October 2023

NSW ARB Policy

DATA BREACH

Contents

Introduction to NSW Mandatory Notification of Data Breach Scheme ('MNDB Scheme')

The *Privacy and Personal Information Protection Amendment Bill 2022* ('PPIP Amendment Bill') was passed by both houses of NSW Parliament on 16 November 2022 and was assented to on 28 November 2022.

Key changes include the creation of a Mandatory Notification of Data Breach Scheme ('MNDB Scheme') which is a mandatory notification requirement under Part 6A of the *Privacy and Personal Information Protection Act 1998* ('PPIP Act').

The MNDB Scheme comes into effect on 28 November 2023.

The MNDB Scheme requires agencies to satisfy data management requirements, including to maintain an internal data breach incident register, and have a publicly accessible data breach policy.

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.

An eligible data breach occurs when there has been:

- unauthorised access, unauthorised disclosure, or loss of personal or health information (where the loss is likely to result in unauthorised access or disclosure), and
- a reasonable person would conclude that this would be likely to result in serious harm to an individual to whom the information relates.

Under the MNDB Scheme, the NSW Architects Registration Board ('NSW ARB') has an obligation to:

- immediately make all reasonable efforts to contain a data breach
- undertake an assessment within 30 days where there are reasonable grounds to suspect there may have been an eligible data breach
- during the assessment period, make all reasonable attempts to mitigate the harm done by the suspected breach
- decide whether a breach is an eligible data breach or there are reasonable grounds to believe the breach is an eligible data breach

- notify the Privacy Commissioner and affected individuals of the eligible data breach, and
- comply with other data management requirements.

The proactive reporting of data breaches is a foundation of privacy protection and increases citizen trust in government agency handling of personal information and data breach incidents.

Steps the NSW ARB has taken to prepare for a data breach

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.

The NSW ARB has enhanced employee awareness of privacy and cyber principles and current threat trends, in addition to training and awareness around identifying, responding to, and managing data breaches.

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.

This Data Breach Policy outlines how actual or suspected data breaches can be reported by a NSW ARB employee, but also by any member of the public outside the NSW ARB.

The kinds of processes the NSW ARB has in place for identifying and preventing data breaches include:

- monitoring services (such as social media monitoring)
- audits and reviews
- employee training and awareness.

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 the NSW ARB meets its obligations under the PPIP Act, these agreements will include provisions in place for ensuring external stakeholders comply with relevant privacy requirements.

Schedule for testing and updating the Data Breach Policy

As both the external threat environment and the NSW ARB's internal makeup and functions are continuously developing and changing, this Data Breach Policy will be regularly reviewed to ensure it remains fit for purpose.

The Registrar has oversight of the Data Breach Policy, ensuring compliance with the PPIP Act. The Senior Lawyer, Regulation and Compliance, in conjunction with the Registrar, will review and monitor the policy and consider whether it is meeting its purpose. The Registrar will approve the version of the policy to be published.

Reports about compliance will be provided to the NSW ARB's Finance and Risk Committee.

If an error or issue is found in the policy, please contact us on:

T: +61 2 9241 4033
E: mail@architects.nsw.gov.au

This policy will be reviewed, tested, and updated annually.

Alignment with other policies

This Data Breach Policy is aligned with existing NSW ARB policies and procedures. It aligns with the NSW ARB Cyber Security Incident Response Plan and Privacy Management Plan. It is also aligned to NSW government protocols on information security event reporting and incident response.

Key terms

What is a data breach?

A data breach occurs when information held by an agency (whether held in digital or hard copy) is subject to unauthorised access, unauthorised disclosure or is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure.

This may or may not involve disclosure of information external to the agency or publicly. For example, unauthorised access to personal information by an agency employee, or unauthorised sharing of personal information between teams within an agency may amount to a data breach.

A data breach may occur as the result of malicious action, systems failure, or human error. A data breach may also occur because of a misconception about whether a particular act or practice is permitted under the Information Protection Principles ('IPPs').

Examples of data breaches include:

- **Human error**
  - When a letter or email is sent to the wrong recipient.
  - When system access is incorrectly granted to someone without appropriate authorisation.
  - When a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information is lost or misplaced.
  - When an employee fails to implement appropriate password security, for example not securing passwords or sharing password and log in information.
- **System failure**
  - Where a coding error allows access to a system without authentication, or results in automatically generated notices containing the wrong information or sends automatically generated notices to incorrect recipients.
  - Where systems are not maintained through the application of known and supported patches.
- **Malicious or criminal attack**
  - Cyber incidents such as ransomware, malware, hacking, phishing, or brute force access attempts resulting in access to or theft of personal information.
  - Social engineering or impersonation leading into inappropriate disclosure of personal information.
  - Insider threats from NSW ARB employees using their valid credentials to access or disclose personal information outside the scope of their duties or permissions.
  - Theft of a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information.

What is an eligible data breach?

The MNDB Scheme applies where an "eligible data breach" has occurred and is defined under section 59D of the PPIP Act.

