information and privacy commission
new south wales

Desktop Review of Data Breach Policy (DBP) Compliance Report

October 2024

Contents

1. Executive summary

Data breaches involving personal information have become increasingly prevalent in our community. The increasing frequency, complexity and the high impact of data breaches observed more generally highlight the significance and importance of preparedness and responsiveness. The passage of legislation in November 2022 to enact the Mandatory Notification of Data Breach Scheme (MNDB Scheme), with effect from November 2023, was a positive step in strengthening privacy protection in NSW and for data breach management.

NSW public sector agencies play a crucial role in safeguarding the personal and health information of the public that is accompanied by a responsibility to capably manage and respond to data breach incidents quickly and effectively. This is essential for maintaining the trust of the people whose data they hold and use.

The size, scale and impact of data breaches in recent years is well documented in the media. Data breaches can arise through error or by the actions of malicious actors. A data breach can give rise to a range of actual or potential harms to individuals, have serious consequences, and erode trust in the agency and the services and functions it provides.

Having a data breach policy (DBP) can help agencies minimise harm to individuals and the agency, be better prepared to respond to a data breach, and to improve the community's trust that they will appropriately handle a breach. The IPC's 2024 Community Attitudes survey[1] found increasing concern over data breaches, with most respondents agreeing that assistance should be provided after such events. This emphasises the need for NSW public sector agencies to communicate transparently and respond to breaches quickly and effectively if they occur.

Leading to the commencement of the MNDB Scheme, the IPC released an extensive suite of guidance materials[2] to support agencies in the transition period from the passage of the legislation to commencement. The IPC has promoted the MNDB Scheme to ensure agencies were prepared to respond to data breaches in line with their obligations under Part 6A of the *Privacy and Personal Information Protection Act 1998 (NSW)* (PPIP Act). These obligations included guidance for preparing a DBP – a legislative requirement.

Preparation and agency readiness under the MNDB Scheme starts with good governance, where a comprehensive DBP and Privacy Management Plan (PMP) are essential. A comprehensive DBP establishes the roles and responsibilities of agency staff in relation to managing a data breach, and the steps the agency will follow when a data breach occurs. Having a DBP and making it publicly accessible enhances transparency and builds trust in the agency's readiness.

A PMP identifies how the requirements of the PPIP Act and the *Health Records and Information Protection Privacy Act 2002* (HRIP Act) apply to the personal and health information that an agency manages in carrying out their functions and activities. There is a clear link in the understanding and identification of the personal and health information holdings of an agency in its PMP and its ability to sufficiently identify (and respond) when an eligible data breach has occurred for the purposes of the MNDB Scheme.

In this review a representative sample of 94 agencies across four sectors were assessed with respect to their DBP compliance and evidence of having revised their PMP as required by the MNDB Scheme.[3]

In summary, the examination found that out of the 94 sample agencies reviewed:

- 56% had a publicly available DBP published on their website

[1] IPC Community Attitudes Study Privacy Breaches March 2024 - https://www.ipc.nsw.gov.au/sites/default/files/2024-05/Community_Attitudes_Study_2024_Presentation_Privacy_Breaches.pdf

[2] MNDB Scheme resources - https://www.ipc.nsw.gov.au/MNDB-Scheme-resources

[3] Section 33(2)(c1) of the PPIP Act

- 44% did not have a publicly available DBP on their website
- 98% of those who had a publicly available DBP had an easily discovered DBP
- 27% had updated their PMP with information about procedures and practices to ensure compliance with the MNDB Scheme
- 56% did not have a PMP addressing the MNDB or provide any relevant information in relation to the MNDB Scheme

Recognising the point in time nature of this review, the level of agencies that did not have a publicly available DBP or had reviewed their PMP addressing the MNDM Scheme at the time is of concern and requiring of prompt attention.

The IPC will continue to work with agencies in building and supporting their maturity under the MNDB Scheme, including as it relates to the development of further resources and guidance.

2. Background

On 28 November 2023, the MNDB Scheme commenced in NSW. This followed a 12-month transition period that enabled agencies to prepare for the commencement of the scheme. The MNDB Scheme requires NSW public sector agencies to notify the Privacy Commissioner and provide notifications to affected individuals in the event of an eligible data breach of personal information.

An eligible data breach occurs where:

- *there is an unauthorised access to, or unauthorised disclosure of, personal information held by a public sector or a loss of personal information 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.*[4]

The MNDB Scheme requires that agencies have a Data Breach Policy (DBP) that outlines the procedures and practices they use to comply with their obligations under the scheme. In preparing the DBP, agencies were also required to amend their PMP to include the procedures and practices used by the agency to ensure its compliance with the obligations and responsibilities of the MNDB Scheme.[5]

A PMP equips agency staff with the necessary knowledge and skills to manage personal and health information appropriately. Together, the DBP and PMP serve as tools to inform all stakeholders about the steps to be taken by NSW public sector agencies when they are impacted by an eligible data breach. The DBP must also be made publicly available.[6]

Prior to this desktop review of DBP compliance, the Privacy Commissioner had published the findings from two previous reviews into PMP compliance. In her June 2023 report, while reiterating the importance of a current PMP, the Privacy Commissioner encouraged agencies to review their policies in preparation for the incoming MNDB Scheme.[7] In this regard agencies were already on notice of the need to undertake a review of their PMP in anticipation of the MNDB Scheme coming into effect.

