Introduction to the Mandatory Notification of Data Breach Scheme

Ensuring your agency is prepared

IPC Webinar
17 August 2023
Microsoft Teams

Samantha Gavel
NSW Privacy Commissioner

information and privacy commission
new south wales

Privacy and Personal Information Protection Amendment Bill 2022

- The PPIP Amendment Bill passed both houses of NSW Parliament on 16 November and was assented to on 28 November 2022.
- Amendments to come into effect 12 months after assent on **28 November 2023**.
- Key changes include:
  - **Creation of a Mandatory Notification of Data Breach (MNDB) Scheme** in which NSW public sector agencies bound by the PPIP Act will need to notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information likely to result in serious harm
  - applying the PPIP Act to all **NSW state-owned corporations** that are not regulated by the Commonwealth *Privacy Act 1988*
  - repealing s117C of the *Fines Act 1996* to ensure that all NSW public sector agencies are regulated by the same mandatory notification scheme.

Mandatory Notification of Data Breach Scheme

- The MNDB Scheme will require NSW public sector agencies bound by the PPIP Act to notify the IPC and affected individuals of data breaches involving personal or health information likely to result in serious harm.
- From **28 November 2023**, agencies will be required to comply.
- Mandatory notification schemes are considered **best practice** and enable individuals to **take action** and **protect themselves** in the event of a breach.
- The proactive reporting of data breaches is a foundation of privacy protection and will increase citizen trust in government agency handling of personal information and data breach incidents.
- In the lead up to 28 November 2023, the IPC is preparing resources for citizens and agencies and other guidance, including a Bi-monthly newsletter that will provide updates about the Scheme.

What is a data breach?

- Occurs when information held by an agency (digital/hard copy) is subject to unauthorised access, disclosure, or is lost in circumstances where the loss is likely to result in unauthorised access or disclosure.
- May or may not involve disclosure of information externally or publicly:
  - Unauthorised access to personal information (PI) by an agency employee
- 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

Human error

- Letter or email is sent to the wrong recipient
- System access is incorrectly granted to someone without authorisation or there is inadequate password protection
- Physical assets with PI are lost/misplaced e.g. records, laptop, USB, phone

