Notifiable Data Breach Policy

Notifiable Data Breach Policy

Contents

1. Summary

This document describes the Policy for a potential or actual Data Breach.

Assetora is committed to managing personal information in accordance with the Privacy Act 1988 (Cth) (the Act) and the Assetora Privacy Policy.

This document sets out the processes to be followed by Assetora staff in the event that Assetora experiences a data breach or suspects that a data breach has occurred. A data breach involves the loss of, unauthorised access to, or unauthorised disclosure of, personal information.

The Privacy Amendment (Notifiable Data Breaches) Act 2017 (NDB Act) established a Notifiable Data Breaches (NDB) scheme requiring organisations covered by the Act to notify any individuals likely to be at risk of serious harm by a data breach. The Office of the Australian Information Commissioner (OAIC) must also be notified.

Accordingly, Assetora needs to be prepared to act quickly in the event of a data breach (or suspected breach), and determine whether it is likely to result in serious harm and whether it constitutes an NDB.

Adherence to this Procedure and Response Plan will ensure that Assetora can contain, assess and respond to data breaches expeditiously and mitigate potential harm to the person(s) affected.

This Procedure and Response Plan has been informed by:

- The OAIC's "Guide to developing a data breach response plan"
- The OAIC's "Data breach notification guide: a guide to handling personal information security breaches"
- NDB Act
- The Act and Australian Privacy Principles (Schedule 1 of the Act)

This document should be read in conjunction with Assetora's Privacy Policy.

2. What is Data Breach?

A data breach occurs when personal information that an entity holds is subject to unauthorized access or disclosure or is lost.

There needs to be three distinct criteria for the breach to be an eligible Data Breach. Eligible data breach

An eligible data breach arises when the following three criteria are satisfied:

1. there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds (see, what is a ‘data breach’?)
2. this is likely to result in serious harm to one or more individuals (see, Is serious harm likely?), and
3. the entity has not been able to prevent the likely risk of serious harm with remedial action (see, Preventing serious harm with remedial action).

What is a ‘data breach’?

The first step in deciding whether an eligible data breach has occurred involves considering whether there has been a data breach; that is, unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information (s 26WE(2)). The Privacy Act 1988 (Cth) (Privacy Act) does not define these terms. The following analysis and examples draw on the ordinary meaning of these words.

Unauthorised access of personal information occurs when personal information that an entity holds is accessed by someone who is not permitted to have access. This includes unauthorised access by an employee of the entity, or an independent contractor, as well as unauthorised access by an external third party (such as by hacking).

Some kinds of personal information may be more likely to cause an individual serious harm if compromised.Examples of the kinds of information that may increase the risk of serious harm if there is a data breach include:

- ‘sensitive information’, such as information about an individual’s health
- documents commonly used for identity fraud (including Medicare card, driver licence, and passport details)
- financial information
- a combination of types of personal information (rather than a single piece of personal information) that allows more to be known about the individuals the information is about.
- The nature of the harm

In assessing the risk of serious harm, Assetora should consider the broad range of potential kinds of harms that may follow a data breach. It may be helpful for entities assessing the likelihood of harm to consider a number of scenarios that would result in serious harm and the likelihood of each. Examples may include:

- identity theft

- significant financial loss by the individual
- threats to an individual's physical safety
- loss of business or employment opportunities
- humiliation, damage to reputation or relationships
- workplace or social bullying or marginalisation.

The likelihood of a particular harm occurring, as well as the anticipated consequences for individuals whose personal information is involved in the data breach if the harm materialises, are relevant considerations

3. Process and Procedure

3.1. Alert

Where a privacy data breach is known to have occurred (or is suspected) any member of Assetora staff who becomes aware of this must, within 24 hours, alert the Chief Executive Officer or the Risk and Compliance Officer.

The Information that should be provided (if known) at this point includes:

a) When the breach occurred (time and date)

b) Description of the breach (type of personal information involved)

c) Cause of the breach (if known) otherwise how it was discovered

d) Which system(s) if any are affected?

e) Which part of Assetora is involved?

f) Whether corrective action has occurred to remedy or ameliorate the breach (or suspected breach)

A template can be found at Annexure A to assist in documenting the required information.