A DBP both supports and prepares agencies in their response management and handling of a data breach. It enables the ability to respond quickly when a breach occurs and can reduce or minimise the impact on affected individuals, reduce the costs to agencies of dealing with a breach, and reduce the potential reputational damage that can result.

Agencies were assisted in meeting their responsibilities to prepare and publish a DBP through the Guide to preparing a data breach policy published by the Information and Privacy Commission (IPC) in advance of the Scheme commencing. This guidance from the IPC was one of the earlier pieces of guidance released and made available to support agencies with their efforts to prepare and publish a DBP.

The absence of a documented DBP can undermine the efforts of agencies in minimising the potential consequences of a data breach. All agencies had a period of 12 months to prepare and publish their DBP. Given the core role of a DBP for breach preparedness and responsiveness and the mandatory nature of the requirement to have a DBP, the Acting Privacy Commissioner undertook a review to assess the extent to which agencies had fulfilled their responsibilities under the MNDB Scheme.

---

[4] Section 59D of the PPIP Act

[5] Section 33(2)(c1) of the PPIP Act

[6] Section 59ZD of the PPIP Act

[7] Follow-up Desktop Audit of Privacy Management Plans (PMP) Report.

In early 2024, the Acting Privacy Commissioner signalled to agencies of the intended desktop review of compliance with the existence of DBP and PMP update as part of a Quarter 4 regulatory initiative.[8]

3. Purpose

Under the MNDB Scheme, all agencies are required to have a DBP that outlines the procedures and practices they use to comply with their obligations under the Scheme. Additionally, agencies should have an updated PMP that demonstrates how they embed privacy into their culture and operations. Notably since the introduction of the MNDB Scheme, PMPs should also include the procedures and practices to ensure compliance with the Scheme.

Having a documented and operationalised plan or framework for quickly and effectively responding to and managing data breaches in the form of a DBP is not only a mandatory legislative requirement but also an important component of an agency's robust privacy governance framework.

Given the mandatory requirements and the function and role that a DBP plays, the purpose of this desktop review is to:

1. examine compliance with the requirement to have a DBP following the commencement of the MNDB Scheme,
2. assess ease of discovery of a DBP,
3. consider the extent to which PMPs have been updated, and
4. make recommendations to improve and support broader sector compliance.

The outcomes from this review of compliance will continue to inform ongoing and future regulatory and educational activities to support agencies in enhancing their privacy maturity and resilience and ensure overall compliance with the MNDB Scheme.

4. Methodology and audit sample

This review was undertaken with reference to the Privacy Commissioner's functions under section 36 of the PPIP Act.

In reviewing the level of compliance by agencies in having a DBP together with updating their PMP's, a broad assessment of agencies across the different sector categories was undertaken.

A representative sample of 94 agencies were selected for inclusion across the sectors. These agencies may be categorised by their agency types and included:

- NSW Government agencies (including all portfolio departments, and a random selection of executive and other separate agencies)
- State-owned Corporations (all)
- Universities (all)
- Councils.

[8] See https://www.ipc.nsw.gov.au/privacy/ppip-hrip-compliance-reports/ipc-privacy-proactive-regulatory-initiatives-program

Table 1 illustrates the number of agencies that were assessed as part of this audit based on their agency type:

Agency type	Number of agencies assessed
NSW Government agencies	36
State-owned Corporations	8
Universities	10
Councils	40
Total	***94***

Table 1. Breakdown of selected agencies by agency type

4.1 Limitations

As the focus of this review is on sector-wide compliance rather than compliance by an individual agency, it was determined that a desktop review would be the most appropriate and efficient means to measure the compliance levels across the sectors. This approach provides the IPC with an ability to establish a baseline understanding of the compliance rates across the sectors.

The scope of this review was limited to a desktop review of the information that was available on the websites of the selected agencies during May 2024.

Given the nature of a desktop assessment more generally, this review is constrained by various factors, including:

- the requirement for independent remote assessment,
- the non-inquisitorial nature of the review, which precludes the seeking of clarification from the selected agencies in relation to the data, and
- the limited focus of assessing the existence, accessibility, and relevancy of PMPs.

Further, given its non-inquisitorial nature, this desktop review does not assess the completeness, comprehensiveness or accuracy of the information contained in the DBP or PMP that were considered as part of the review.

Where an agency was assessed as non-compliant with respect to the legislative requirement to publish a publicly available DBP, it was not possible to assess that agency in relation to the second criterion regarding the ease of discovery of the policy.

The IPC acknowledges that this audit reflects a point in time snapshot of compliance across the four sectors, and that agency updates may have been pending during this review or thereafter, and therefore are not reflected in the findings or observations made in this desktop audit.