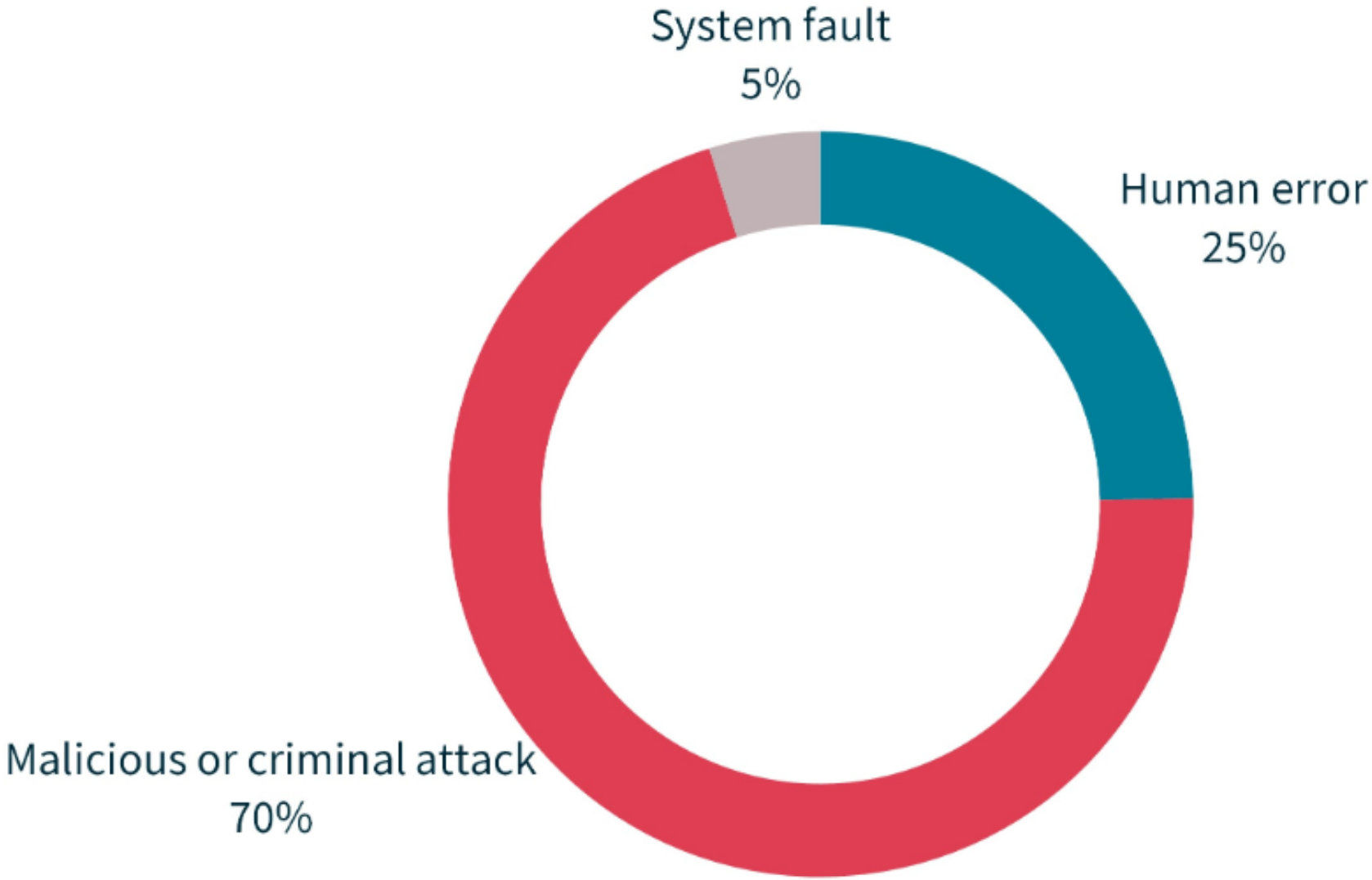
System failure

- Coding error allowing system access without authentication, or automatically generates notices
- Systems are not maintained through the application of known and supported patches

Malicious or criminal attack

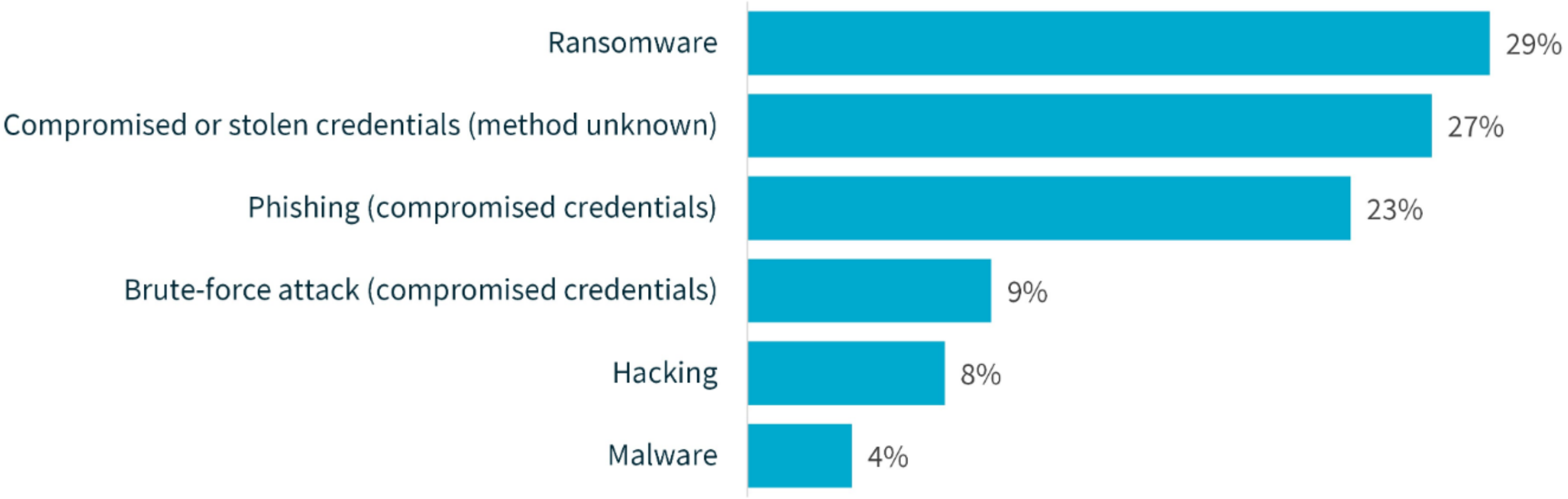
- Cyber incidents e.g. ransomware, malware, hacking, phishing, brute force access attempts
- Social engineering/impersonation meaning inappropriate disclosure of PI
- Insider threats (employees) using valid credentials to access/disclose PI outside the scope of their duties or permissions