For a data breach to constitute an "eligible data breach" under the MNDB Scheme, there are **two tests to be satisfied**:

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 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, the NSW ARB is not required to notify individuals or the Commissioner but should still take action to respond to the breach. The NSW ARB may still provide voluntary notification to individuals where appropriate.

Personal information and health information

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

The definition of personal information for the purposes of the MNDB Scheme includes "health information", as defined in section 6 of the *Health Records and Information Privacy Act 2002* ('HRIP Act'). This means that for the purposes of the MNDB Scheme (Part 6A of the PPIP Act only), "personal information" includes information about an individual's physical or mental health, disability, and information connected to the provision of a health service.

Expanding the definition of personal information to include health information for the purposes of the Scheme ensures that data breaches involving health information are treated in the same way as those involving other personal information, and that agencies take active steps to investigate, remediate and where appropriate, notify of such breaches.

What is serious harm?

The term "serious harm" is not defined in the PPIP Act.

Whether the unauthorised access, disclosure or loss of an individual's personal information is likely to result in serious harm to them, will be assessed by the NSW ARB as part of its response to the data breach. This requires an objective assessment determined from the viewpoint of a reasonable person.

The NSW ARB will consider the circumstances of the breach, how likely it is that the breach will cause harm, and the consequences and severity of that harm. Harms that can arise as the result of a data breach are context-specific and will vary. In making this determination, the NSW ARB may consider the following:

- The type of personal information accessed, disclosed, or lost, and whether a combination of types of personal information might lead to increased risk, for example, an email address is likely to be considered less likely to result in serious harm than credit card details.
- The level of sensitivity of the personal information accessed, disclosed, or lost, for example, if it relates to a person's finances, health, or sexual orientation.
- The amount of time the information was exposed or accessible, including the amount of time information was exposed prior to the NSW ARB discovering the breach, for example whether the personal information is or was protected by security measures such as encryption and therefore unlikely to be accessed or misused.
- The circumstances of the individuals affected and their vulnerability or susceptibility to harm (that is, if any individuals are at heightened risk of harm or have decreased capacity to protect themselves from harm).
- Actions taken by the NSW ARB to reduce the risk of harm following the breach.

- Who has access to the personal information.
- Whether the person/s who accessed the personal information may have a malicious intent and whether they may be able to circumvent security measures.
- The nature of the likely harm.
- Any other matter specified in the Privacy Commissioner's guidelines.

Serious harm occurs where the harm arising from the eligible data breach has, or may, result in a real and substantial detrimental effect to the individual. 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. It may include:

- financial loss through fraud
- a likely risk of physical or psychological harm, such as by an abusive ex-partner
- identity theft, which can affect an individual's finances and/or credit record
- serious harm to an individual's reputation.

Although quantitative analysis has a role in assessment of likelihood, in most cases the exercise **should be primarily a qualitative one**. That is, the NSW ARB will avoid relying too heavily on mathematical calculations to determine the likelihood of serious harm. Instead, the NSW ARB will consider the factors which affect the risk and err on the side of notification when there is doubt as to whether a data breach is "likely to result" in serious harm.

What is considered "reasonable"?

The term "reasonable" is not defined under the PPIP Act and will therefore bear its ordinary meaning. Whether something is considered "reasonable" will depend on the facts and circumstances in each case.

Whether an employee or officer has "reasonable grounds to suspect" is an objective test. The High Court has observed that whether there are "reasonable grounds" to support a course of action "requires the existence of facts which are sufficient to [persuade] a reasonable person", it "involves an evaluation of the known facts, circumstances and considerations which may bear rationally upon the issue in question" (see: George v Rockett (1990) 170 CLR 104 at 112 (Mason CJ, Brennan, Deane, Dawson, Toohey, Gaudron & McHugh JJ); McKinnon v Secretary, Department of Treasury (2006) 228 CLR 423 at 430 (Gleeson CJ & Kirby J). As that indicates, there may be a conflicting range of objective circumstances to be considered, and the factors supporting the presence of "reasonable grounds" should outweigh those against that conclusion.

For example, an information security officer observing unusual access to agency information systems by a colleague who is known to be away on leave and unlikely to log on to work while absent may give rise to "reasonable grounds" to suspect a data breach that warrants reporting to the head of the agency.

To constitute an eligible data breach under the MNDB Scheme, an employee or officer must be satisfied that "a reasonable person" would conclude that the data breach would be "likely to result in serious harm" to affected individuals. A "reasonable person" is a hypothetical individual who is properly informed with sound judgement.

How can an eligible data breach occur?

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.

Unauthorised access

The unauthorised access to personal information occurs when personal information held by the NSW ARB is accessed by someone who is not permitted to do so.

Unauthorised access can occur:

- **Internally within an agency** – for example, an employee browses agency records relating to a family member or an employee intentionally opens an electronic or paper file containing personal information when they do not have permission to access that information, without a legitimate purpose.
- **Between agencies** – for example, a team at one agency may be provided with access to systems and data at a second agency as part of a joint project. Unauthorised access may occur if a member of the team were to use that access beyond what is required for their role as part of that project.
- **Externally outside an agency** – for example, personal information is compromised during a cyberattack and accessed by a person external to the agency.