4.2 Assessment criteria

The review examined and considered the following assessment criteria reflective of the legislative requirements on agencies:

Assessment Criteria	
Existence of the DBP	Is the Data Breach Policy published on the agency's website?
Ease of discovery of the DBP	Is the Data Breach Policy easily discoverable on the agency's website?
Relevancy of the PMP	Does the agency's Privacy Management Plan include information about procedures and practices to ensure compliance with MNDB obligations?

Table 2. Assessment criteria

4.3 Conduct of the analysis

This desktop review was conducted in May 2024. In collating and analysing the data, the IPC reviewed each agency's website to ascertain:

- whether the agency's DBP was published on the agency's website
- the ease with which the DBP was discoverable on the agency's website
- the extent to which the agency's PMP had been updated.

The findings of this review are presented in two parts:

- assessment against the criteria set out above in *Table 2*; and
- specific tables, findings, observations, and recommendations to assist agencies in complying with legislated requirements concerning the publishing of MNDB Scheme related policies and procedures.

IPC officers who carried out the audit reviewed the websites for each agency selected for inclusion in the review to examine the agency's compliance with their PPIP Act obligations in relation to the MNDB Scheme across the three audit criteria.

In undertaking the review, the IPC recorded and retained data for each agency. However, no commentary is provided on individual agency performance, as the findings and recommendations made are applicable generally.

5. Findings and observations

5.1 Whether agencies have a Data Breach Policy published on the agency's website?

Criterion		Result
1	Existence of the DBP - Is the Data Breach Policy published on the agency website?	• 56% (53) of agencies are compliant by having a publicly available DBP published on their website • 44% (41) of agencies are non-compliant

Comments, findings and recommendations

Comments: Agencies are required to prepare and publish a DBP. The existence of a DBP supports stakeholders to understand how an agency will respond in the event of a data breach and provides confidence that an agency has a documented plan for the management of such an event.

Failure to have a DBP and make it publicly available undermines public trust and confidence in agencies and in their preparedness and ability to respond to data breaches. A comprehensive DBP can help limit the consequences of a breach, including the risk of harm to the individuals whose privacy has been breached. An effective and timely response to a data breach can help preserve the community's confidence in the agency.

Findings:

Figure 1 demonstrates that over half of the agencies were in compliance with the essential requirement to have a publicly available data breach policy.

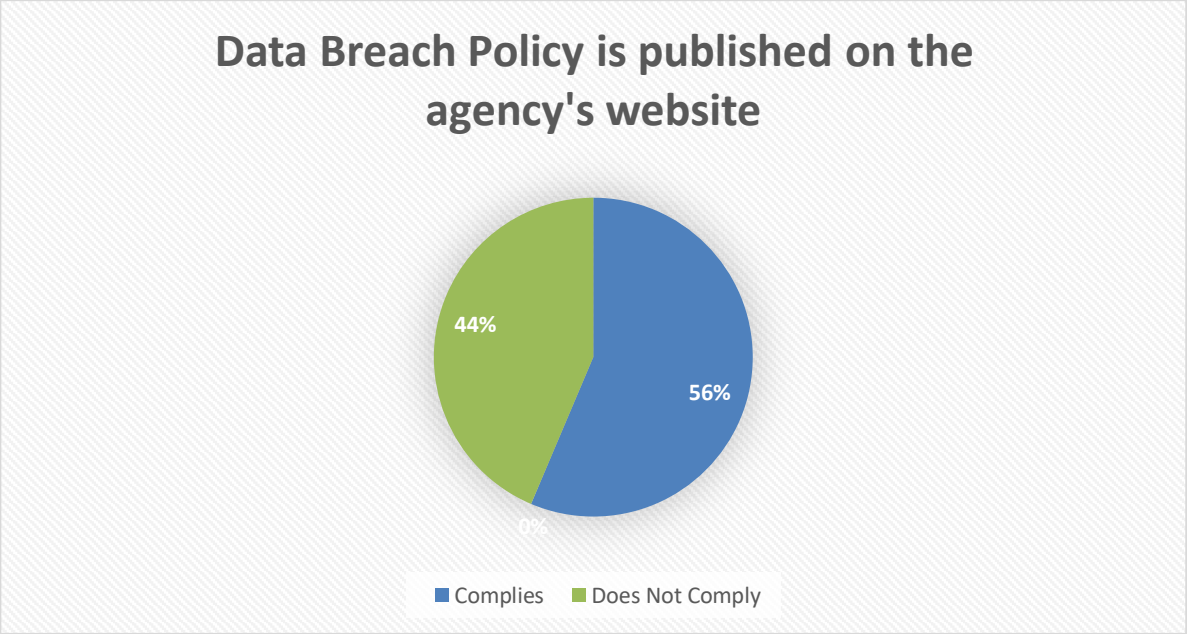

Figure 1. provides overall compliance rates with section 59ZD of the PPIP Act to make a DBP publicly available

Comments, findings and recommendations

Figure 1 illustrates that 44% of agencies did not have a publicly available, published DBP or one that could be located. Accordingly, these agencies were assessed as non-compliant for the purposes of this review. This represents a significant proportion of agencies that despite the time afforded to prepare for the commencement of the MNDB Scheme have not taken the necessary steps to fulfill a core legislative requirement of the Scheme – to develop and publish a DBP. It demonstrates a lack of appreciation for the importance of preparedness if a data beach was to occur.