Sources of data breaches



OAIC Notifiable Data Breaches Report: July to December 2022

Cyber incident breakdown



OAIC Notifiable Data Breaches Report: July to December 2022

What is an eligible data breach?

- 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.
- The Privacy Commissioner will issue Guidelines soon to guide agencies through the considerations necessary for determining whether there has been an eligible data breach and whether the serious harm threshold has been met.
- Agencies must have regard to the Guidelines when conducting an assessment under Part 6A of the PPIP Act.

What is serious harm?

- ***Serious harm*** is not defined under the legislative amendments. The amendments provide a series of factors that an agency should consider when assessing the risk of serious harm occurring as a result of a data breach.
- Harms that can arise as the result of a data breach are context-specific and will vary based on:
  - type of PI accessed, disclosed or lost, and whether a combination of types of PI might lead to increased risk
  - level of sensitivity of the PI accessed, disclosed or lost
  - amount of time the PI was exposed or accessible, including prior to the discovery of the breach
  - circumstances of the individuals affected and their vulnerability or susceptibility to harm
  - circumstances in which the breach occurred
  - actions taken by the agency to reduce the risk of harm following the breach

MNDB Scheme – agency obligations

Where there are reasonable grounds to suspect that an eligible data breach may have occurred, agencies must:

- Make all reasonable efforts to contain the breach
- Assess whether there has been unauthorised access, disclosure or loss of PI held by an agency within 30 days
- Assess if there is a likelihood of serious harm to any affected individual within 30 days
- Make all reasonable attempts to mitigate the harm done by the suspected breach.

Where a data breach is assessed as an eligible data breach, agencies must:

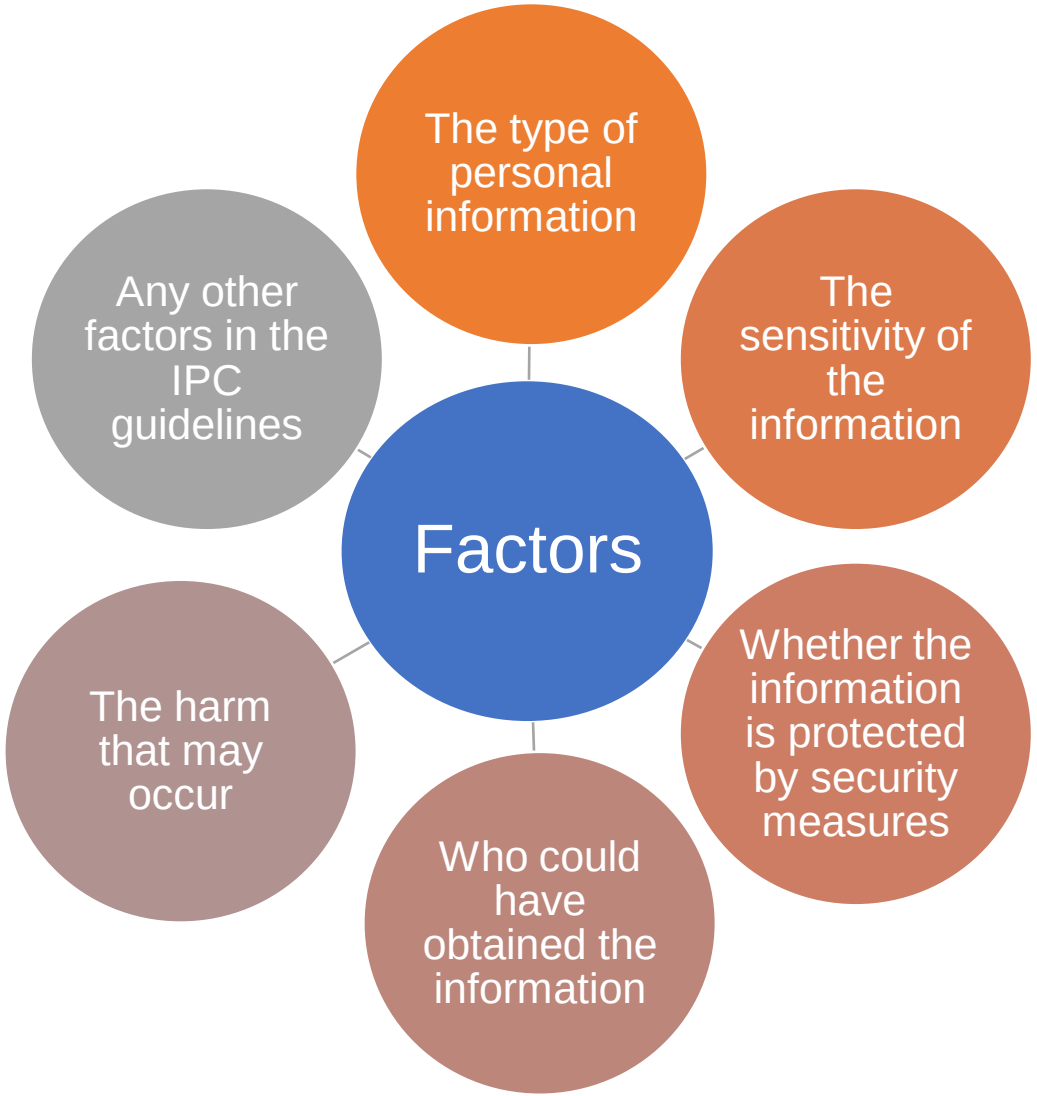
- Notify the Privacy Commissioner immediately, using the form on the IPC website
- Notify affected individuals as soon as practicable.

Agencies must also maintain:

- **A public data breach policy**, setting out how the agency will respond to a data breach
- **A public register of data breach notifications** issued by the agency
- **An internal register of eligible data breaches** at the agency.

