification obligations under both the MNDB scheme and under the Commonwealth Notifiable Data Breach (**NDB**) scheme.

For example, a data breach at a NSW public sector agency 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.

[2] s59ZD(2).

The MNDB scheme has been designed to be consistent with and adopt, as far as possible, key features of the Commonwealth NDB scheme.[3] For example, the MNDB scheme adopts the same thresholds for assessing and notifying data breaches so that agencies can meet both requirements with a single process.

3 What should be included in a DBP?

A DBP should outline an agency's overall strategy for managing data breaches from start to finish. Having a clear and well-defined DBP enables agencies to:

- prepare for, evaluate, respond to and report on data breaches at the appropriate level and in a timely fashion
- mitigate potential harm to affected individuals and the agency itself
- meet compliance obligations under the PPIP Act.

Agencies should include at least the following in their DBPs:

1. How the agency has prepared for a data breach.
2. A clear description of what constitutes a breach.
3. Strategy for containing, assessing, and managing eligible data breaches.
4. Roles and responsibilities of staff members.
5. Record keeping requirements.
6. Post-breach review and evaluation.

3.1 How the agency has prepared for a data breach

A DBP should provide a high-level outline of the steps that an agency has taken to prepare for a data breach, and how these fit within the agency's broader systems, policies and procedures (such as cyber response, broader incident or emergency management processes, communications strategies and risk management frameworks). The DBP should cover key controls, systems and processes that the agency has in place to promptly identify actual or suspected data breaches, and to ensure they are effectively managed.

3.1.1 Training and awareness

Most data breaches, both in Australia and internationally, involve a human element (e.g., either through direct human error or cyber-attacks that rely on a human compromise). Building a well-trained and aware workforce is a strong front-line defence against breaches and other privacy risks.

An agency's DBP should outline its approach to staff training and awareness, (e.g., by enhancing staff awareness of privacy and cyber principles and current threat trends), in addition to training and awareness around identifying, responding to and managing data breaches.

3.1.2 Processes for identifying and reporting breaches

The quicker an agency can detect a data breach, the better the chance that it may be contained, and potential harms mitigated through prompt action.

An agency's DBP should clearly state how an actual or suspected data breach can be reported by staff or contractors within the agency, but also by any member of the public outside the agency.

[3] Data breach preparation and response (oaic.gov.au)

An agency's DBP could also outline the kinds of processes the agency has in place for identifying data breaches, though agencies should consider whether publishing details of specific controls places them at an additional risk. Other measures for identifying and preventing data breaches will depend on the size and sophistication of an agency and its security program, but could include:

- technical controls (such as Data Loss Prevention tools)
- monitoring services (such as dark web monitoring, or social media monitoring)
- audits and reviews
- staff training and awareness.

3.1.3 Appropriate provisions in contracts / other collaborations

Agencies are often required to outsource functions to external service providers or another agency (for example, for IT solutions). These relationships are usually covered by legally binding contracts, memorandums of understanding or non-disclosure agreements. To ensure agencies meet their obligations under the PPIP Act, these agreements often include provisions in relation to the management and notification of data breaches.

A DBP should outline the agency's approach to managing these collaborations and the contractual controls in place for ensuring external stakeholders comply with relevant privacy requirements. This could extend to third-party assurances made in relation to assisting the agency manage third-party data breaches (including in relation to notification and remediation).

3.1.4 Schedule for testing and updating the DBP

A DBP will only be effective if it is current, appropriately targeted and operationalised. As both the external threat environment, and agencies' internal makeup and functions, are continuously developing and changing, a DBP should be regularly reviewed to ensure it remains fit for purpose.

Agencies should develop a schedule for reviewing and updating their DBPs. This schedule should be set out in the DBP.

Regular testing of the data breach response process is the best way to ensure that all relevant staff understand their roles and responsibilities, and to check that the details of the response process (contact numbers, reporting lines, approval processes, etc.) are up to date. Testing the DBP could involve the development of a hypothetical or test incident and a review of the way agency personnel manage the event.

DBPs should be reviewed, tested and updated annually.