Agencies that did not have a publicly available DBP were found to be concentrated in the Council and State-Owned Corporations (SOCs) sectors. In one case it appears that the DBP was only available after making a request for access. Any condition or limitation around the ability to access the DBP such as by having to make a request is non-compliant with the requirement to publish and make the DBP available on the agency website.

In another case, it was observed that the DBP appeared to be in draft form and not final despite the period available to prepare for the Scheme. This review also observed that in some cases the DBP was embedded in other documents such as within a Privacy Policy, a PMP, or a broader Information Technology Policy. The PPIP Act clearly specifies the requirement of agencies to prepare and publish a DBP which is to be made publicly available. Inclusion of a DBP within another policy does not align with the legislative intent and requirement of section 59ZD.

Figure 2 provides a breakdown of compliance to publish a DBP under section 59ZD of the PPIP Act by agency type.

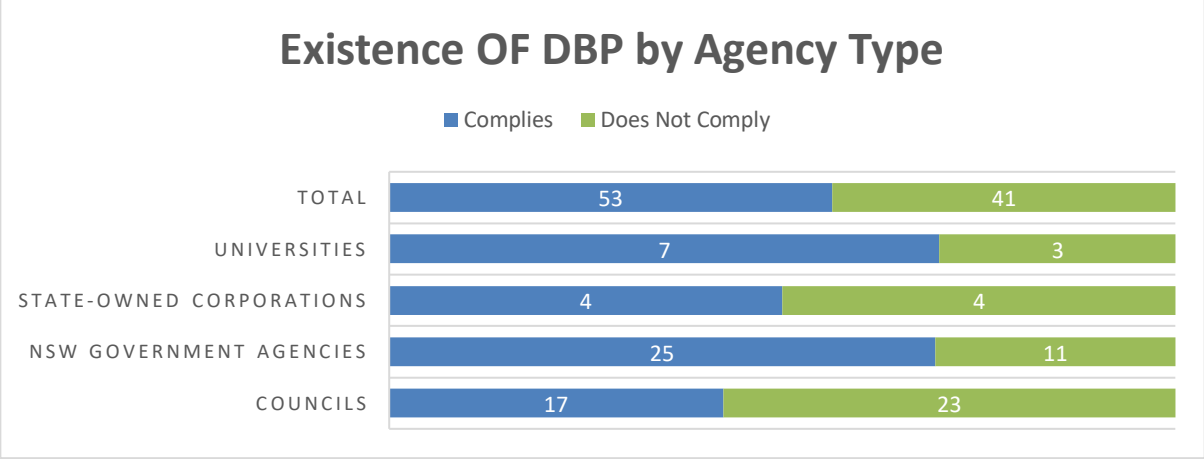

Figure 2. Publicly Available DBP Compliance rates by sector.

The majority of non-compliance with the measure of existence of a DBP was found to be concentrated in the Council and SOCs sectors. Over half of the Councils reviewed (57.5%) did not have a published DBP, followed by 50% of SOCs. Although the non-compliance was higher in these sectors, the review found levels of non-compliance across all sectors.
SOCs are newly regulated entities under the PPIP Act. Throughout the lead up to the MNDB Scheme, the IPC engaged directly with these newly regulated entities to support their overall compliance. With only 50% at the time of the review having a published DBP, this review has identified the need for the IPC to continue its engagement with SOCs.

The requirement to publish a DBP is a clear and specific obligation for agencies. Noncompliance with this obligation by agencies is undesirable. All agencies must ensure that they create, maintain, and publish a DBP to their website consistent with their legislative requirement.

Comments, findings and recommendations
In advance of the commencement of the MNDB Scheme, the IPC released guidance on DBPs, providing useful information about what should be included. Although this review did not look at the particular contents of any DBP, in preparing their DBP agencies should review the guidance to maximise the value and benefit that can be derived from its DBP. **Recommendation 1:** Agencies should ensure that they comply with the obligation to have a DBP and ensure that the DBP is published to the agency website. Agencies that have not published a DBP to date, should take immediate steps to publish their DBP in accordance with section 59ZD of the PPIP Act. **Recommendation 2:** Agencies should ensure that they make their DBP publicly available on their website without limitations or conditions on ease of access. **Recommendation 3:** All agencies should ensure that they have a distinguishable DBP published in final form. **Recommendation 4:** Agencies should consult the IPC Guide: Mandatory Notification of Data Breach Scheme: Guide to preparing a Data Breach Policy in developing their DBP.

