Independent
Review Office

IRO Data Breach Policy

December 2023

Contents

Document Data

Policy Owner	Independent Review Officer
Compliance required by	All staff, contractors
Approved by	Independent Review Officer
Date created	November 2023
Next review due	November 2026
Drivers	*Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act), Part 6A, section 59ZD *Health Records and Information Privacy Act 2002* (NSW) (HRIP Act)
Legislative compliance	**Commonwealth Legislation** *Privacy Act 1988* *Privacy Amendment (Notifiable Data Breaches) Act 2017* **New South Wales Legislation** *Privacy and Personal Information Protection Act 1998* *Health Records and Information Privacy Act 2002* *State Records Act 1998*
Reference	DCS Data Breach Policy DCS Data Breach Response Procedure
Contact officer	Principal Policy Officer
Compliance assurance	Incident monitoring, annual reporting, data breach register
Policy location	On the IRO website: https://iro.nsw.gov.au/about-us/public-access-information/privacy-statement

Revision History

Version	Approved by	Amendment notes
1	Independent Review Officer and IRO Executive	-

1. About the IRO

The Independent Review Officer is an independent statutory office established under the *Personal Injury Commission Act 2020* (NSW) (PIC Act).

The Officer is supported by an expert team of staff; collectively this is the IRO. The statutory functions of the IRO include to:

- find solutions for persons injured at work or in motor vehicle accidents with complaints about their insurers
- manage and administer the Independent Legal Assistance and Review Service (ILARS)
- conduct inquiries into matters arising in connection with the operation of the PIC Act and the workers compensation and motor vehicle accident legislation.

1.1 Our structure

The work of the IRO is conducted by three specialist groups:

Solutions Group

This team investigates and resolves complaints made by persons injured at work or in motor vehicle accidents about the acts or omissions of insurers.

Independent Legal Assistance and Review Service (ILARS)

ILARS is operated by Principal Lawyers, paralegals and administrative assistants who assess and manage applications for grants of funding from independent IRO Approved Lawyers to provide legal advice and assistance to injured workers.

Strategy, Policy and Support (SPS)

This team is responsible for the development of policy recommendations, engagement, education and communication with IRO stakeholders.

2. Data Breach Policy

2.1 Purpose

The Data Breach Policy (Policy) explains how we fulfill our obligation under NSW privacy laws to handle breaches of personal and health information. The consequences of a data breach for users of our services can be significant. Effective data breach management helps to prevent repeated incidents and avoid or reduce harm to those who use our services.

The relevant legislation is:

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

Health Records and Information Privacy Act 2002 (NSW) (HRIP Act)

The Policy outlines the processes to contain, assess, manage and notify an eligible data breach under the Mandatory Notification of Data Breach (MNDB) scheme established by Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act).

Notifying individuals affected by a privacy breach can enable them to take steps to mitigate the consequences the breach. It is also a positive step IRO can take to help rebuild trust with the affected individuals. Notifying the NSW Privacy Commissioner improves oversight of the data breach response, from initial notification through to additional learnings that arise in notifying individuals. Notification also allows the Privacy Commissioner to provide a more comprehensive report to government and Parliament on data breaches experienced across the NSW public sector.

2.2 What is a data breach?

A data breach occurs where there is:

- an unauthorised access to, or unauthorised disclosure of, personal or health information held by a public sector agency or,
- loss of personal or health information held by a public sector agency in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information.

2.3 What is an 'eligible' data breach?

The MNDB Scheme applies where an 'eligible data breach' has occurred.

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 or health 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 if it is 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 any of the individuals to whom the information relates.

Whether a data breach is 'likely to result' in serious harm requires determination from the perspective of a reasonable person and on the facts of the specific breach in question. Serious harm to an individual may include, but is not limited to, serious physical harm; economic, financial or material harm; emotional or psychological harm; and financial or reputational harm.

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. That is, the effect on the individual must be more than mere irritation, annoyance, or inconvenience.

2.4 Data Breach Response Procedure

IRO maintains a Data Breach Response Procedure (Procedure) document which sets out the roles and responsibilities for managing the response to a data breach. The Procedure provides guidance for how IRO will manage and respond to a data breach and includes:

- steps IRO staff need to take to contain, assess, report and review data breaches quickly, and mitigate potential harm to affected individual(s)
- more details on roles and responsibilities of IRO staff when responding to a data breach
- guidance on when to notify data breaches to individual(s), as well as the NSW Privacy Commissioner

IRO has controls in place to ensure it is prepared in the event of a data breach:

- mandatory staff training on our obligations under privacy legislation
- internal resources to help staff identify and report a suspected data breach
- attendance at a regular forum of privacy practitioners from across the Department of Customer Service (DCS) to discuss learnings from breaches and opportunities to strengthen data breach management
- maintaining and continually improving information security management systems that comply with ISO/IEC 27001:2022 standard
- aligning our obligations under the DCS Cyber Security Policy
- adopting best practice in electronic and paper records management and complying with our obligations under the *State Records Act 1998* (NSW), including keeping information for only as long as necessary
- providing mandatory information security awareness training to IRO employees via DCS
- provisions in contracts to require contractors and third-party providers to assist IRO in complying with our obligations under privacy legislation, notification and management of data breaches.