Unauthorised disclosure

Unauthorised disclosure of personal information can occur if information is provided to, or is accessible by, people outside the NSW ARB. Unauthorised disclosure occurs when the NSW ARB (intentionally or accidentally) discloses personal information in a way that is not permitted by the PPIP Act or HRIP Act.

For example, an unauthorised disclosure may occur where:

- Simple human or technical errors without malicious intent, for example where an agency accidentally publishes a data set containing personal information on its website.
- A system update results in the unintended publication of customer records containing personal information on an agency's website.
- An agency intends to provide de-identified information to a person but accidently sends the data with personal identifiers included.
- An agency provides personal information to the wrong recipient regardless of whether the information was viewed or accessed by the recipient.
- A database hosted in a cloud environment or a web facing application containing personal information does not have appropriate access controls and personal information in the data set is visible and accessed by unauthorised individuals.
- A third party downloading data from an unsecured computer system or platform.

Unauthorised access and disclosure are not mutually exclusive and may occur as a result of the same breach or as part of a chain of events. For example, if a malicious external actor gains unauthorised access to the NSW ARB records during a cyber attack, and steals information from those records, this may amount to unauthorised access to, and unauthorised disclosure of, the personal information held within those records.

Loss

Loss refers to situations in which personal information is removed from the possession or control of the agency. Loss may occur because of a deliberate or accidental act or omission of the NSW ARB, or due to the deliberate action of a third party. For example, personal information might be lost when:

- An agency sells or disposes of a physical asset (such as a laptop or filing cabinet) that still contains personal information.
- An agency employee accidentally leaves a device containing personal information on the bus.
- A device containing personal information is stolen from agency premises or an employee's home.

The loss of personal information will only result in an eligible data breach where such loss is likely to result in unauthorised access or disclosure of this information. If the personal information is inaccessible due to security

measures or because the information is retrieved before it is accessed or disclosed, then it is unlikely that an eligible data breach has occurred. Examples of this may include where:

- A password protected laptop containing client files is left on a bus but is handed into the depot and the agency is able to retrieve the laptop, which has not been accessed.
- A USB containing personal information is lost but is both encrypted and password protected.
- A tablet device containing client records is stolen from an employee's home, but it is only accessible via multifactor authentication.

As the loss of personal information in the above examples did not result in an unauthorised access or disclosure, no eligible data breach has occurred.

In some cases, a loss that results in serious harm to an individual may not necessarily amount to an eligible data breach. For example, where customer records are unintentionally deleted from a records management system, resulting in the denial of a particular service to those customers. Although this would not be an eligible data breach and notification is not mandatory in this scenario, the NSW ARB may consider voluntarily informing individuals of the loss of their information where there is a risk of serious harm.

Personal information "held" by an agency

Personal information is any information that identifies an individual and includes:

- a written record which may include name, address and other details about an individual
- photographs, images, video, or audio footage
- fingerprints, blood, or DNA samples.

Under section 59C of the PPIP Act, personal information is "held" by a public sector agency if:

- the agency is in possession or control of the information, or
- the information is contained in a state record for which the agency is responsible under the *State Records Act 1998*.

Health information is a specific type of "personal information" which may include information about an individual's physical or mental health or disability.

The MNDB Scheme does not generally apply to private sector service providers providing services on behalf of government. This is because information held by a private sector service provider is usually "held" by the service provider and not by a public sector agency. However, in some circumstances, information in the hands of a private sector 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. This will most commonly arise in the case of software-as-a-service contracts or cloud service provision where the agency has control over the use and access to the information.

Roles and responsibilities of the NSW ARB employees

The MNDB Scheme imposes various obligations on agency heads and the officers and employees of an agency. The NSW ARB agency head is the Registrar.

The Registrar, or their delegates, is responsible for:

- Immediately after receiving a report of a suspected data breach, making all reasonable efforts to contain the breach.
- Carrying out an assessment of a data breach within 30 days – the Registrar may appoint an assessor to carry out the assessment.
- Making all reasonable attempts to mitigate the harm done by the suspected breach.

- Approving an extension of the time periods for conducting an assessment.
- Following the assessment, deciding whether the breach is an eligible data breach or there are reasonable grounds to suspect the breach is an eligible data breach.
- Deciding whether an exemption from notification to affected individuals applies.
- Making a notification to the Privacy Commissioner and to affected individuals.
- Issuing a public notification in certain circumstances.
- Keeping the required registers under the MNDB scheme.
- Preparing and publishing a data breach policy.

Agency heads are authorised to delegate their functions under the MNDB Scheme to a person employed in or by their agency.

Officers and employees of the NSW ARB are responsible for:

- Reporting a suspected data breach to the Registrar – the NSW ARB should ensure all employees are aware of the process for reporting a suspected data breach, including relevant contact points.
- Where appointed as an assessor – carrying out an assessment of a data breach within 30 days.

The Finance Compliance and Risk Officer is appointed as an assessor for the NSW ARB.