5.2 Whether an agency's Data Breach Policy was easily discoverable on an agency's website.

Criterion		Result
1	Is the Data Breach Policy easily discoverable on the agency's website?	• 98% (52) of agencies with a DBP complied having an easily discovered DBP publicly available on their respective websites • 2% (1) (partially complied) of agencies had a discoverable DBP that required some effort to discover, requiring between 6–10page navigations to discover

Comments, findings and recommendations
Comments: The requirement to have a DBP is accompanied by a requirement that the DBP is to then also be publicly available. This requirement is explicitly provided for at section 59ZD of the PPIP Act. In practice, this is achieved by agencies publishing the DBP on their website. Making a DBP publicly available both contributes to and enhances transparency and accountability for the way that an agency responds to a data breach. Easy discovery of a DBP assists in strengthening confidence, general trust and accountability with the public in relation to agencies' management of data breaches and empowers the public to independently inform themselves without necessitating a need to make a request for the information from the agency. However, if the DBP is difficult to locate or source on an agency's website, it has the effect of diminishing its value and purpose. Agency compliance with the accessibility of their DBP was assessed on whether the DBP could be easily located by navigating from the agency's home page with a minimum of click throughs and in a straightforward manner.

Comments, findings and recommendations

Findings:

Of the 53 agencies complying with Criterion 1, each agency was assessed on how easy it was to conduct a search of their website to discover a DBP. The level of compliance with the accessibility was found to be high at 98%, however this level of compliance, while welcome, needs to be understood in a context in which 44% of the sample cohort did not have a published DBP at all.

Several agency DBPs were discoverable via subpages within the NSW.gov domain which indexed results of multiple DBPs across agencies under the domain. Where possible a DBP under the NSW.gov domain should be titled to include the name of the agency it relates to, ensuring accurate search results return for customers to easily locate the appropriate DBP related to their search.

The average page navigations required to discover an agency's DBP was 1 to 2 clicks, starting the search from the use of an agency's website search tool. In those cases where the DBPs were not discovered via a search tool, the ability to discover the DBP through page navigation clicks followed a logical sequence, where DBPs are generally discovered on an agency's' 'privacy', 'governance' or 'policies' webpage. Website search tools should ensure the DBP is easily discoverable from the search results across a range of key words.

In a small number of cases, the review observed that agencies placed DBP content within their PMP documents. While section 33(c)(1) requires that a PMP is updated to reflect the procedures and practices used by the agency to ensure compliance with the MNDB Scheme, a DBP is a distinct policy with a specific purpose that is required by section 59ZD of the PPIP Act. That purpose is to outline an agency's overall strategy for managing data breaches from start to finish. A DBP focuses on the operationalisation of agency data breach readiness and provides a road map for the staff response to a breach, whereas the PMP is directed to how an agency proposes to comply with the information protection principles, among other aspects.

Figure 3 provides a breakdown of the ease of discovery of agencies' publicly available DBPs.

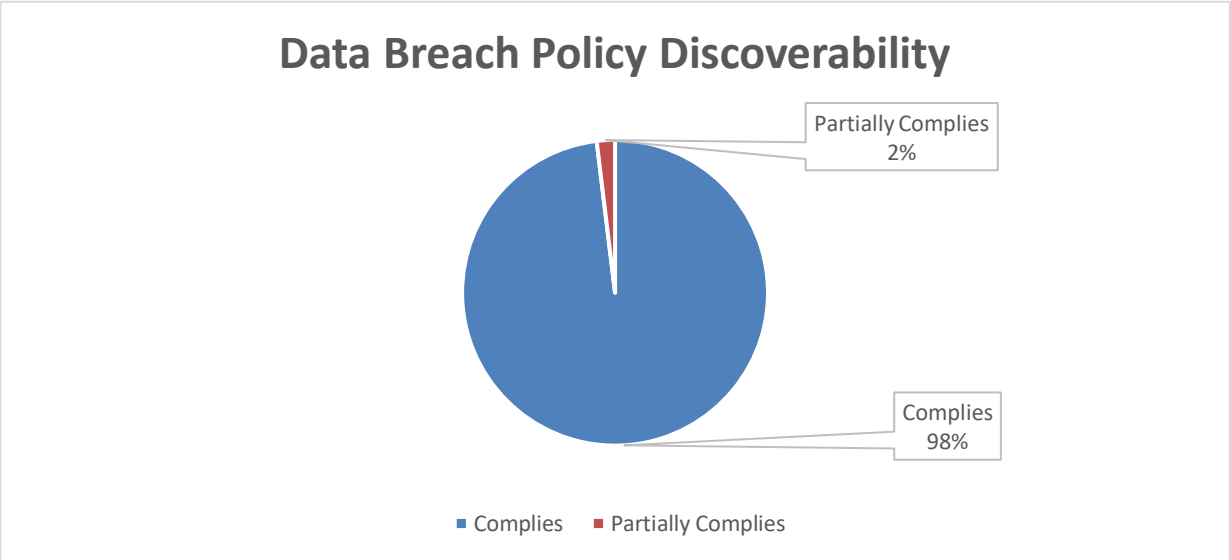

Figure 3. DBP Compliance rates by ease of discovery. Whether publicly available published Data Breach Policies were easily discovered on Agency websites.

Recommendation 5: All agencies should review their publication of their DBP to their website to ensure its prominence, ease of searchability and access.

