RIVERSIDE ACCESS

2025

RIVERSIDE ACCESS DATA BREACH POLICY

DOCUMENT DETAILS

Version	Date Amended	Person Responsible	Date for next review (Min: Every 2 Years)
2025 Version 1	22/1/2025	Kate Bevan	22/1/2027

CONTENTS

DATA BREACH POLICY

PURPOSE

The Data Breach Policy explains how Riverside Access handles 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.

WHAT IS A DATA BREACH?

A data breach occurs when personal information that an entity holds is subject to unauthorised access or disclosure, or is lost. Personal information is information about an identified individual, or an individual who is reasonably identifiable.

Entities should be aware that information that is not about an individual on its own can become personal information when it is combined with other information, if this combination results in an individual becoming 'reasonably identifiable' as a result. A data breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems.

CONSEQUENCES OF A DATA BREACH

Individuals whose personal information is involved in a data breach may be at risk of serious harm, whether that is harm to their physical or mental wellbeing, financial loss, or damage to their reputation. Examples of harm include:

- financial fraud including unauthorised credit card transactions or credit fraud
- identity theft causing financial loss or emotional and psychological harm
- reputational damage
- embarrassment or humiliation
- emotional distress
- family violence
- physical harm or intimidation.

Organisations can also suffer harm as a result of a data breach. Responding to the initial breach and subsequent complaints may have financial, legal and resource implications. Furthermore, data breaches can result in reputational damage and a loss of public trust.

OUR OBLIGATIONS

The *Riverside Access Privacy Policy* outlines the steps taken by Riverside Access to protect the privacy of personal information that Riverside Access comes into contact with. The Privacy Policy outlines the procedures for collection, storage, use, disclosure, and destruction of personal information. Adherence to the Privacy Policy will reduce the risk of a data breach occurring.

If there are reasonable grounds to believe an 'eligible data breach' has occurred the General Manager must notify the Office of the Australian Information Commissioner (OAIC) and affected individuals as soon as practicable. Eligible data breaches arise when:

1. personal information held by the entity is lost or subjected to unauthorised access or disclosure (a 'data breach')
2. the breach is likely to result in serious harm to individuals to whom the information relates
3. the entity has not been able to prevent the risk of serious harm with remedial action.

If it is impracticable to notify the affected individuals then a copy of the statement will be published on the Riverside Access website and reasonable steps will be taken to bring its contents to the individuals' attention.

The statement must include the following information:

- Riverside Access' contact details
- a description of the data breach believed to have occurred
- a description of the kinds of information concerned
- recommendations about the steps individuals should take to avoid or mitigate harm from the data breach.

NOTE: If an entity acts quickly to remediate a data breach, and as a result of this action the data breach is not likely to result in serious harm, there is no requirement to notify any individuals or the OAIC.

DATA BREACH RESPONSE PLAN

IDENTIFYING ELIGIBLE DATA BREACHES

STEP 1:

Determine if a data breach has occurred (unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information). If a staff member has reason to believe a data breach has occurred, they are to report to the General Manager immediately.

STEP 2:

The General Manager will then decide whether, from the perspective of a reasonable person, the data breach would be likely to result in serious harm to an individual whose personal information was part of the data breach.

For the Notifiable Data Breaches (NDB) scheme a 'reasonable person' means a person in the entity's position (rather than the position of an individual whose personal information was part of the data breach or any other person), who is properly informed, based on information immediately available or following reasonable inquiries or an assessment of the data breach. In general, entities are not expected to make external enquiries about the circumstances of each individual whose information is involved in the breach.

The phrase 'likely to result' means the risk of serious harm to an individual is more probable than not (rather than possible).

The General Manager should assess the risk of serious harm holistically, having regard to the likelihood of the harm eventuating for individuals whose personal information was part of the data breach and the consequences of the harm. The NDB scheme includes a non-exhaustive list of 'relevant matters' that may assist entities to assess the likelihood of serious harm. These are set out in s 26WG as follows:

- the kind or kinds of information
- the sensitivity of the information
- whether the information is protected by one or more security measures
- if the information is protected by one or more security measures – the likelihood that any of those security measures could be overcome
- the persons, or the kinds of persons, who have obtained, or who could obtain, the information
- if a security technology or methodology:
    - was used in relation to the information, and
    - was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information
- the likelihood that the persons, or the kinds of persons, who:
    - have obtained, or who could obtain, the information, and
    - have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates
    - have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology
- the nature of the harm
- any other relevant matters.

EXAMPLE CASES:

Example 1: Strong encryption making notification unnecessary

Insure, an insurance company, decides to update its customer relationship management and record keeping software. While running a test, the IT team installing the software discovers that some customer records were accessed by an unauthorised third party more than a year ago. The customer records involved are primarily encrypted payment card information.

Since Insure suspects fraudulent activity as the motive for the unauthorised access, it notifies the police and hires an external IT security consultant to conduct an audit and security assessment. The audit confirms that 500 customer records were involved in the data breach, and that an overseas source was responsible for the hack. The IT security consultant's comprehensive sweeps of the internet and dark web were unable to find evidence that the information was offered for sale or otherwise disclosed online. The IT security consultant also assesses that because of the high standard of encryption used for the credit card information, it is unlikely that this information could be accessed by the hacker. Insure implemented the recommendations of its IT security consultant, including new IT security protocols and intrusion detection software.

