ODPP
New South Wales

ODPP – Data Breach Policy

SEPTEMBER 2023

Contents

1. Introduction 3
2. Scope 3
3. Purpose 3
4. The Mandatory Notification of Data Breach (MNDB) Scheme 3
5. Key Responsibilities 4
6. What is a data breach? 5
7. What is an 'eligible data breach'? 5
8. What is 'serious harm?' 6
9. Responding to a data breach 6
    - 9.1. Step 1 Initial Assessment and Triage 7
    - 9.2. Step 2 Contain the breach 7
    - 9.3. Step 3 Mitigate the risks 8
    - 9.4. Step 4 Notify 9
    - 9.5. Step 5 Register 11
    - 9.6. Step 6 Prevent a repeat 11
    - 9.7. Step 7 Other data breaches 11
10. Document ownership, control and history 12

Appendix A – Template Correspondence 13

Appendix B - Public MNDB Scheme Register 14

1. Introduction

This policy sets out the ODPP procedures for managing data breaches, including the relevant considerations for notifying persons whose privacy may be affected by the breach.

Effective data breach management, including notification where required, assists the ODPP to avoid or reduce possible harm to both the affected individuals/organisations and the ODPP, and may prevent future breaches.

This policy forms part of the IMTC Information Security Framework IMTC - Information Security Management Framework , the ODPP Information Security Policy Information Security Policy, and the ODPP Privacy Management Plan Privacy.

2. Scope

This policy applies to all staff and contractors of the ODPP. This includes temporary and casual staff, private contractors and consultants engaged by the ODPP.

3. Purpose

The purpose of this policy is to provide guidance to ODPP staff in responding to a data breaches, especially personal information and to comply with the Mandatory notification of data breach scheme.

This policy sets out the ODPP procedures for managing a data breach including:

- examples of situations considered to be a data breach
- the steps involved in responding to a data breach
- template correspondence for notifying persons whose privacy may be affected by the breach
- procedures for maintaining a public register of eligible data breaches.

4. The Mandatory Notification of Data Breach (MNDB) Scheme

The mandatory notification of data breach scheme (MNDB) now requires public sector agencies including the ODPP to notify the Privacy Commissioner and the affected individuals of data breaches involving personal or health information that are likely to result in serious harm. As part of the scheme the ODPP is also required to publish a data breach policy on its website, which outlines the Office's overall strategy for managing data breaches. The ODPP must also maintain a register of eligible data breaches as set out at 9.5 of this policy.

5. Key Responsibilities

Director of Public Prosecutions	Co-ordinate the ODPP response to data breaches and respond to inquiries from Government agencies and the public about a data breach. Make the final determination about whether a data breach is an 'eligible data breach' and notify the Privacy Commissioner of eligible breaches under the MNDB scheme.
Privacy Officers (Deputy Solicitor (Legal) and Deputy Solicitor (Legal Operations)	Ensure the ODPP addresses breach of privacy considerations arising from a data breach, evaluate the risks and assist the Director to take appropriate action to notify the Privacy Commissioner, other organisations and individuals about any data breaches. Work with the Director IM&T to prevent a repeat. Raise awareness of this Policy.
Director IM&T	Ensure all necessary steps are taken to ensure the breach is contained. Assist the Privacy Officers evaluate the risks prevent a repeat.
Managers	Assist staff to identify and act on data breaches. Notify the Director IM&T and Privacy Officers immediately of any breach. Assist Privacy Officers to evaluate the risks associated with the breach.
ODPP Staff Statutory appointees (including Crown Prosecutors) Contractors Volunteers	Immediately report data breaches to their manager and take any action they are able to contain the breach. Assist the Privacy Officers to identify personal information that is the subject of the breach and evaluate the risks associated with the breach.
IM&T Team	Provide support to ODPP staff to contain a data breach and identify evidence about the breach. Assess whether the breach impacts other agencies within NSW Government. Report cyber incidents and data breaches related to IT systems to Cyber Security NSW.