5.3 Whether the agency's Privacy Management Plan includes MNDB provisions?

Criterion		Result
1	Does the agency's Privacy Management Plan include information about procedures and practices to ensure compliance with MNDB obligations?	• 27% (22) of agencies were assessed as compliant by having a PMP with information about procedures and practices to ensure compliance with the MNDB Scheme • 17% (14) of agencies were assessed as partially compliant in only briefly mentioning the MNDB Scheme or providing limited information in relation to the procedures and practices to ensure compliance with the Scheme • 56% (45) of agencies were assessed as non-compliant in having a PMP that did not address the MNDB Scheme or provide any relevant information in relation to the Scheme • 14% (13) of the agencies audited did not have a locatable PMP.

Comments, findings and recommendations

Comments:

Section 33 of the PPIP Act, requires NSW public sector agencies to have a PMP. A PMP is a strategic planning document in which each public sector agency describes the measures it proposes to take to ensure that it complies with the PPIP Act and the HRIP Act.

A PMP identifies and documents safeguards of the personal and health information holdings of an agency while the DBP guides the response of the agency to a data breach to ensure the personal and health information is secured and affected people are notified to minimise harm.

A PMP, like a DBP should also be made publicly available on the agency's website and made available in other ways on request. Additionally, section 33 of the PPIP Act further provides that agencies must provide a copy of their PMP to the Privacy Commissioner as soon as practicable after preparation or amendment.

To assist agencies, the IPC has published privacy resources and guidance that are specifically tailored for the formulation of NSW public sector agency PMPs. As part of the MNDB Scheme, agencies were required to develop DBP, and in turn, were required to amend their PMPs to include information about the procedures and practices used by the agency to ensure their compliance with the MNDB Scheme. This requirement is explicitly provided for by section 33(2)(c1) of the PPIP Act.

As agencies published their DBP, this should have resulted in a consequential review and amendment of the respective agency PMP on or around the same time. Ensuring that both the DBP and PMP are complimentary provides a holistic picture of the agency's understanding and approach for both managing personal information and its responsibilities under the MNDB Scheme.

Comments, findings and recommendations

Findings:

This review observed that the majority of agencies were observed as non-compliant in fulfilling the requirements of section of 33 in amending their PMP's. As demonstrated in *Figure 5*, although noncompliance was representative across all sectors, it was particularly noted in the Council sector with the highest proportion of noncompliance overall, followed by the University and SOCs sectors. Only a small number of agencies were assessed as having met the requirement.

Where agencies were assessed as 'Partially Complies' this was primarily due to their PMP only mentioning the MNDB Scheme and not providing detail on any practices or procedures.

Setting out the key information in a PMP related to an agency's obligation under the MNDB Scheme provides the customer with a cohesive link between the DBP policy in the broader context of the privacy strategy.

Significantly, the inability to assess the compliance of fourteen agencies due to an inability to locate their PMP, reinforces the need to ensure the ease of accessibility of them, if they are to serve their intended purpose.

A detailed consideration of compliance with the obligation of the agency to have a PMP was outside of the scope of this review. However, it is notable that the Privacy Commissioner has undertaken two previous reviews into PMP compliance, both of which observed levels of compliance that were worthy of attention in the Council sector.

Figure 4 provides a breakdown of agency compliance with updating their PMP to include information about procedures and practices to ensure compliance with MNDB obligations.