3.1.5 Alignment with other policies

Agencies should ensure that their DBP is aligned with existing policies, procedures, and capabilities. For example, an agency's DBP should align with their cyber security response plan and Privacy Management Plan, including cross references where relevant. If an agency has existing incident or crisis management processes, the DBP should be integrated into those processes as well.

Agencies should also ensure that their DBP is aligned to NSW government protocols on information security event reporting and incident response.

3.2 What a data breach is and how to identify one

To assist staff and others in identifying data breaches, a DBP should include a clear description of what a data breach is and how a data breach may occur. Consistent with the definition of 'eligible data breach' in section 59D of the PPIP Act, a DBP should note that a data breach may involve unauthorised access, unauthorised disclosure, or loss of personal information. A DBP should also be clear that each data breach should be assessed on a case-by-case basis and no template response can be applied in all cases.

Further, a DBP could note that a data breach may be deliberate or accidental and may occur by a range of different means or channels, including but not limited to, loss or theft of physical devices, misconfiguration or over-provisioning of access to sensitive systems, inadvertent disclosure, social engineering or hacking.

Agencies should also consider contextualising what a data breach is most likely to look like for internal agency staff by providing agency-relevant examples or scenarios. For example, an agency that handles a large amount of health information could provide examples or scenarios touching on the actual ways that health information is collected, used, stored, and disclosed in practice, reflecting any known risk factors for that agency.

Providing context-specific examples focusing on real life events can help agency personnel more quickly identify a future breach or high-risk activities and processes that could lead to a breach. It can also help agency staff identify how a breach might impact the agency, its functions and the people whose information it handles.

3.3 Plan for managing data breaches

A DBP should outline the steps an agency will take to respond to a reported, suspected or confirmed data breach.

3.3.1 Plan to triage, contain, assess, notify, prevent

To help ensure responses to data breaches are easily and quickly put into action, the DBP should clearly outline the agency's process for:

1. Initial assessment and triage of breach reports.
2. Containing a breach or suspected breach to minimise the possible damage.
3. Assessing or evaluating the information involved in the breach and the risks associated with the breach to determine next steps and implementing any additional actions identified to mitigate risks.
4. Notifying individuals / organisations affected by the breach, and the Privacy Commissioner.
5. Post incident review and preventative efforts, based on the type and seriousness of the breach.

3.3.2 Strategies for managing supplier and/or partner agency breaches

The DBP should outline strategies for managing data breaches that may occur at business-critical suppliers or partners that affect agency data. This could include documenting key contacts and clarifying roles in relation to assessment, remediation, notification to affected individuals and reporting to the IPC.

3.3.3 Other obligations including external engagement or reporting

Agencies may be required by contract or by other laws or administrative arrangements to take specific steps in response to a data breach. These may include taking specific containment or remediation steps, or engaging with or notifying external stakeholders (in addition to the Privacy Commissioner), where a data breach occurs.

Depending on the circumstances of the data breach and the categories of data involved, agencies may need to notify or engage with:

- NSW Police Force
- Department of Customer Service
- Cyber Security NSW
- The Office of the Australian Information Commissioner
- Australian Federal Police

- The Australian Taxation Office
- The Australian Digital Health Authority
- The Department of Health
- The Office of the Government Chief Information Security Officer
- The Australian Cyber Security Centre
- Any third-party organisations or agencies whose data may be affected
- Financial services providers
- Professional associations, regulatory bodies or insurers
- Foreign regulatory agencies.

An agency's DBP should outline the situations in which external notification or engagement is necessary and where there is a discretion, how that decision is made.

3.3.4 Clear communication strategy

The DBP should include a clear communication strategy that enables agency staff to quickly communicate with affected individuals and other stakeholders.

The strategy should outline:

- Responsibilities for implementing the communication strategy.
- How to determine when affected individuals or organisations must be notified.
- Key contacts for communications.
- How affected individuals will be contacted and managed.
- Responsibilities for consulting with external stakeholders.