Employees or the public can immediately report a suspected breach to the Registrar. The Registrar will maintain the role and responsibility for managing a data breach or suspected data breach. The Senior Lawyer, Regulation and Compliance and / or the Finance Compliance and Risk Officer will assist the Registrar as an appointed assessor in identifying, reporting, and responding to a breach or suspected breach.

A person can make a report to the Registrar in writing by email or letter to the Registrar, or orally by having a discussion with the Registrar either face-to-face, via telephone or virtually.

If a person has any questions or concerns, the Registrar's contact details are listed below:

Head of Agency

Dr Kirsten Orr
T: 02 9241 4033
M: 0403 617 760
E: registrar@architects.nsw.gov.au

The NSW ARB's plan for containing, assessing and managing data breaches

The Privacy Commissioner is empowered under section 59ZI of the PPIP Act to make guidelines for the purpose of exercising the Commissioner's functions under Part 6A.

The IPC Guidelines on the assessment of data breaches under Part 6A of the PPIP Act, made in accordance with that section of the PPIP Act, are intended to provide agencies with guidance on:

- the process of undertaking an assessment to determine whether an eligible data breach has occurred, and
- the factors to consider when assessing where serious harm to affected individuals is likely to result from a data breach.

These Guidelines supplement the provisions of the PPIP Act.

In assessing the data breach, the NSW ARB must have regard to the Guidelines in accordance with section 59I of the PPIP Act.

Assessment trigger

The obligation to assess a suspected data breach is triggered "if an officer or employee of an agency is aware that there are reasonable grounds to suspect there may have been an eligible data breach". On becoming aware, the officer must report the data breach to the head of the agency (or to any person to whom the head of the agency has delegated functions). The NSW ARB head of the agency is the Registrar.

Following receipt of this report, the Registrar must:

- immediately take all reasonable efforts to contain the data breach, and
- carry out an assessment to determine whether the data breach is an eligible data breach, or there are reasonable grounds to believe the data breach is an eligible data breach.

Where a breach is found to be an eligible breach, notification obligations to the Privacy Commissioner and affected individuals are triggered.

Assessment timeframe

To reduce the risk of harm to affected individuals, the NSW ARB will undertake its assessment of a suspected data breach as quickly and efficiently as possible. Section 59E provides that an agency must undertake an assessment of a suspected data breach within 30 days. To meet this timeframe the person undertaking the assessment must take all reasonable steps to ensure it is completed within 30 days.

The assessment timeframe commences when the NSW ARB officer or employee becomes aware that there are reasonable grounds to suspect an eligible data breach has occurred. The officer or employee becoming aware of a potential breach is the trigger for the time period to commence rather than when the breach is reported to, or received by, the Registrar or their delegate.

The 30-day assessment period refers to calendar days, not business (working) days.

As there is an additional requirement for agencies to carry out the assessment in an expeditious way, the NSW ARB will treat the 30 days as the maximum timeframe and where possible aim to complete the assessment in a shorter timeframe.

Extensions of time

Where the Registrar is satisfied that an assessment cannot reasonably be carried out within 30 days, they may approve an extension of time to conduct the assessment.

Where an extension is applied, the Registrar must provide written notice to the Privacy Commissioner advising:

- when the assessment commenced, and
- that the head of the agency has approved an extension of time to carry out the assessment.

As a matter of best practice, the notice provided to the Privacy Commissioner should also include advice on the reason for the delay in undertaking the assessment.

If the assessment is not completed within the extended time period, the Registrar must provide further written notice to the Privacy Commissioner:

- advising that the assessment is ongoing,
- that a new extension of time has been granted, and
- specifying the new extension period.

As with an initial extension notification, the notice provided to the Privacy Commissioner should also include advice on the reason for the delay in undertaking the assessment.

Who should conduct an assessment?

The Registrar may direct one or more persons to carry out the assessment (the "assessor"). Section 59G of the PPIP Act provides that an assessor may be:

1. An officer or employee of the agency subject to the breach.
2. An officer or employee of another agency acting on behalf of the agency subject to the breach. For example, this may include NSW agency employees under secondment, or the Chief Information Officer of another agency assigned to assist based on their previous experience in assessing data breaches.
3. An external party who has been engaged, whether through employment or contract, by the agency to conduct the assessment on the agency's behalf, including the external party's employees.

Note, if the Registrar has reason to suspect an individual was involved in an act or omission that led to the data breach, that person is not permitted to take on the role of the assessor.

Containing a breach or suspected breach to minimise the possible damage

During an assessment, the NSW ARB must make all reasonable attempts to contain the breach and mitigate any harm arising as a result of the breach.

The Registrar must immediately make all reasonable efforts to contain the breach and while the assessment is being conducted, make all reasonable attempts to mitigate any harm done by the suspected breach.

"Containing" a data breach means limiting its extent or duration or preventing it from intensifying. This could be done by stopping an unauthorised practice, recovering, or limiting the dissemination of records disclosed without authorisation, or shutting down a compromised system. Containment actions can be distinguished from mitigation actions, which involve managing or remediating harms arising as a result of the breach.

