Vinarc Pty Ltd Data Breach Response Plan

Release Date | February 2018

Overview

This Data Breach Response Plan is designed to provide guidance on how to identify, contain, assess and respond to data breaches.

It applies to Vinarc Pty Ltd and all subsidiary companies (the Licensee), including employees, directors, officers and financial advisers.

Throughout this document ‘the Licensee’ may be referred to as ‘we’, ‘us’ and ‘our’.

Roles and Responsibilities

Role	Responsibility
Directors, Officers, Financial Advisers	Identification and notification of potential data breaches to the Data Breach Response Team
Data Breach Response Team	Investigation, assessment, remediation and communication plans for data breaches. Members of the Data Breach Response Team include: - Gavin Glozier - Director - Marc Bineham – Responsible Manager

What is a data breach?

A data breach is where personal information held by an entity is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference.

Examples of a data breach include:

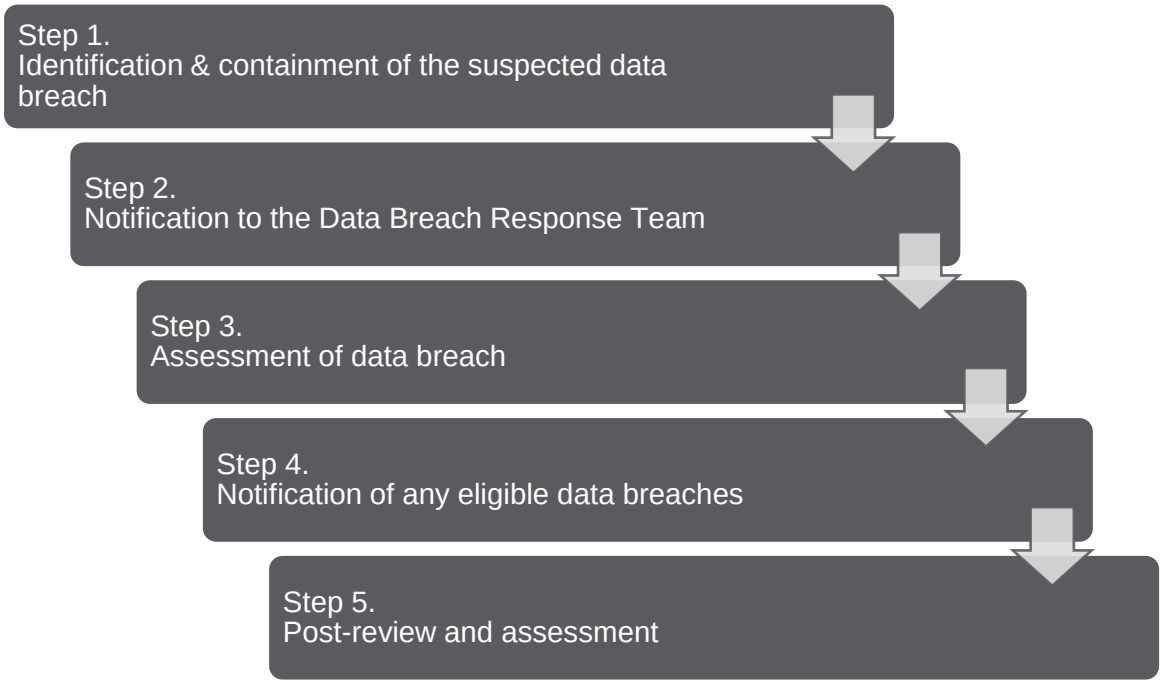
- Lost or stolen portable devices or physical files which may contain personal information
- Digital storage media being disposed of or returned to lessors without the contents first being erased
- Unsecure disposal of paper records (e.g. failure to utilise shredding services)
- Unauthorised access to personal information (e.g. hacking)
- Software security issues that allow visibility or access to personal information to unauthorised personnel
- Disclosure of personal information to the wrong person (e.g. emailing a spreadsheet containing client information to the wrong email recipient)

A data breach can be relatively minor or serious in nature. A serious data breach may be classified as an ‘eligible data breach’ which requires notification to the Office of the Australian Information Commissioner (OAIC) and the affected individuals.

An eligible data breach is classified where the data breach is likely (more probable than not) to result in a real risk of serious harm to the individuals affected, and where remediation action has not been able to prevent the likely risk of serious harm.

Serious harm to an individual may include serious physical, psychological, emotional, financial or reputational harm.

Data Breach Response Plan Summary



Step 1. Identification and containment of the suspected data breach

Where an employee or representative of the Licensee discovers or suspects that a data breach has occurred they should take immediate action to contain the breach and mitigate any future data breaches.

The actions required will differ depending upon the nature of the data breach, however it could include steps such as:

- changing passwords or removing security access for certain individuals
- attempt to ‘recall’ emails associated with the breach
- make contact with the individual who has received the incorrect information and request they destroy the information immediately
- contacting any institutions or individuals that may have received requests from hackers and request that they do not proceed with transactions
- notifying relevant technology services if applicable

Employees and representatives are encouraged to consult with a member of the Data Breach Response Team to determine appropriate containment action.