3.3.5 Capability, expertise and resourcing

To be effective, the strategies outlined above must be able to be quickly and effectively implemented and actioned. However, this depends on having staff with the relevant skillsets available to deal with the breach. Where relevant, a DBP should outline the agency's strategy for ensuring:

- That it has access to requisite expertise and resourcing to respond effectively. This may involve engaging (in advance) an outsourced cyber incident response service provider.
- Where agency staff are called upon to assess a data breach or make an escalation decision, that those staff are trained and capable of adequately assessing the breach and its impact.

3.4 Roles and responsibilities

A DBP should establish clear roles and responsibilities for managing a data breach or suspected data breach, including:

- Clear guidance for agency heads, executive officers, privacy officers, staff and any other personnel of their roles and functions in relation to identifying, reporting and responding to a breach or suspected breach.
- The constitution of the response team, including:
    - The roles and functions within the team.

  - Subject matter expertise required in the team (this could include incident response specialists, legal, communications, cybersecurity, physical security, human resources, key agency operations staff, key outsourcing/relationship managers).
  - Delineation of responsibility for dealing with relevant elements of a breach within that team.
- Escalation procedures for staff, including how to immediately report a suspected breach and when line managers can handle a breach.
- The circumstances in which a breach should be escalated to the response team (typically based on severity or the level of response required).
- Responsibility for:
  - Escalation decisions at each level.
  - Determining reporting obligations including notification to the IPC, affected individuals, external stakeholders or other bodies.
  - Maintaining, testing and updating the DBP.
  - Record keeping (see below).
  - Post-breach review and evaluation (see below).

3.5 Record-keeping

Agencies should maintain appropriate records to provide evidence of how suspected breaches are managed, including those not escalated to the response team or notified to the Privacy Commissioner. Tracking data breaches allows organisations to monitor, analyse and review the type and severity of suspected breaches along with the effectiveness of the response methods. This may help agencies to identify and remedy weaknesses in security or processes that are prone to error. Agencies' approach to this documentation should be included in the DBP.

The DBP should also outline who has responsibility for this record keeping and how an agency approaches their record keeping obligations under the PPIP Act to:

- Maintain and publish (on their website) a public notification register for any notifications given under section 59N(2).[4]
- Establish and maintain an internal register for eligible data breaches.[5]

3.6 Post-breach review and evaluation

Understanding what went wrong, how issues were addressed and whether changes were needed to processes and procedures following a breach will mitigate future risks and are key to ensuring agencies continue to proactively manage data breaches in line with regulator and community expectations.

Agencies' DBPs should include:

- A strategy to identify and remediate any processes or weaknesses in data handing that may have contributed to the breach.
- A post-response assessment of how the agency responded to the breach and the effectiveness of the DBP.

[4] Section 59P

[5] Section 59ZE

Annexure A

Data Breach Policy quick checklist

Agencies can use this checklist to confirm their DBPs addresses relevant issues in line with IPC expectations.

Information to be included	Yes/No	Comments
Steps the agency has taken to prepare for a data breach		
What a data breach is and how staff can identify one		
The agency's plan for containing, assessing, and managing data breaches		
Processes that outline when and how individuals are notified		
Processes for responding to incidents that involve another entity		
Circumstances in which external engagement, including with law enforcement, regulators (such as the Privacy Commissioner), or other third parties may be necessary		
Requirements under agreements with third parties such as insurance policies or service agreements		
A clear communication strategy		
Clear escalation procedures and reporting lines for suspected data breaches		
Members of the data breach response team, including roles, reporting lines and responsibilities		
Details of any relevant external expertise or resources and when they should be engaged		
A record-keeping policy to ensure that breaches are documented		
A schedule for regular review and testing of the DBP		
A review process for identifying and addressing any root causes that contributed to the breach		
A system for a post-breach review and assessment of the data breach response and the effectiveness of the data breach policy		

Document information

Identifier/Title:	Guide to Preparing a Data Breach Policy
Business Unit:	IPC
Author:	Legal Counsel and Regulatory Advice
Approver:	Privacy Commissioner
Date of Effect:	1 May 2023
Next Review Date:	1 May 2025
EDRMS File Reference:	D23/012539/DJ
Key Words:	Mandatory notification of data breach, eligible data breach, preparation and response, policy