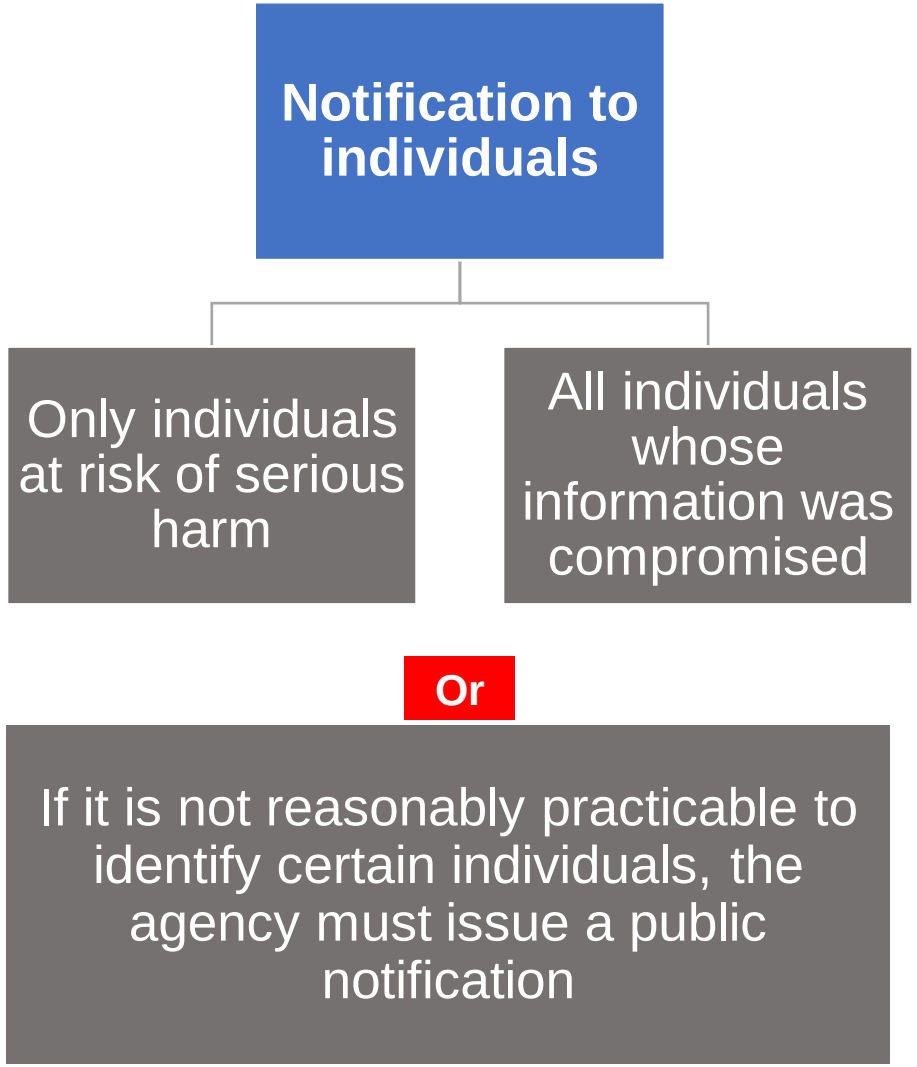
Assessment of data beaches

- If an agency reasonably **suspects** an eligible data breach has occurred, the head of the agency must assess and decide whether the data breach is an eligible data breach within **30 days.**
- If the head of the agency is satisfied the assessment cannot reasonably be conducted within 30 days, they may approve an extension of time.
- The legislation provides a non-exhaustive list of factors that an agency may consider when making an assessment.