To support compliance with the PPIP Act, IRO staff must respond to a data breach in accordance with the IRO Data Breach Response Procedure, which is updated from time to time, and includes the following four stages of responding to a data breach.

1. Report and advise
2. Assess and mitigate the risks associated to determine next steps
3. Consider notification to the Privacy Commissioner and affected individuals, where applicable
4. Review and report on the breach

The Procedure is aligned with this Policy and the IRO Privacy Management Plan and applies to all IRO staff and covers all data breaches involving personal and/or health information held by IRO.

3. Roles and responsibilities

3.1 All IRO Staff

All IRO staff are responsible for immediately reporting a suspected or actual data breach to their Team Leader/Manager or the IRO Privacy Officers across the Strategy Policy and Support (SPS), Solutions and ILARS Teams.

3.2 Team Leaders and Managers

Team leaders and Managers should review existing processes and identify how internal controls could be strengthened. This helps ensure the incident is contained and reduce the risk of it happening again in the future. They must also notify their Privacy Officer and Director.

3.3 Head of the Agency (Independent Review Officer)

It is the Head of Agency or their delegate's responsibility to assess whether the breach is an eligible data breach and if so, notify the Privacy Commissioner and affected individuals.

3.4 Privacy Officers at IRO

Privacy Officers are a central point of contact within a business area in all matters related to privacy. In the event of a data breach, the Privacy Officer manages the relevant area's breach response and provides advice to the Team Leader/Manager reporting the incident. At IRO, the Privacy Officers are nominated annually in each division, including SPS, Solutions and ILARS Teams. The Privacy Officers meet quarterly.

3.5 Breach Management Team

A Breach Management Team (BMT) may be stood up by the relevant Privacy Officer(s) to respond to complex data breaches. The BMT is constituted in accordance with the Data Breach Response Procedure and can be scaled depending on the size of the data breach, the resources required to respond, and the number of agencies affected. It can be made up of IRO staff from across relevant areas such as Policy, Information Security and Communications, as well as from other agencies as required, for example DCS, that may assist in responding to the breach.

The BMT will act as the single point of management of the breach and coordinate with external agencies. The head of the BMT will assess the need for and provide notification to the Privacy Commissioner and individuals.

At IRO, the Breach Management Team comprises members of the IRO Executive and representatives from each group across IRO, including information management subject matter experts.

4. Record keeping requirements

4.1 Data Breach Register

IRO maintains an internal register for data breaches, including eligible data breaches. For eligible data breaches where we are unable or it is not practicable to notify individuals, IRO will publish a notification on our website. The Data Breach Register is a requirement under the MNDB scheme, including details of the following:

- who was notified of the breach
- when the breach was notified
- the type of breach
- details of steps taken by IRO to mitigate harm done by the breach
- details of the actions taken to prevent future breaches
- the estimated cost of the breach.

Information about every data breach is recorded regardless of whether a BMT is formed, or the breach amounts to an eligible data breach.

Tracking data breaches allows IRO to monitor, analyse and review the type and severity of suspected breaches along with the effectiveness of the response methods. IRO will use this information to identify and improve weaknesses in security or processes.

5. Where we may not notify

We may not notify individuals in certain circumstances including:

- where multiple agencies are involved in an eligible breach and one of those agencies has provided notification
- where an eligible data breach would prejudice an ongoing investigation and certain proceedings
- where IRO has taken action before the data breach results in harm or loss to individuals
- where notification results in serious harm to an individual
- where compliance would be inconsistent with secrecy provisions of other legislation
- where compliance would result in serious risk of harm to health and safety
- where compliance would worsen IRO or DCS cyber security or lead to further data breaches

6. Post-breach review and evaluation

Following data breaches, the Privacy Officer(s) or BMT undertakes a post-breach review and drafts a report outlining the cause of the breach, identifying strategies to address any weaknesses in data handling that may have led to the breach.

The post-breach review assesses IRO's response to the breach and should consider:

- an investigation of the cause of the breach
- implementing a strategy to identify and address any weaknesses in data handling that contributed to the breach
- updating the Data Breach Response Procedure if necessary
- making appropriate changes to policies and procedures if necessary
- revising staff training practices if necessary
- the option of an audit to ensure necessary outcomes are affected
- whether the response team needs other expertise
- the preservation of evidence to determine the cause of the breach or allowing the Privacy Commissioner to take appropriate corrective action
- a communications or media strategy to manage public expectations and media interest.

7. Contact Information

If you suspect that your personal and/or health information has been breached by IRO, you can contact us at privacy@iro.nsw.gov.au.