6. What is a data breach?

A data breach occurs when there is a failure that has caused or has the potential to cause unauthorised access or unauthorised disclosure to ODPP data, such as:

- accidental loss or theft of sensitive material or data or equipment on which such data is stored (e.g. loss of a paper record, laptop, tablet or mobile phone or USB stick)
- unauthorised use, access to or modification of data or information systems (e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to data or information systems)
- unauthorised disclosure of sensitive material or personal information (e.g. an email sent to the wrong recipient or document posted to an incorrect address or addressee)
- compromised user account (e.g. accidental disclosure of user login details / information through phishing)
- failed or successful attempts to gain unauthorised access to ODPP information or information systems
- equipment failure
- malware infection (e.g. ransomware)
- disruption to or denial of IT services (e.g. Denial of Service activity).

A data breach most commonly, but not exclusively, results in unauthorised access to, or the unauthorised collection, use or disclosure of, personal information.

7. What is an 'eligible data breach'?

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 the organisation or individual to whom the information relates.[1]

[1] S59B PPIP Act

8. What is 'serious harm?'

The term 'serious harm' is not defined in the *Privacy and Personal Information Protection Act 1998* (PPIP Act). Serious harm that can arise as the result of a data breach is context-specific and will vary based on:

- the type of personal information accessed, disclosed or lost, and whether a combination of types of personal information might lead to increased risk
- the level of sensitivity of the personal information accessed, disclosed or lost
- the amount of time the information was exposed or accessible, including the amount of time information was exposed prior to the agency discovering the breach
- 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)
- the circumstances in which the breach occurred, and
- actions taken by the agency to reduce the risk of harm following the breach.

Serious harm occurs where the harm arising from the eligible data breach has, or may, result in a real and substantial detrimental effect. The effect 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 ODPP's position would identify as a possible outcome of the data breach.

9. Responding to a data breach

Depending on the size or nature of a data breach, the consequences for individuals can be significant. Data breaches can also have serious consequences for government agencies. A breach may create risk through the disclosure of sensitive information, or otherwise impact an agency's reputation and lead to a loss of trust and confidence in an agency and the services it provides. The ODPP deals with both sensitive and personal information. It is important that any suspected data breaches are responded to promptly.

The Privacy Officers and the Director of IM&T must be informed of any data breach to ensure the application of this policy, provide advice to the Director of Public Prosecutions (the Director) to assist in responding to enquiries made by the public, and manage any complaints that may be received as a result of the breach.

The MNDB scheme also imposes the following obligations on agencies where there are reasonable grounds to suspect an eligible breach may have occurred:

1. initial assessment and triage
2. contain the breach
3. mitigate the risks
4. notify
5. register
6. prevent a repeat.

The ODPP's compliance with each step is set out in further detail below. The first four steps should be carried out concurrently where possible. The last two steps provide opportunities for recommendations to be made about longer-term solutions and prevention strategies.

9.1. Step 1 Initial Assessment and Triage

Any suspected data breaches should be reported immediately to the Privacy Officers or the Director IM&T who will conduct an initial assessment and triage.

The Privacy Officers or Director IM&T will assess the following

i) whether there has been unauthorised access to, or unauthorised disclosure of, personal information, or a loss of personal information held by the ODPP in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information, and

ii) whether there is a likelihood of serious harm to any affected individual.

Both assessments will be conducted within 30 days.[2] The Privacy Officers or Director IM&T will then make a recommendation to the Director or her delegate as to whether the breach should be considered an 'eligible data breach'.

9.2. Step 2 Contain the breach

Containing the breach is the priority of the ODPP. All necessary steps possible must be taken to contain the breach and minimise any resulting damage. For example, recover the personal information, shut down the system that has been breached, suspend the activity that led to the breach, revoke or change access codes or passwords.

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

[2] S59(E)(2) PPIP Act

9.3. Step 3 Mitigate the risks

To determine what other steps are needed, an assessment of the type of data involved in the breach and the risks associated with the breach will be undertaken.

Some types of data are more likely to cause harm if it is compromised. For example, personal information, health information, and security classified information will be more significant than names and email addresses on a subscription list. Given the ODPP's prosecutorial function the release of matter related sensitive information, including personal or health information, will be treated very seriously. A combination of data will typically create a greater potential for harm than a single piece of data (for example an address, date of birth and bank account details, if combined, could be used for identity theft).