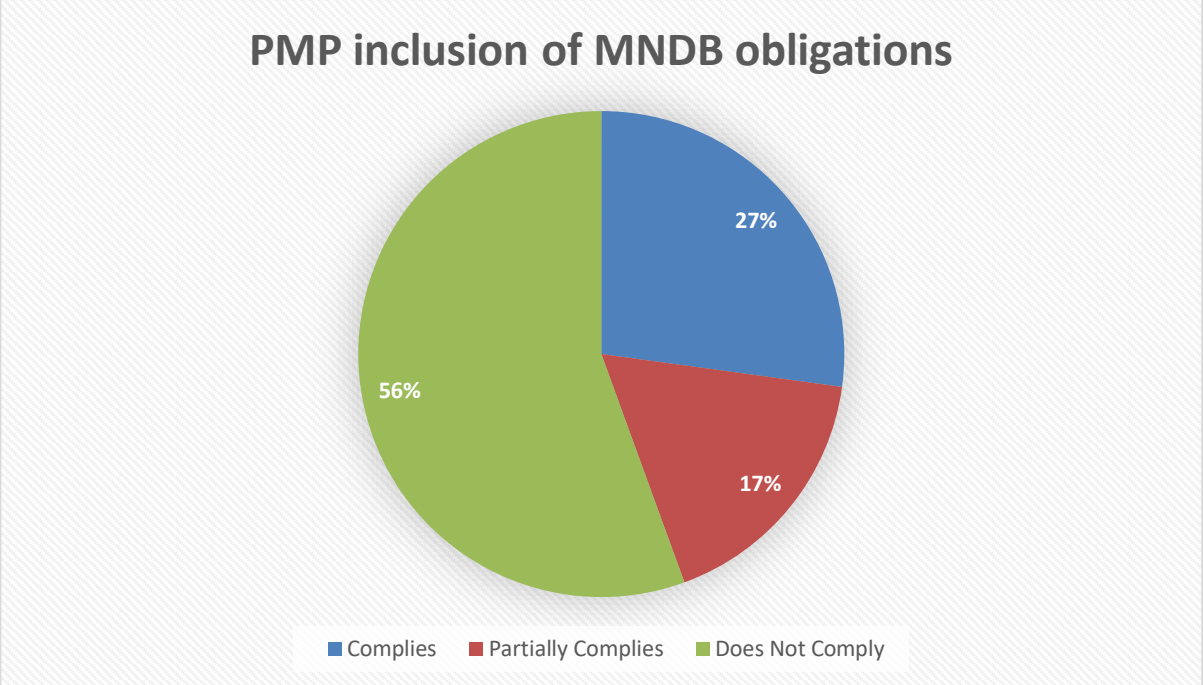

Figure 4. Breakdown of agency compliance with updating their PMP to include information about procedures and practices to ensure compliance with MNDB obligations.*

**Agencies that do not have a locatable PMP were marked as N/A and are not included in the data above.*

Comments, findings and recommendations

Figure 5 provides a breakdown of agency compliance with updating their PMP to include information about procedures and practices to ensure compliance with MNDB obligations by agency type.

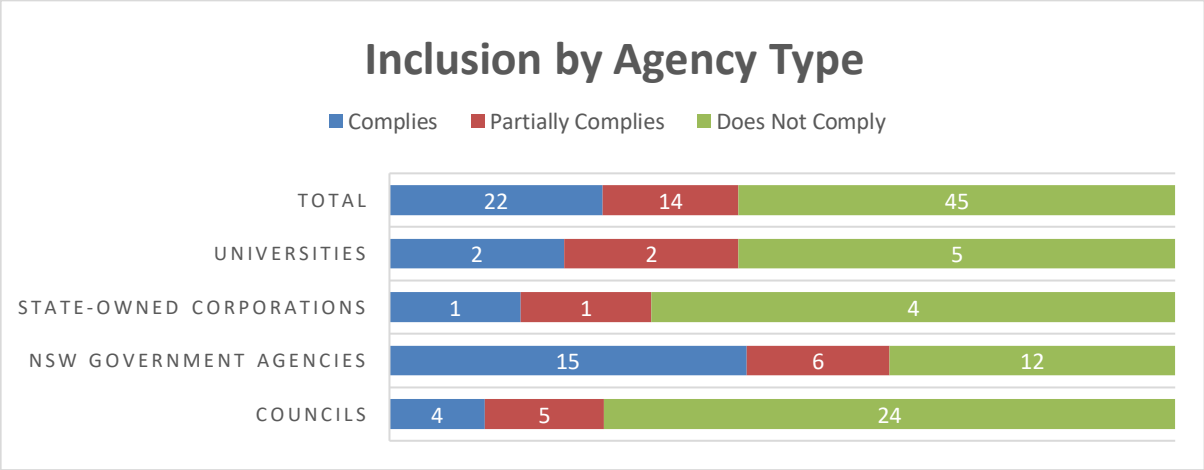

Figure 5: Breakdown of agency compliance with updating their PMP to include information about procedures and practices to ensure compliance with MNDB obligations, by agency type.

Recommendation 6: Agencies should review their PMPs to ensure the information contained therein is up to date and includes meaningful information about the procedures and practices with respect to the MNDB Scheme in accordance with Part 6A of the PPIP Act.

Recommendation 7: Agencies should be clear on their obligations and the separate purposes for their DBP and PMP, ensuring each contains the necessary information.

Recommendation 8: For agencies that have not yet published a PMP, it is recommended that immediate action is taken to develop a PMP in compliance with section 33 of the PPIP Act, including procedures and practices to ensure compliance with MNDB obligations and responsibilities as set out in Part 6A of the PPIP Act.

6. Conclusions

A suite of resources,[9] including an MNDB bi-monthly e-newsletter for agencies to explain the Scheme, and what steps should be taken to ensure compliance were published to support and prepare agencies. In particular, the April 2023 edition included information about agencies' obligation to prepare and publish a DBP. The June 2023 edition provided agencies with information and resources about updating PMPs to ensure compliance with the newly established provision of section 33(2)(c1) under the PPIP Act.

Despite the advanced notice and these measures taken by the IPC to inform agencies of their incoming obligations following the commencement of the MNDB Scheme, the findings of this review highlight notable gaps. Whilst there were some encouraging results from all sectors, it is also the case that there remains room for improvement across the four sectors.

Data breaches are occurring at increasing rates in the broader environment. Agencies are not immune and need to be proactive and well prepared in their approaches to protecting against and capably managing and responding to data breaches. The requirement to have a DBP is more than simply a legislative compliance requirement. A DBP is a critical step to documenting an organisation's plan for their response, clearly communicating roles and responsibilities for the effective management and mitigation of a data breach. An agency's preparation for, and response to, data breaches are key to fostering community trust and assuring the public of the agency's capability and readiness to address any eligible data breaches. A clearly visible and easily discoverable policy enhances public trust and confidence in government and the services it provides.