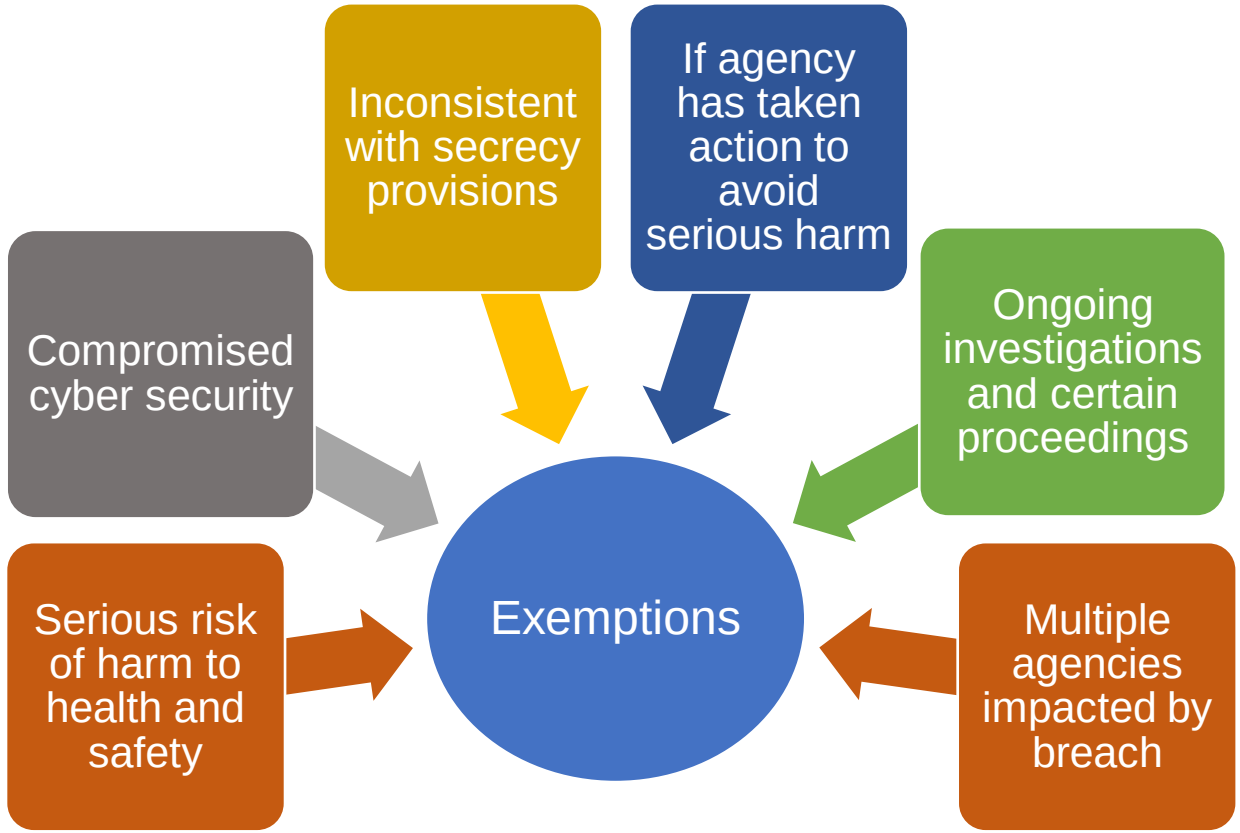
Notification

- Once an agency head determines that an eligible data breach has occurred they must:
  - **immediately** notify the Privacy Commissioner, and
  - **as soon as practicable** notify certain individuals.
- There are **three options** for notifying individuals that are affected by a breach.



Exemptions from Notification to Individuals

- An agency is not required to notify individuals of an eligible data breach if an exemption applies. However, **an agency is still required to notify the Privacy Commissioner.**
- In some instances, the Privacy Commissioner will receive written notification when an agency exercises an exemption.
- The IPC has published a fact sheet on this to assist agencies in the exercise of some exemptions: www.ipc.nsw.gov.au/node/2372



Other requirements for agencies

- **Privacy Management Plan** – a PMP will need to include information on the procedures & practices used by the agency to comply with MNDB obligations
- **Data Breach Policy –** prepare and publish a data breach policy
- **Notification Register –** public notification register on the agency's website for notifications made by way of a public notice
  - each notification must be publicly available for at least 12 months and contained specified information.
  - a link must be provided to the Privacy Commissioner and published on the IPC website
- **Incident Register –** establish & maintain an internal register of eligible data breaches

Enforcement Powers for the Scheme

- **Direction:** Issue a direction to an agency requiring the agency to provide specified information where the Commissioner has reasonable grounds to believe there has been an eligible data breach.
- **Recommendation:** Recommend that an agency notify individuals of a suspected eligible data breach.
- **Investigation:** Investigate, monitor, audit and report on the exercise of a function of an agency, including the systems, policies and practices.
- **Entry of Premises:** Can enter premises, observe systems, policies & procedures, and inspect documents for the purpose of monitoring and reporting on the agency's compliance.
- **Reports and Recommendations:** Issue a report in relation to a function of the Privacy Commissioner. The report may be published, given to the Minister or given to the head of an agency.

Privacy and Personal Information Protection Amendment Bill 2022

To prepare for the scheme, agencies will need to:

- Establish and clarify roles & responsibilities
- Review and update their Privacy Management Plan
- Prepare and publish a Data Breach Policy
- Review and update relevant policies and procedures
- Establish an incident register
- Establish a public notification register

E-Newsletter

The IPC is publishing a bi-monthly e-newsletter to update NSW practitioners about new resources and information relating to the MNDB Scheme.

Privacy and Personal Information Protection Amendment Bill 2022

IPC guidance on the MNDB Scheme:

- **NEW** Fact Sheet for agencies: Exemptions from notification to affected individuals
- **NEW** Guide to preparing a data breach policy
- **NEW** Fact Sheet for citizens: What is the MNDB Scheme
- **NEW** Fact Sheet for citizens: Notification to affected individuals of a Data Breach
- **NEW** Guide for agencies: Managing data breaches in accordance with the PPIP Act
- **NEW** Form: Data Breach Notification to the Privacy Commissioner
- Guideline: Assessing an eligible data breach (Aug 23, Minister approval)
- Guideline: Exemption under s 59W (health and safety) (Aug 23, Minister approval)
- Guideline: Exemption under s 59X (cybersecurity) (Aug 23, Minister approval)

In addition, the IPC will also be releasing other resources such as e-learning modules and animations later in the year.