In addition to the factors set out in section 59H of the PPIP Act, factors to consider will include:

i) *Who is affected by the breach?*

The ODPP assessment will include reviewing whether individuals and organisations have been affected by the breach, how many individuals and organisations have been affected and whether any of the individuals have personal circumstances which may put them at risk of harm.

ii) *What was the cause of the breach?*

The ODPP assessment will include reviewing whether the breach occurred as part of a targeted attack or through inadvertent oversight. Was it a one-off incident, has it occurred previously, or does it expose a more systemic vulnerability? What steps have been taken to contain the breach? Has the data or personal information been recovered? Is the data or personal information encrypted or otherwise not readily accessible?

iii) *What is the foreseeable harm to the affected individuals/organisations?*

The ODPP assessment will include reviewing what possible use there is for the data or personal information. This involves considering the type of data in issue (such as health information, personal information subject to special restrictions under *s19(1) of the PPIP Act* if it could be used for identity theft, or lead to threats to physical safety, financial loss, or damage to reputation). Who is in receipt of the data? What is the risk of further access, use or disclosure, including via media or online? If matter related, does it risk embarrassment or harm to an individual and/or damage to the ODPP's reputation?

The ODPP will take all reasonable steps to mitigate any data breach.[3] The mitigation strategies will depend on the nature of the breach but may include things like resetting ODPP password, deceiving remote access and referral to other agencies if required.

The final decision about whether a breach is an 'eligible data breach' for the purposes of the MNDB scheme will be made by the Director or her delegate.[4]

[3] S59F PPIP Act
[4] S59J PPIP Act

9.4. Step 4 Notify

If the Director determines that an eligible data breach has occurred, the Director must comply with the mandatory notification scheme set out below:

i) Notify the Privacy Commissioner

Once the Director determines an eligible data breach has occurred, the ODPP must immediately notify the Privacy Commissioner about the breach in the approved form.[5]

ii) Determine whether an exemption applies

If one of the six exemptions set out in Division 4 of the MNDB Scheme applies in relation to an eligible data breach, the ODPP may not be required to notify affected individuals.

The Director is to receive advice from the Privacy Officers or the Director IM&T as to whether any of the exemption notification requirements apply. [6]

iii) Notify individuals

Unless an exemption applies, the ODPP is required to notify affected individuals or their authorised representative as soon as reasonably practicable. Notification should be made directly to the individual concerned or their authorised representative. Where the ODPP is unable to notify directly or it is not reasonably practicable to do so, notification must be made publicly.[7] This will be done via the ODPP's public register as set out at 9.5 of this policy.

For data breaches that are not 'eligible breaches' the ODPP will have regard to the impact upon individuals in recognition of the need to balance the harm and distress caused through notification against the potential harm that may result from the breach. There are occasions where notification can be counterproductive. For example, the information may be less sensitive and notifying individuals about a privacy breach which is unlikely to result in an adverse outcome for the individual may cause unnecessary anxiety and de-sensitise individuals to a significant privacy breach.

Factors the ODPP will consider when deciding whether notification is appropriate include:

- are there any applicable legislative provisions or contractual obligations that require the ODPP to notify affected individuals?
- what type of information is involved?
- what is the risk of harm to the individual/organisation?
- is this a repeated and/or systemic issue?
- what risks are presented by the mode of breach e.g. is it encrypted information or contained in a less secure platform e.g. email?

[5] S59M PPIP Act
[6] Ss59S-59X PPIP Act
[7] S59N PPIP Act, s59O PPIP Act

- does the breach relate to matter functions and include matter related material flowing from our prosecutorial function?
- what steps has the ODPP taken to avoid or remedy any actual or potential harm?
- even if the individual/organisation would not be able to take steps to rectify the situation, is the information that has been compromised sensitive, or likely to cause humiliation or embarrassment for the individual/organisation?

Notification should be done promptly to help avoid or lessen the damage by enabling the individual/organisation to take steps to protect themselves.

The method of notifying affected individuals/organisations will depend on the type and the scale of the breach, as well as practical issues such as having the contacted details of those affected.