Agencies should review the findings from the report and recommendations contained to both review and build upon their compliance with the MNDB Scheme. With almost a year having passed since the MNDB Scheme commenced, it is timely for agencies to consider that a failure to have a DBP is akin to planning to fail.

[9] MNDB Scheme resources - https://www.ipc.nsw.gov.au/MNDB-Scheme-resources

7. Recommendations

This report makes a number of recommendations to assist agencies to improve their compliance with the legislative requirements to have and publish a DBP and the associated requirements to update their PMP as required by the PPIP Act.

The recommendations have been set out in the following table:

Recommendations	
Recommendation 1	Agencies should ensure that they comply with the obligation to have a DBP and ensure that the DBP is published to the agency website. Agencies that have not published a DBP to date, should take immediate steps to publish their DBP in accordance with section 59ZD of the PPIP Act.
Recommendation 2	Agencies should ensure that they make their DBP publicly available on their website without limitations or conditions on ease of access.
Recommendation 3	All agencies should ensure that they have a distinguishable DBP published in final form.
Recommendation 4	Agencies should consult the IPC Guide: Mandatory Notification of Data Breach Scheme: Guide to preparing a Data Breach Policy in developing their DBP
Recommendation 5	All agencies should review their publication of their DBP to their website to ensure its prominence, ease of searchability and access.
Recommendation 6	Agencies should review their PMPs to ensure the information contained therein is up to date and includes meaningful information about the procedures and practices with respect to the MNDB Scheme in accordance with Part 6A of the PPIP Act.
Recommendation 7	Agencies should be clear on their obligations and the separate purposes for their DBP and PMP, ensuring each contains the necessary information.
Recommendation 8	For agencies that have not yet published a PMP, it is recommended that immediate action is taken to develop a PMP in compliance with section 33 of the PPIP Act, including procedures and practices to ensure compliance with MNDB obligations and responsibilities as set out in Part 6A of the PPIP Act.

8. Appendix A: Audit Methodology

The review was undertaken with reference to the Privacy Commissioner's functions under section 36(2)(e) of the PPIP Act.

The review was limited to:

- a desktop audit and review of agency compliance with section 59ZD and section 33(2)(c1) of the PPIP Act
- a review of agency websites.

A desktop approach was determined as an appropriate and efficient preliminary assessment of sector wide adoption of the MNDB Scheme policy and procedural obligations for agencies. In this way, the IPC can compare general compliance across NSW public sectors rather than a focus on any individual sector or agency to establish baseline compliance in early learnings about the scheme.

This methodology allows for a direct point-in-time snapshot comparison with respect to the same criterion when a follow-up audit is undertaken.

The methodology applied should be recognised as constrained by the following factors:

- independent remote assessment
- non inquisitorial nature of the audit
- focused on identifying existence, ease of discovery of data breach policies and relevancy of MNDB Scheme policy and procedures contained in PMPs.

Accordingly, the IPC conducts desktop reviews to elevate compliance by way of guidance, awareness raising, and making recommendations to an agency as required.

As part of the assessment, a representative sample of 94 agencies were selected for inclusion in the review. These agencies are categorised by sector and included:

- a random selection of NSW Government Agencies
- State-owned Corporations within jurisdiction (all)
- Universities (all)
- Councils.

With respect to the Council sector, the IPC considered the Australian Classification of Local Governments, which groups Councils into the following council types:

- Metropolitan
- Regional Town/City
- Metropolitan fringe
- Rural
- Large Rural.

Eight councils from each council type were randomly selected for inclusion providing a representative sample from across all local councils.

9. Appendix B: Audit chronology

Date	Event
10 May 2024	Desktop Audit assessment completed
10 May 2024 – 28 October 2024	Analysis and Report Drafting
October 2024	Final Report Published

10. Appendix C: Abbreviations

The following table lists the commonly used abbreviations within this report.

Acronyms or abbreviation	Explanation
PPIP Act	*Privacy and Personal Information Protection Act 1998*
HRIP Act	*Health Records and Information Privacy Act 2002*
IPC	Information and Privacy Commission NSW
MNDB Scheme	Mandatory Notification of Data Breach Scheme
DBP	Data Breach Policy
PMP	Privacy Management Plan

11. Appendix D: Legislation

Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act)

Part 3 Division 2 Privacy management plans

33 Preparation and implementation of privacy management plans

> *(2) The privacy management plan of a public sector agency must include provisions relating to the following*
>
> > *(c1) 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.*

Part 4 Division 2 Functions of Privacy Commissioner

36 General functions

> *(2) In particular, the Privacy Commissioner has the following functions–*
>
> > *(e) to provide assistance to public sector agencies in preparing and implementing–*
> >
> > > *(i) privacy management plans under section 33, and*
> > >
> > > *(ii) data breach policies under section 59ZD*

Division 6 Other requirements for public sector agencies

59ZD Public sector agency to publish data breach policy

> *(1) The head of a public sector agency must prepare and publish a data breach policy.*
>
> *(2) The policy must be publicly available.*