Impacts for the IPC

Implementation work is underway across all teams:

- **Case management** – development of workflows, procedures and templates
- **Infrastructure** – updates to Resolve, webform for notification
- **Statutory guidelines** – processes for undertaking an assessment, how to assess likelihood of serious harm, factors to consider when applying certain exemptions
- **Resources** – guides and fact sheets for citizens and agencies
- **Reporting** – external and internal reporting
- **Communications** – development of communication campaign, dedicated MNDB webpage, media releases, presentations, etc

Preventing and Mitigating Data Breaches

- **Robust Data Governance Framework** – policies and procedures covering every part of the data lifecycle
- **Data Breach Response Plan** – Data breach response team
- **Multi-Factor Authentication** – for staff logging into agency systems
- **Don’t use email to store or share personal information**
- **Access Controls** – for agency systems, as well as access audits
- **Email Client Software**
- **Regular training for staff and contractors in privacy and cyber security**
- **Consider third party risks**

Privacy and Personal Information Protection Amendment Bill 2022

Links to additional content

- **IPC Website:** The IPC website has a dedicated MNDB page which will be regularly updated in the lead up to the scheme: www.ipc.nsw.gov.au/privacy/MNDB-scheme
- **NSW Parliament website:** The legislation is also available to view via the NSW Parliament website: www.parliament.nsw.gov.au/bills/Pages/bill-details.aspx?pk=4040

Connect with us

www.ipc.nsw.gov.au

ipcinfo@ipc.nsw.gov.au

1800 472 679

/company/information-and-privacy-commission-nsw

@IPCNSW

/InformationandPrivacyCommissionNSW

www.youtube.com/user/IPCNSW

Responses to Questions

Third Party Providers

Under the MNDB Scheme, an agency is taken to 'hold' personal information if:

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

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, 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.

Responses to Questions

Third Party Providers (cont.)

Agencies holding personal information in systems or platforms provided by private sector service providers should ensure that procurement contracts include clauses providing:

- 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.

More information can be found in section 3.6 and 3.7 of the Guide to managing data breaches in accordance with the PPIP Act.

For concerns regarding cloud solutions, please see IPC guidance – Transition to the Cloud: Managing your agency's privacy risks.

Responses to Questions

Resources

Guidelines being released by the IPC

The Guidelines on Assessing a Data Breach will be provided to Ministers for consultation in late August. The IPC hopes to have them finalised for publication by late September and made available via the IPC website.

MNDB templates

The IPC will be publishing its own Data Breach Policy and Data Breach Public Register, which agencies can view, in coming weeks. Advice on the information that should be included in the Data Breach Incident Register and Notification Register is provided in the Guide to managing data breaches (section 3.4).

The form for Data Breach Notification to the Privacy Commissioner can be accessed here. Should you wish to use a static URL (which will not change if the form is updated) you are also able to link to: https://www.ipc.nsw.gov.au/media/3710. The notification form is outlined in section 59M of the legislative amendments.

Plans and policies

It is recommended that agencies establish clear roles and responsibilities for managing a data breach or suspected data breach. These should be documented in the agency's Data Breach Policy, and should include:

- Clear guidance for agency heads, executive officers, privacy officers, staff and any other personnel of their roles and functions in relation to identifying, reporting and responding to a breach or suspected breach.
- The constitution of the agency's data breach response team, including:
    - The roles and functions within the team.
    - Subject matter expertise required in the team (this could include incident response specialists, legal, communications, cybersecurity, physical security, human resources, key agency operations staff, key outsourcing/relationship managers).
    - Delineation of responsibility for dealing with relevant elements of a breach within that team.

Responses to Questions

Plans and policies (cont.)

- Escalation procedures for staff, including how to immediately report a suspected breach and when line managers can handle a breach.
- The circumstances in which a breach should be escalated to the response team.
- Responsibility for:
  - Escalation decisions at each level
  - Determining reporting obligations including notification to the IPC, affected individuals, external stakeholders or other bodies
  - Maintaining, testing and updating the Data Breach Policy
  - Record keeping
  - Post-breach review and evaluation.

See the Guide to preparing a Data Breach Policy for further information.

The MNDB Scheme takes effect on 28 November 2023 and agencies are expected to comply with the Scheme from that date. The IPC recommends that agencies update their PMP so the updated version is ready to go live on their website just before or when the Scheme commences. The IPC will not need to review your Data Breach Policy ahead of the Scheme.