Step 4 What to say

Section 59O of the *PPIP Act* sets out specific information that must, if reasonably practical, be included in the notification (also see Appendix A):

- the date the breach occurred
- a description of the breach
- how the breach occurred
- the type of breach that occurred
- the personal information included in the breach
- the amount of time the personal information was disclosed for
- actions that have been taken or are planned to secure the information, or to control and mitigate the harm done
- recommendations about the steps an individual should take in response to the breach
- information about complaints and reviews of agency conduct
- the name of the agencies that were subject to the breach
- contact details for the agency subject to the breach or the nominated individual to contact about the breach.

9.5. Step 5 Register

The ODPP will maintain an internal register for eligible data breaches.[8] Each eligible data breach must be entered on the register by the Privacy Officers, with the following information included for each entry where practicable:

1. who was notified of the breach
2. when the breach was notified
3. the type of breach
4. details of steps taken by the public sector agency to mitigate harm done by the breach
5. details of the actions taken to prevent future breaches
6. the estimated cost of the breach.

The ODPP will also maintain and publish on its website a public notification register for any public data breach notifications that the ODPP has issued.[9] See template at Appendix B.

9.6. Step 6 Prevent a repeat

The ODPP will investigate the circumstances of the breach to determine all relevant causes and consider what short or long-term measures could be taken to prevent any reoccurrence.

Preventative actions could include a:

- security audit of both physical and technical security controls
- review of policies and procedures
- review of staff/contractor training practices; or
- review of contractual obligations with contracted service providers

9.7. Step 7 Other Data Beaches

As a matter of good practice, the Privacy Officers will notify the NSW Privacy Commissioner of any non-eligible data breaches where personal information has been accessed and there are risks to the privacy of individuals. In doing so the ODPP will ensure that relevant evidence is contained and secured for access by the Privacy Commissioner should regulatory action be considered appropriate. Such notification will:

- demonstrate to the affected individuals and the public that the ODPP views the protection of personal information as an important and serious matter and may therefore maintain public confidence in the ODPP.
- facilitate full, timely and effective handling of any complaints made to the Privacy Commissioner in regard to the breach and thus assist those whose privacy has been breached.

[8] S59ZE PPIP Act
[9] 59P PPIP Act

10. Document ownership, control and history

Version	Endorsed by Committee	Approved	Approved by the Director
1	Information Management Technology Committee	31 July 2023	7 August 2023

Appendix A – Template Correspondence

«Date»

Dear «Name»

«Subject»

I write to you with important information about a recent data breach involving your personal information/ information about your organisation. The ODPP became aware of this breach on «date».

The breach occurred on or about «date» and occurred as follows:

«Details»

[Describe the event, including as applicable, the following:

- *a brief description of what happened*
- *description of the data that was inappropriately access, collected, used or disclosed*
- *risks to the individual/organisation caused by the breach and amount of time personal information was disclosed for*
- *steps the individual/organisation should take to protect themselves from potential harm from the breach*

a brief description of what the ODPP is doing to investigate the breach, control or mitigate harm to individuals/organisations and to protect against further breaches.] We take our role in safeguarding your information and using it in an appropriate manner very seriously. Please be assured that we are doing everything we can to rectify the situation.

Please note that under the «PIPP/HRIP/GIPA» Act you are entitled to register a complaint with [*check whether complaint first to Privacy Officer at ODPP]* the NSW Privacy Commissioner or NSW Information Commissioner with regard to this breach. Complaints may be forwarded to the following:

«Details»

Should you have any concerns or questions regarding this notice or if you would like more information, please do not hesitate to contact me (insert contact details here).

Yours faithfully

Privacy Officer

Appendix B - Public MNDB Scheme Register

Description of Data Breach	Action taken
Date of Breach - «date» **Description -** «description» **Type -** «Type» **Mechanism** - «Mechanism»	Notification - «details» Containment - «details»
Description of Risks	**Action required**
Type of data - «type» **Risk** - «risk» **Harm** - «harm» **Affecting** - «affecting»	**Eligible date breach** - «Yes/No» **Mandatory reporting** – «Yes/No» **Public notification** - «Yes/No», «date»
Description of Causes	**Action proposed**
How - «how» **Why** - «why»	Change Train Remind Review Stop Media Remedy
Notification to the NSW Privacy Commissioner	

Signed

Director, Information Management & Technology
Privacy Officer