Insure determines that it is not likely that the individuals whose personal information is involved in the data breach are at risk of serious harm. Therefore, Insure decides it is not an eligible data breach, and is not required to notify affected individuals or the Commissioner.

Nonetheless, it decides that as a customer service measure, it should tell the individuals about the incident. It sends an email to the customers informing them of the incident and providing some advice on personal information security measures they can take. This notification is not required by the NDB scheme, so can take any form that Insure considers appropriate.

Example 2 :Notification following unintentional publication of sensitive data

Medicines, a chain of low-cost pharmacies, becomes aware that its customer database, including records about dispensing of prescription drugs, has been publicly available on the internet due to a technical error. Medicines' security consultants identify that the database was publicly available for a limited time and that it was only accessed a few times.

However, Medicines is unable to determine who accessed the data or if they kept a copy. Given the sensitivity of the personal information contained in the database, including drugs related to the treatment of addictive and psychiatric conditions, Medicines' risk assessment concludes that the data breach would be likely to result in serious harm to some of its customers.

Medicines decides to notify all customers whose personal information is involved in the data breach and the Commissioner. Because it does not have contact details for many of the customers who filled prescriptions with it in person, it publishes a notice describing the breach on its website and posts a copy in a prominent location at each of its stores.

PREVENTING SERIOUS HARM WITH REMEDIAL ACTION

The NDB scheme provides entities with the opportunity to take positive steps to address a data breach in a timely manner, and avoid the need to notify. If an entity takes remedial action such that the data breach would not be likely to result in serious harm, then the breach is not an eligible data breach for that entity or for any other entity (s 26WF(1), s 26WF(2), s 26WF(3)). For breaches where information is lost, the remedial action is adequate if it prevents unauthorised access to, or disclosure of personal information (s 26WF(3)).

If the remedial action prevents the likelihood of serious harm to some individuals within a larger group of individuals whose information was compromised in a data breach, notification to those individuals for whom harm has been prevented is not required.

An example of remedial action:

A data file, which includes the personal information of numerous individuals, is sent to an incorrect recipient outside the entity. The sender realises the error and contacts the recipient, who advises that the data file has not been accessed. The recipient has an ongoing contractual relationship with the sender, and regards the recipient as reliable and trustworthy. The sender then confirms that the recipient has not copied, and has permanently deleted the data file. In the circumstances, the sender decides that there is no likely risk of serious harm.

ASSESSING A SUSPECTED DATA BREACH

If Riverside Access' General Manager is aware of reasonable grounds to believe that there has been an eligible data breach, it must promptly notify individuals at risk of serious harm and the Commissioner about the eligible data breach. If the General Manager only has reason to suspect that there may have been a serious breach, they need to move quickly to resolve that suspicion by assessing whether an eligible data breach has occurred. If, during the course of an assessment, it becomes clear that there has been an eligible breach, then the General Manager needs to promptly comply with the notification requirements.

TIME FRAMES

The General Manager must take all reasonable steps to complete the assessment within 30 calendar days after the day they became aware of the grounds (or information) that caused them to suspect an eligible data breach (s 26WH(2)). This timeframe is a maximum and as such the General Manager must endeavour to complete the assessment in a much shorter timeframe.

Where an assessment cannot be reasonable completed within 30 days, the following should be documented:

- all reasonable steps have been taken to complete the assessment within 30 days
- the reasons for the delay
- proof the assessment was reasonable and expeditious.

STAGES OF ASSESSMENT (TO BE COMPLETED BY THE GENERAL MANAGER):

Stage 1 (Initiate): Decide whether an assessment is necessary and identify which person or group will be responsible for completing it.

Stage 2 (Investigate): Quickly gather relevant information about the suspected breach including, for example, what personal information is affected, who may have had access to the information and the likely impacts.

Stage 3 (Evaluate): Make a decision, based on the investigation, about whether the identified breach is an eligible data breach. Once it has been established that there are reasonable grounds to believe that there has been an eligible data breach (whether during the course of an assessment, or when the assessment is complete) the General Manager must promptly notify affected individuals and the Commissioner about the breach. The General Manager will document the assessment process and outcome.

NOTE: At any time, including during an assessment, the General Manager can, and should, take steps to reduce any potential harm to individuals caused by a suspected or eligible data breach. If remedial action is successful in preventing serious harm to affected individuals, notification will not be required.

NOTIFYING INDIVIDUALS ABOUT AN ELIGIBLE DATA BREACH

Once the General Manager has reasonable grounds to believe there has been an eligible data breach, they must, as soon as practicable, make a decision about which individuals to notify, prepare a statement for the Commissioner and notify individuals of the contents of this statement.

There are three options for notifying individuals at risk of serious harm:

Option 1: Notify all individuals

If it is practicable, the General Manager can notify each of the individuals to whom the relevant information relates(s 26WL(2)(a)). That is, all individuals whose personal information was part of the eligible data breach.