3.2. Assess and determine the potential impact

Once notified of the information above, the Chief Executive Officer or Risk and Compliance Officer must consider whether a privacy data breach has (or is likely to have) occurred and make a preliminary judgement as to its severity. The Risk and Compliance Officer should be contacted for advice.

3.3.Criteria for determining whether a privacy data breach has occurred

a) Is personal information involved?

b) Is the personal information of a sensitive nature?

c) Has there been unauthorised access to personal information, or unauthorised disclosure of personal information, or loss of personal information in circumstances where access to the information is likely to occur?

For the purposes of this assessment the following terms are defined in section 9 of the Privacy Policy: personal information, sensitive information, unauthorised access, unauthorised disclosure and loss.

3.4.Criteria for determining severity

a) The type and extent of personal information involved

b) Whether multiple individuals have been affected

c) Whether the information is protected by any security measures (password protection or encryption)

d) The person or kinds of people who now have access

e) Whether there is (or could there be) a real risk of serious harm to the affected individuals

f) Whether there could be media or stakeholder attention as a result of the breach or suspect breach

With respect to 4.4(e) above, serious harm could include physical, physiological, emotional, economic/financial or harm to reputation and is defined in section 9 of the Privacy Policy and section c 26WG of the NDB Act.

Having considered the matters in 4.1 and 4.2, the Chief Executive Officer must notify the Risk and compliance Officer within 24 hours of being alerted under 4.1.

3.5.Risk and Compliance Officer to issue pre-emptive instructions

On receipt of the communication by the Chief Executive Officer under 4.2, the Risk and Compliance Officer will take a preliminary view as to whether the breach (or suspected breach) may constitute an NDB. Accordingly, the Risk and Compliance Officer will issue pre-emptive instructions as to whether the data breach should be managed at the local level or escalated to the Data Breach Response Team (Response Team). This will depend on the nature and severity of the breach.

3.6.Data breach managed at Assetora

Where the Risk and Compliance Officer instructs that the data breach is to be managed at Assetora, the Chief Executive Officer must:

- ensure that immediate corrective action is taken, if this has not already occurred (corrective action may include retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system); and
- submit a report via the Risk and Compliance Officer within 48 hours of receiving instructions under 3.3.

The report must contain the following:

1. Description of breach or suspected breach
2. Action taken
3. Outcome of action
4. Processes that have been implemented to prevent a repeat of the situation.
5. Recommendation that no further action is necessary

The Risk and Compliance Officer will be provided with a copy of the report and will sign-off that no further action is required.

The report will be logged by the Privacy Officer.

3.7.Data breach managed by the Response Team

Where the Risk and Compliance Officer instructs that the data breach must be escalated to the Response team, the Privacy Officer will convene the Response Team and notify the Chief Executive Officer.

3.8.Response Team & Duties Response Team

Risk and Compliance Officer Chief Commercial Officer (CCO) Head of IT

Chief Financial Officer (CFO) Chief Operating Officer (COO)

Primary role of the Response Team

There is no single method of responding to a data breach and each incident must be dealt with on a case-by-case basis by assessing the circumstances and associated risks to inform the appropriate course of action.

The following summary steps should be undertaken by the Response Team:

1. Contain the data breach to prevent any further compromise of personal information.
2. Assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.

3. Notify individuals and the Commissioner if required. If the breach is an 'eligible data breach' under the NDB scheme, it may be mandatory for the entity to notify about a serious data breach.

Generally, we would have 30 days to assess whether a data breach is likely to result in serious harm.

When a data breach occurs, we are expected to try to reduce the chance that an individual experiences harm. If successful, and the data breach is not likely to result in serious harm, we are not required to tell the individual about the data breach.

1. Review the incident and consider what actions can be taken to prevent future breaches. Process:
    - Immediately contain the breach (if this has not already occurred). Corrective action may include retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system.
    - Evaluate the risks associated with the breach, including collecting and documenting all available evidence of the breach having regard for the information outlined in sections 4.1 and 4.2 above.
    - Call upon the expertise of, or consult with, relevant staff in the particular circumstances.
    - Engage an independent cyber security or forensic expert as appropriate.
    - Assess whether serious harm is likely (with reference to section 4.2 above and section 26WG of the NDB Act)
    - Make a recommendation to the Risk and Compliance Officer whether this breach constitutes an NDB for the purpose of mandatory reporting to the OAIC and the practicality of notifying affected individuals.
    - Consider developing a communication or media strategy including the timing, content and method of any announcements to students, staff or the media.