Guidance on containment and mitigation measures is contained in the IPC Guide to managing data breaches under the PPIP Act.

How to conduct an assessment

There is no specific procedure by which an agency must conduct an assessment. In general, an assessment by the NSW ARB will involve the following:

1. **Information gathering:** collect all relevant information regarding the suspected breach. This may involve contacting relevant stakeholders, identifying what information was or may have been compromised, and investigating logs or other evidence from compromised systems that may be relevant to the assessment of the suspected breach.
2. **Analysis:** review the information collected during the previous phase to evaluate the scale, scope, and content of the suspected data breach, and its potential impact on affected individuals. The analysis should include a careful consideration of the type of information involved in the breach, the actual or potential harms that may arise for affected individuals, the seriousness of the harm and the likelihood of that harm occurring.
3. **Decision:** come to a conclusion as to the eligibility of the suspected data breach based on the factors considered throughout the analysis.

In assessing the data breach, the NSW ARB will follow the IPC Guidelines on the assessment of data breaches under Part 6A of the PPIP Act.

Processes for when and how individuals are notified

The MNDB Scheme imposes notification obligations on agencies. The NSW ARB must notify both the Privacy Commissioner and affected individuals of an eligible data breach.

Once the Registrar determines that a data breach is an "eligible data breach" for the purposes of the Scheme, they must:

- **immediately** notify the Privacy Commissioner using the form approved by the Privacy Commissioner for this purpose, which is available on the IPC website, and
- **as soon as practicable**, take reasonable steps to notify affected individuals (unless an exemption applies). If an agency is unable to directly notify any or all affected individuals, the agency must issue and publicise a public notification.

An individual to whom the information relates and "affected individuals"

When an agency determines that an eligible data breach has occurred it has an obligation to notify "affected individuals". An "affected individual" is defined under s59D of the PPIP Act as an individual:

- to whom the information subject to unauthorised access, unauthorised disclosure or loss relates, and
- who a reasonable person would conclude is likely to suffer serious harm as a result of the data breach.

The phrase "to whom the information relates" is not defined and should be given its ordinary meaning, i.e., the person who is the subject of the information. An individual will be an affected individual, regardless of whether the information was originally collected directly from the individual or from a third party, if the information involved in the breach is about them.

Impacts on individuals, agencies or others that are indirectly connected to the breached information (but are not an "individual to whom the information relates") should be excluded from the assessment for the purposes of the MNDB Scheme. In general, an individual who is only indirectly connected to the information involved in a data breach, for example through a family relationship or community group, and who may suffer detriment following a data breach as a result of that connection, would not ordinarily be an "individual to whom the information relates".

If the NSW ARB believes that third parties might be significantly affected by a data breach, and that notification may assist in mitigating any harm, the NSW ARB may also elect to make a public notification.

Requirements to notify

When the head of an agency decides that an eligible data breach has occurred, the notification process under Division 3 of the MNDB Scheme is triggered. There are **four** elements of the notification process:

1. Notify the Privacy Commissioner

Once the NSW ARB determines an eligible data breach has occurred, the Registrar must immediately notify the Privacy Commissioner about the breach in the approved form.

The form asks a number of questions relating to the breach. The responses to those questions will assist the IPC to assess whether the NSW ARB is meeting the requirement for immediate notification of the breach to the Privacy Commissioner.

In some cases, it may be obvious that a breach will be an eligible breach even before the assessment is completed. If this is the case, the NSW ARB should consider notifying the Privacy Commissioner immediately rather than waiting until the assessment is finalised.

2. Determine whether an exemption applies

After notifying the Privacy Commissioner, the NSW ARB must notify individuals unless an exemption applies. The six exemptions are:

- Where an eligible data breach affects multiple public sector agencies, and another agency has undertaken to notify individuals. Both agencies must still conduct their own assessment, containment, and mitigation, and notify the Privacy Commissioner.

- Where notification of the eligible data breach would be likely to prejudice an investigation that could lead to the prosecution of an offence or proceedings before a court or a tribunal.
- Where the agency has taken mitigation action that successfully prevents serious harm from occurring, so that a reasonable person would conclude that the breach is no longer likely to result in serious harm to an individual.
- Where notification would be inconsistent with a secrecy provision in another Act.
- Where notification would create a serious risk of harm to an individual's health or safety.
- Where notification would worsen the agency's cyber security or lead to further breaches.

The above exemptions do not affect the NSW ARB's obligation to notify the Privacy Commissioner.

Although Part 6A does not impose a timeframe for the Registrar to make this assessment, the IPC expects that in most instances this assessment should occur as part of or immediately following the assessment of the data breach.

Agencies relying on exemptions relating to health or safety or cyber security must provide a written notice to the Privacy Commissioner advising of their reliance on the exemption and provide other specified information. The NSW ARB will keep appropriate records of any assessment and decision-making process leading to reliance on an exemption.