This option may be appropriate, and the simplest method, if the General Manager cannot reasonably assess which particular individuals are at risk of serious harm from an eligible data breach that involves personal information about many people, but where the General Manager has formed the view that serious harm is likely for one or more of the individuals.

The benefits of this approach include ensuring that all individuals who may be at risk of serious harm are notified, and allowing them to consider whether they need to take any action in response to the eligible data breach.

Option 2: Notify only those individuals at risk of serious harm

If it is practicable, the General Manager can notify only those individuals who are at risk of serious harm from the eligible data breach (s 26WL(2)(b)). That is, individuals who are likely to experience serious harm as a result of the eligible data breach.

The benefits of this targeted approach include avoiding unnecessary distress to individuals who are not at risk, limiting possible notification fatigue among members of the public, and reducing administrative costs, where it is not required by the NDB scheme.

Option 3: Publish notification

If neither option 1 or 2 above are practicable, for example, if the entity does not have up-to-date contact details for individuals, then the General Manager must:

- publish a copy of the statement on the Riverside Access Website
- take reasonable steps to publicise the contents of the statement (s 26WL(2)(c))

It is not enough to simply upload a copy of the statement prepared for the Commissioner on any webpage of the Riverside Access website. Riverside Access must also take proactive steps to publicise the substance of the eligible data breach (and at least the contents of the statement), to increase the likelihood that the eligible data breach will come to the attention of individuals at risk of serious harm.

Riverside Access will keep the statement accessible on their website for at least 6 months.

HOW DO I NOTIFY AND WHAT DO I NEED TO SAY

The General Manager can use any method to notify individuals (for example, a telephone call, SMS, physical mail, social media post, or in-person conversation), so long as the method is reasonable. In considering whether a particular method, or combination of methods is reasonable, the notifying entity should consider the likelihood that the people it is notifying will become aware of, and understand the notification, and weigh this against the resources involved in undertaking notification.

The entity can tailor the form of its notification to individuals, as long as it includes the content of the statement required by s 26WK. That statement (and consequently, the notification to individuals) must include the following information:

- the identity and contact details of the entity (s 26WK(3)(a))
- a description of the eligible data breach that the entity has reasonable grounds to believe has happened (s 26WK(3)(b)). Information may include:
    - the date, or date range, of the unauthorised access or disclosure
    - the date the entity detected the data breach
    - the circumstances of the data breach (such as any known causes for the unauthorised access or disclosure)
    - who has obtained or is likely to have obtained access to the information
    - relevant information about the steps the entity has taken to contain or remediate the breach.
- the kind, or kinds, of information concerned (s 26WK(3)(c))
- recommendations about the steps that individuals should take in response to the eligible data breach (s 26WK(3)(d)). Recommendations should include practical steps that are easy for the individuals to action. In the case the General Manager does not have the requisite knowledge or capacity to provide advice to affected individuals, they should seek specialist advice or assistance in preparing this section.

STEPS FOR PUBLISHING A NOTIFICATION

If affected persons are not able to be notified individually then the General Manager will publish a copy of the statement prepared for the Commissioner on the Riverside Access website, and take other reasonable steps to publicise the contents of that statement.

A reasonable step when publicising an online notice, might include:

- ensuring that the notice is prominently placed on the relevant webpage, which can be easily located by individuals and indexed by search engines
- publishing an announcement on the entity's social media channels
- taking out a print or online advertisement in a publication or on a website the entity considers reasonably likely to reach individuals at risk of serious harm.

NOTE: The General Manager should take care to ensure that the online notice does not contain any personal information. While it may help to provide a general description of the cohort of affected individuals, this

description should not identify any of the affected individuals or provide information that may make an individual reasonably identifiable.

NOTIFICATIONS OF DATA BREACHES TO THE COMMISSIONER

An online form is available on the OAIC website to help in the lodgment of notification statements and provide additional supporting information. https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach

The Commissioner's response to notifications

The Commissioner will acknowledge receipt of all data breach notifications.

The Commissioner may also make inquiries or offer advice and guidance in response to notifications. In deciding whether to make inquiries or offer advice and guidance in response to a notification, the Commissioner may consider the type and sensitivity of the personal information, the numbers of individuals potentially at risk of serious harm, and the extent to which the notification statement and any additional supporting information provided demonstrate that:

- the data breach has been contained or is in the process of being contained where feasible
- the notifying entity has taken, or is taking, reasonable steps to mitigate the impact of the breach on the individuals at risk of serious harm
- the entity has taken, or is taking, reasonable steps to minimise the likelihood of a similar breach occurring again.

The Commissioner may also decide to take regulatory action on the Commissioner's own initiative in response to a notification, or a series of notifications. In deciding whether to take regulatory action, the Commissioner will have regard to the OAIC's Privacy regulatory action policy and Guide to privacy regulatory action.

However, generally the Commissioner's priority when responding to notifications is to provide guidance to the entity and to assist individuals at risk of serious harm.

FOR MORE INFORMATION

More information can be found on the OAIC website: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response