The Response Team must undertake its assessment within 48 hours of being convened.

The Risk and Compliance Officer will provide periodic updates to the Chief Executive Officer as deemed appropriate.

3.9.Notification

Having regard to the Response team's recommendation in 3.4 above, the Risk and Compliance Officer will determine whether there are reasonable grounds to suspect that an NDB has occurred.

If there are reasonable grounds, the Risk and Compliance Officer must prepare a prescribed statement and provide a copy to the OAIC as soon as practicable (and no later than 30 days after becoming aware of the breach or suspected breach).

If practicable, Assetora must also notify each individual to whom the relevant personal information relates. Where impracticable, Assetora must take reasonable steps to publicise the statement (including publishing on the website). Where serious harm cannot be mitigated through remedial action, we must notify individuals at risk of serious harm and provide a statement to the Commissioner, as soon as practicable, within 30 days of identification.

The prescribed statement will be logged by the Risk and Compliance Officer.

3.10.Secondary Role of the Response Team

Once the matters referred to in 4.4 and 4.5 have been dealt with, the Response team should turn attention to the following:

- Identify lessons learnt and remedial action that can be taken to reduce the likelihood of recurrence – this may involve a review of policies, processes, refresher training.
- Prepare a report for submission to the Chief Executive Officer.
- Consider the option of an audit to ensure necessary outcomes are effected and effective.

4. Updates to this Procedure

In line with Assetora Policy, this procedure is scheduled for review every five years or more frequently if appropriate.

4.1 Revisions made to this Procedure

Date	Major or Minor Revision	Description of Revision(s)
18/10/2022	Minor	Review and update

5. Contact details

Contact for all matters related to privacy, including complaints about breaches of privacy, should be directed as follows:

Privacy Officer

E: privacy@Assetora.com.au

6. Staff Training

All staff will receive initial training on how to identify possible data breaches, escalation procedures, reporting lines, members of the data breach response team and improving areas of potential weakness.

Annexure A

Privacy Policy Data Breach Report Template

Where a privacy data breach is known to have occurred (or is suspected) any member of Assetora staff who becomes aware of this must, **within 24 hours, alert the Chief Executive Officer or the Privacy Officer.**

The Information that should be provided (if known) at this point includes:

a. Person making report and to Whom

b. When the breach occurred (time and date)

c. Description of the breach (type of personal information involved)

d. Cause of the breach (if known) otherwise how it was discovered

e. Which system(s) if any are affected?

f. Which part of Assetora is involved?

g. Whether corrective action has occurred to remedy or ameliorate the breach (or suspected breach)

Annexure B

Notifiable Data Breach Statement

This statement must be submitted to the Office of the Australian Information Commissioner as soon as practicable after becoming aware of the notifiable data breach (and no later than 30 days), in accordance with section 3.5 of the Data Breach Procedure & Response Plan.

Part 1	**Refers to requirements set out in section 26WK of the** *Privacy Amendment (Notifiable Data Breaches) Act 2017*
Organisation Name	
Contact Name	
Contact Phone Number	
Address	
Description of the Notifiable Data Breach that Assetora has reasonable grounds to believe has happened	
Kind(s) of personal information involved in the data breach	☐ Financial details ☐ Government identifiers ☐ Contact information ☐ Health information ☐ Other sensitive information ☐ Other
Steps Assetora recommends that individuals take to reduce the risk that they experience serious harm as a result of this data breach	
Other entities affected	☐ Yes ☐ No Contact details:

Part 2	The information that Assetora provides on part two of the form does not need to be included in the notification(s) to affected individuals, and Assetora may request that it be held in confidence by the OAIC.
Date the breach occurred	
Date the breach was discovered	
Primary cause of the data breach	☐ Malicious or criminal attack ☐ System fault ☐ Human error
Description of how the data breach occurred	
Number of individuals whose personal information is involved in the data breach	
Description of any action Assetora has taken to assist individuals whose personal information was involved in the data breach	
Description of any action Assetora has taken to prevent reoccurrence	
How does Assetora intend to notify individuals who are likely to be at risk of serious harm as a result of the data breach?	
When will this occur?	
List any other data protection authorities, law enforcement bodies or regulatory bodies that you have reported this data breach to:	