Your agency's Data Breach Policy may include outlining roles and responsibilities, however depending on your agency's size and scale you may wish to also have an internal policy in place further outlining this or included in any separate Data Breach Response Plan.

Responses to Questions

Assessment, reporting and notifications

The MNDB Scheme comes into effect on 28 November 2023 and is not retrospective. Breaches identified from 28 November 2023 will be subject to the Scheme's requirements.

The Scheme requires any officer or employee of an agency with reasonable grounds to **suspect** that an eligible data breach has occurred, to report this suspected breach to the head of the agency or their delegate, who must immediately make all efforts to contain the breach and must carry out an assessment of whether the data breach is an eligible data breach within 30 days.

The 30 days for assessment commences when an agency employee becomes aware there are reasonable grounds to suspect that an eligible data breach has occurred. The employee must report the suspected data breach to the head of the agency, The Scheme requires the head of an agency to **immediately** notify the Privacy Commissioner if an eligible data breach has occurred. The head of the agency is required to use the approved form for notifying the Privacy Commissioner of the breach, which asks a number of questions relating to the breach. The responses to those questions will assist the IPC to assess whether the agency is meeting the requirement for immediate notification of the breach to the Privacy Commissioner.

The PPIP Act provides that head of the agency may direct one or more persons to carry out the assessment (the 'assessor'). The Scheme does prescribe or limit the number of people an agency head can delegate authority to. The head of the agency may delegate their authority in keeping with the usual practice of the agency.

An assessor may be:

a) An officer or employee of the agency subject to the breach.

b) 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.

c) 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.

If the head of the agency 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.

Responses to Questions

Assessment, reporting and notifications (Cont.)

For a data breach to constitute an 'eligible data breach' under the 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.

A data breach only needs to be notified to the Privacy Commissioner if both of these tests are satisfied.

If an eligible data breach is identified, the agency is required to notify the Privacy Commissioner of the breach. The IPC will treat all notifications to the Privacy Commissioner as eligible data breaches under the Scheme. The agency is responsible for assessing the data breach and notifying the Privacy Commissioner and affected individuals if it is assessed as an eligible data breach.

An agency may be exempt from notification requirements to affected individuals where:

- Mitigation action taken by the agency has prevented any likely serious harm resulting from the breach.

If the agency is unable to notify, or if it is not reasonably practicable for the agency to notify, any or all of the affected individuals, the agency must publish a notification and take reasonable steps to publicise it. The notification should contain the same information as a notification made directly to an affected individual, with the exception of any personal information or information that would prejudice the agency's functions.

Agencies must maintain and publish (on their website) a public notification register for any public data breach notifications that the agency has issued.

The IPC expects that the register should contain the following information:

1. the date the breach occurred
2. a description of the breach

Responses to Questions

Assessment, reporting and notifications (Cont.)

3. the type of breach (unauthorised access, unauthorised disclosure or loss of information)
4. how the breach occurred
5. the type of personal information that was impacted by the breach
6. actions taken or planned to ensure that personal information is secure or to mitigate harm to individuals
7. recommended steps individuals should take in response to the breach
8. date the public notification was published
9. where to contact for assistance or information
10. a link to the full public notification.

Personal information relating to individuals should not be placed on the public register. The purpose of the register is to ensure that citizens are able to 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.

Any public notification made by the agency must be published on the public notification register and remain available for at least 12 months after the date of publication.

Responses to Questions

Public Disclosure Act 2022

When the *Public Disclosure Act 2022* comes into effect on 1 October 2023, the Privacy Commissioner will be prescribed as an agency for the purposes of the Act and will be able to receive PIDs about privacy contraventions.

The aim of the PID Act is to enable the reporting of “serious wrongdoing”. The IPC will be providing information on its website about PIDs relating to a privacy contraventions prior to the new Act taking effect.

Definitions within guidance

The MNDB Scheme Guideline on Assessing a Data Breach will provide information about the definitions of ‘reasonableness’ and ‘likely to cause harm’. The guideline will be available on the IPC website in coming months, once consultation with Ministers has been finalised.

information and
privacy commission

new south wales