Further information about the application of the exemptions can be found in the Privacy Commissioner's Guidelines on the exemption for risk of serious harm to health or safety under section 59W, Guidelines on the exemption for compromised cyber security under section 59X, and Fact Sheet - Mandatory Notification of Data Breach Scheme: Exemptions from notification requirements.

3. Notify individuals

Unless an exemption applies, agencies are required to notify affected individuals as soon as reasonably practicable. Notification should be made directly to the individual concerned, their parent or guardian (in the case of children) or an authorised representative. Where the NSW ARB is unable to notify directly or it is not reasonably practicable to do so, a public notification must be made.

If there is an eligible data breach and none of the exemptions apply, agencies must notify relevant individuals of the eligible data breach.

See the IPC Fact Sheet – Notification to affected individuals of a data breach for further information on the notification process which also includes tips on how to protect personal information.

a) Who must be notified?

Agencies may elect to notify either:

1. each individual to whom the compromised information relates, regardless of their risk of harm, or
2. only affected individuals, meaning those individuals who are likely to suffer serious harm as a result of the compromise of personal information that relates to them.

If the NSW ARB is unable, or it is not reasonably practicable, to notify all relevant individuals, it must issue a public notification instead (see below).

b) When should agencies notify?

Notification to individuals must be made "as soon as reasonably practicable" after determining that a breach is an eligible data breach.

Timely notification is important to help individuals affected by a breach take personal steps to limit or mitigate the risks of misuse or further exposure. The NSW ARB should avoid undue delay and should work to make affected individuals aware of the breach as soon as possible.

Agencies should carefully balance speedy notification to individuals with ensuring that citizens are provided with reliable and accurate information about the breach. Most importantly, notifications should provide recipients with an accurate sense of what risks may arise for them and what practical measures they can take to protect themselves. If an agency is not yet able to provide meaningful detail in a data breach notification, it may be too early to provide it.

Similarly, a notification that gets things wrong can cause more harm than good. A notification that provides inaccurate advice about what information has been breached or provides incorrect advice about who may be at risk, can cause unnecessary anxiety and stress in those not seriously affected and may fail to achieve the central objective of enabling those who are affected from taking protective action.

c) What should be included in the notification?

For most people, receiving a notification that their personal information has been breached can be very stressful. In some cases, it can have a significant impact on an individual's emotional and psychological wellbeing, particularly where they are at risk or especially vulnerable.

The way the NSW ARB tells people that their information has been breached is important. Notifications will avoid minimising the severity of a breach, but also seek to avoid causing undue alarm. Notifications will provide recipients with an accurate sense of what happened, what risks may arise, and what they can do to protect themselves. Notifications will be made in plain English, using clear and easily understood language.

A notification will generally be made in writing. The NSW ARB will send notifications to the affected individuals by email. In some instances, such as where the individual may be at imminent risk of physical violence as a result of a data breach, a notification by phone may be appropriate. This will always be followed by a written notification.

Section 59O of the PPIP Act sets out specific information that must, if reasonably practicable, be included in a notification:

1. The date the breach occurred.
2. A description of the breach.
3. How the breach occurred.
4. The type of breach that occurred.
5. The personal information included in the breach.
6. The amount of time the personal information was disclosed for.
7. Actions that have been taken or are planned to secure the information, or to control and mitigate the harm done.
8. Recommendations about the steps an individual should take in response to the breach.
9. Information about complaints and reviews of agency conduct.
10. The name(s) of the agency(s) that were subject to the breach.
11. Contact details for the agency subject to the breach or the nominated individual to contact about the breach.

d) What post-notification support should agencies provide for citizens?

The type of assistance or support the NSW ARB will provide following a notification will depend on the specific circumstances of the data breach. Examples include:

- A dedicated contact point to provide further information to affected individuals.
- Advice to individuals on how to protect their personal information.
- Provision of links to support services such as ID Care and ID Support NSW.
- Provision of links to counselling or mental health support services.

The NSW ARB will carefully consider what may be required within the context and scope of the particular data breach.

e.) Public notification register

The NSW ARB must maintain and publish on its website a public notification register for any public data breach notifications that the agency has issued.

A "public data breach notification" is a notification made to the public at large rather than a direct notification to an identified individual. The MNDB Scheme provides for a public data breach notification to occur in two circumstances:

- A public notification **must** be made by an agency if it is unable, or it is not reasonably practicable, to notify any or all the individuals affected by the breach directly. Direct notification may be impracticable for a range of reasons, such as where a breach involves older records, and the NSW ARB does not hold current, direct contact details for some or all the affected individuals, or
- An agency head may also decide to make a public notification concurrently with direct notifications to affected individuals. The issuing of a public notification in these circumstances does not excuse the NSW ARB from the requirement to make direct notifications if it is reasonably practicable to do so.

The PPIP Act does not prescribe the information that must be included on the public notification register. However, the purpose of the register is to ensure that citizens can access sufficient information about eligible data breaches to determine whether they may be affected by the breach and take action to protect their personal information. This means the agencies should provide information about:

- what happened
- what has been accessed
- what the agency is doing, and
- what an affected individual can do.

The IPC expects that the public notification must include all the same information that would be included in a direct notification, but should exclude:

- Personal information about an individual. For example, an agency may exclude information about specific individuals involved in the breach or breach response.
- Information that would prejudice the agency's functions. For example, an agency may omit certain details about a breach if they would expose a confidential investigation or publicise a vulnerability that still exists and can be further exploited.

In making a public notification, the NSW ARB must:

- Keep a public notification register on their website.
- Publish the notification on the public notification register for at least 12 months.
- Advise the Privacy Commissioner of how to access the notification on the public register (for example, by emailing the link to the notification website).

In addition to publishing the notification on its website, the NSW ARB must take reasonable steps to publicise the contents of the statement, to increase the likelihood that it will come to the attention of those individuals at risk of serious harm. This will be done by a notice on the main NSW ARB website.

4. Provide further information to the Privacy Commissioner (as required)

Agencies may be required to provide additional information to the Privacy Commissioner if they have been unable to provide complete information in their initial notification, if they have made a public notification, or if they are relying on an exemption.

Notification of an eligible data breach to the Privacy Commissioner will not usually be a once-off. The NSW ARB will seek to keep the Privacy Commissioner updated as the breach response progresses, and new information comes to light.

The MNDB Scheme includes several further requirements on agencies to update the Privacy Commissioner on their breach response and approach to notification:

- If an agency omits information from its immediate notification to the Privacy Commissioner, it is required to provide an updated notification once that information becomes available.
- If an agency relies on either of the exemptions relating to health or safety or cyber security, they must additionally provide a written notice to the Privacy Commissioner advising of their reliance on the exemption, whether the exemption is permanent or temporary, and if temporary, the expected time the exemption is to be relied on.
- If an agency publishes a public notification, it must advise the Privacy Commissioner of how to access the notification on the public register (for example, by emailing the link to the notification website).
- Notifying affected individuals when a breach occurs allows them to take actions to protect themselves from harm and regain control of their information. Timely notification can be key to minimising the risks of serious harm resulting from a data breach.

Processes for responding to incidents that involve another entity

Breaches involving more than one agency

The MNDB Scheme recognises that agencies often hold information jointly, and there may be situations in which the breach of personal information held by one agency must be managed across multiple agencies.

Under section 59C of the PPIP Act, an agency is taken to "hold" personal information if:

1. the agency is in possession or control of the information, or
2. the information is contained in a state record in respect of which the agency is responsible under the *State Records Act 1998*.

Two agencies may "hold" information jointly. For example, where one agency has physical custody of the record, while a second agency retains authority to determine what is done with the records.

In the event of a data breach affecting personal information that is jointly held between agencies, each agency is required to assess the breach and if the breach is determined to be an eligible breach, each agency must notify the Privacy Commissioner. However, only one of the affected agencies is required to notify affected individuals or make a public notification (if required).

The PPIP Act does not specify which agency is responsible for such notification. In general, the agency with the most direct relationship with the affected individuals will be best placed to notify and provide direct support as required.

Breaches involving private sector service providers

The MNDB Scheme does not generally apply to private sector service providers providing services on behalf of government. This is because information held by a private sector service provider is usually "held" by the service provider and not by a public sector agency.

However, as noted above, an agency is taken to "hold" personal information if the agency is in "possession" or "control" of the information. This means that information in the hands of a private sector 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.

Some examples of when information in the hands of a private sector service provider may still be "held" by the outsourcing agency include:

- Cloud-based IT services, also known as Software-as-a-Service (SAAS) or Infrastructure-as-a-Service (IAAS), where agency data is hosted on IT infrastructure owned and operated by the service provider.

- Physical archiving services, where agency hardcopy records are stored and maintained by the service provider.

The NSW ARB holding personal information jointly with private sector service providers, such as the Architects Accreditation Council of Australia, will incorporate the following in their procurement contracts:

- A requirement that the service provider promptly report data breaches to the agency, take mitigating actions and assist the agency in undertaking assessments.
- A statement of who should notify affected individuals and provide support in the event of the breach. As the organisation with the most direct relationship with the affected individuals the public sector agency will generally be best placed to notify and provide direct support as required.

Special considerations when dealing with third-party breaches

Data breaches involving third-party service providers are increasingly common, and present unique challenges for agencies. As noted above, the NSW ARB will seek to include contractual terms in outsourcing arrangements that require service providers to report data breaches and cooperate with the NSW ARB in their breach response.

However, even with appropriate contractual powers in place, it can be difficult to take effective containment and mitigation actions or to conduct a timely and accurate assessment when the relevant information is split between the parties: the service provider having the knowledge about the system and the breach, while the agency possesses the contextual knowledge about the personal information needed to assess risk of serious harm.

When dealing with a third-party breach, the NSW ARB will:

- Engage their legal and procurement teams to review relevant contracts to understand parties' rights and obligations in detail.
- Work collaboratively with the third party to understand the nature and extent of the breach. Where the affected third party is a smaller service provider, this may include stepping in to assist them with containment or other steps.
- Where the affected third party is a large supplier with contracts across multiple public sector agencies, affected agencies should consider coordinating to jointly engage with the vendor on containment and remediation actions.

Record-keeping

The NSW ARB must 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. The NSW ARB must keep full and accurate records with respect to all information received in connection with the MNDB Scheme. This ensures that the NSW ARB complies with its obligations under the PPIP Act.

The information will be stored securely on the NSW ARB internal server and eligible data breached will be recorded in the Internal Breach Incident Register.

Recording 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 the NSW ARB to identify and remedy weaknesses in security or processes that are prone to error.

Systems for post-breach review of a data breach

Dealing with a data breach extends beyond immediate assessment and notification requirements. Understanding what went wrong, how issues were addressed and whether changes to systems, processes and procedures following a breach will mitigate future risks, is key to ensuring agencies continue to proactively manage data breaches in line with regulator and community expectations.

The NSW ARB considers a data breach incident as an opportunity to review and strengthen information security and data handling practices. A post incident review will often highlight processes that are vulnerable to human error or weaknesses in existing systems and security controls that should be addressed to reduce the likelihood of future breaches.

Documenting issues and remedies

Following a data breach, the NSW ARB will take time to investigate what went wrong and to update relevant policies and procedures to remedy any issues to prevent future breaches. A post incident review will look into:

- The effectiveness of the agency's Data Breach Policy and incident response process itself.
- A root cause analysis of the data breach.
- If required, more focused reviews of particular systems, policies and procedures involved in the breach. For example,
    - If the breach exposed a large number of old and unnecessary records, a review of the agency's data retention and deletion processes.
    - If the breach involved human error in a manual process, a review of how the process might be made safer.
    - If the data breach involved a security flaw in a particular system or collection of systems, a security review and root cause analysis.
    - If the data breach involved a supplier, a review of that supplier's contractual arrangements and security posture.

The NSW ARB will document agreed remediation actions arising from the post incident review in the Privacy Management Plan.

Preventing future breaches

Possible preventative measures to address specific types of breaches, which may assist the NSW ARB to identify potential pathways to improvement after a data breach, are considered below.

1. Breaches involving the sharing of information with unintended recipients

If the breach was caused by the accidental sharing of an email or other type of communication to unintended recipients, preventative measures could include:

- Ensuring employees are aware of, and receive training on, the handling guidelines.
- Establishing alternative processes and systems so that highly sensitive documents or information are not shared by email.
- Encouraging employees to send links to files rather than full file attachments where possible.
- Using passwords/encryption to protect documents containing sensitive information or large amounts of personal information.
- Training employees to consider whether an entire document or spreadsheet needs to be sent or if there is a way of extracting only the relevant information intended for the recipient.

2. Breaches involving the theft or loss of devices

If the breach was caused by the theft or loss of devices, preventative measures could include:

- Establishing a policy for the types of information that can be stored on a portable device.
- Imposing additional security measures for portable devices such as encryption, password locks, multi-factor authentication, remote wiping, and physical security.
- Protecting sensitive documents and information using physical security measures such as locks or filing cabinets.

- Training employees to ensure documents, computers or other electronic devices are not visible in homes or in parked cars.
- Establishing a protocol for deleting personal information and other data when it is no longer needed in accordance with the retention requirements under the *State Records Act 1998*.

3. Breaches involving malicious online attacks

If the breach was caused by malicious online attacks, preventative measures could include:

- Investing in security capability and maturity.
- Applying mitigation strategies such as the Australian Cyber Security Centre's Essential Eight.
- Applying a cyber security risk management framework such as the US Government's National Institute of Standards and Technology (NIST) Cyber Security Framework.
- Requiring multi-factor authentication and the use of strong passwords for all employee accounts.
- Investing in regular employee training on IT security.
- Undertaking a regular phishing simulation program to test employees' awareness of, and capacity to identify, suspicious emails.
- Restricting employees' ability to install software onto work computers.

4. Breaches involving unauthorised access and/or disclosure by employees

If the breach was caused by unauthorised access or disclosure by employees, preventative measures could include:

- Instituting role-based access to files (e.g., locking files down and only providing access to those employees with a need to know).
- Logging and monitoring employee access to files, flagging and investigating unusual or suspicious activity, and taking disciplinary action where appropriate.
- Clearly establishing in the agency's code of conduct that access to personal information is on a need-to-know basis, with clear consequences for violations of the code.
- Training employees on the handling and management or personal information, including organisational practices around monitoring and auditing of file access.

Review and update data breach policy

It is common for agencies to identify opportunities for improvement in the Data Breach Policy and breach response process itself after each data breach response. Processes, thresholds, escalation, and reporting pathways that sounded reasonable when the policy was drafted may be ineffective in practice. To take advantage of these learnings, the NSW ARB will review the policy after every breach response and update it to address any opportunities for improvement that may have been identified.

This policy will be reviewed, tested, and updated annually.

If an issue is found in the policy, the NSW ARB can be contacted on:

T: 02 9241 4033
E: mail@architects.nsw.gov.au

Policy updated October 2023