Step 2. Notification to the Data Breach Response Team

All data breaches, no matter how minor, should be reported and discussed with a member of the Data Breach Response Team.

Any data breach which has the potential to be an eligible data breach should be notified to the Data Breach Response Team by utilising the Data Breach Notification Form (Appendix A).

The Data Breach Response Team may request additional information, containment and/or mitigation actions. Representatives and employees should await further instructions from the Data Breach Response Team.

Step 3. Assessment of the data breach

The Data Breach Response Team is responsible for the investigation, review and completion of the assessment section of the Data Breach Notification Form.

All reasonable steps must be taken to complete the assessment within 30 days of the Licensee being made aware of the potential data breach. Where assessment is unable to be completed within 30 days, the Data Breach Response Team will document the reasons for the delay.

The Data Breach Response Team will consider a range of criteria in completing the assessment; including but not limited to:

- Are there multiple individuals affected?
- Is there a greater chance of serious harm due to malicious or criminal attack?
- Does the data breach involve sensitive information?
- Is the affected individual's identity identifiable or ascertainable?
- How could the personal information potentially be used?
- Is the data breach systemic or isolated?
- Is the risk of serious harm more probable than not?
- Has the remediation action prevented the likely risk of serious harm?

The Data Breach Response Team may recommend additional remediation or mitigation actions as a result of the data breach. This could include:

- notifying any law enforcement agencies or regulators
- staff and representative training
- additional security measures
- updating any relevant policies and procedures

The Data Breach Response Team are responsible for ensuring the recommendations are actioned.

Step 4. Notification of any eligible data breaches

Where the Data Breach Response Team assess the data breach as an eligible data breach, the following notification process is required.

The Data Breach Response Team are responsible for the notification process.

a) Notifying the OAIC

The Data Breach Response Team will complete the online Notifiable Data Breach Form.

b) Identify and notify the affected individuals

The notification of the affected individuals must occur prior to, or as soon as practicable after, notifying the OAIC.

This could include notifying all individuals whose personal information was part of the eligible data breach, or only notifying a subset of individuals who are likely to experience serious harm as a result of the eligible data breach (e.g. only notifying clients who had personal information containing identification documentation compromised versus those that only had contact information compromised).

c) Public notification

Where the Data Breach Response Team are unable to notify the individuals affected (e.g. contact details may be incorrect), a statement is to be published on the Licensee's website and where applicable any related websites (e.g. financial adviser websites). The statement must remain on the website for a minimum of 6 months.

All reasonable steps must also be made to publicise the contents of the statement. This may include a media release to a relevant media publication or publishing the announcement on social media. The Data Breach Response Team are responsible for the publication and any communication plan to handle resulting media or public enquiries.

d) Contents of the individual or public notification

The notification must include:

- The identity and contact details of the relevant entity (e.g. The Licensee or the relevant subsidiary company)
- A description of the eligible data breach
- The kinds of information relevant to the eligible data breach
- Recommendations about steps the individual should take in response to the eligible data breach

It may also include:

- Other information sources (e.g. link to the OAIC)
- Whether the data breach was notified to the regulator or other law enforcement agencies
- Other organisations involved with the data breach
- Details of how the data breach has been contained
- Available assistance that is being offered to the individuals
- How an individual can make a complaint

The Data Breach Response Team are responsible for the content, format and delivery of the individual and public notification. Legal advice may be required in some circumstances.

Step 5. Post-breach review and assessment

The Data Breach Response Team will conduct a post-breach review and assessment to ensure the following:

- All notifications were delivered in accordance with the notification plan
- All recommended remediation or mitigation actions were completed
- Assess if any additional training is required for employees, directors, officers or representatives
- Assess if there are any improvements to be made to the Data Breach Response Plan

Other relevant information

This Data Breach Response Plan will be reviewed annually or as required by law or upon changes to our business operations.

All records associated with the identification and assessment of the data breach are to be maintained for seven years. All data breaches notified to the Data Breach Response Team are to be recorded in the Breach and Incident Register.

Any queries in relation to the Data Breach Response Plan should be directed to the Data Breach Response Team.

The Data Breach Response Team
Vinarc Pty Ltd
Level 10, 53 Walker St North Sydney, NSW
P| 02 9922 3866
E| admin@vinarc.com.au

Data Breach Response Team Contact Details:

Gavin Glozier – gaving@noallco.com.au

Marc Bineham – marcb@noallco.com.au

Appendix A

Data Breach Notification Form	
Company name	
Notifier name and contact details	
Notification date	
Data breach description (include information on how it occurred)	
Primary cause of data breach	☐ Malicious or criminal attack ☐ System fault ☐ Human error
Information involved in the data breach	
Select relevant categories involved with the data breach	☐ Financial details ☐ Tax File Number (TFN) ☐ Identification information (e.g. Centrelink reference number, passport, drivers licence number, Medicare number) ☐ Contact information (e.g. home address, phone number, email address) ☐ Health information ☐ Other sensitive information (e.g. sexual orientation, political or religious views)
Date breach occurred and duration	
Date breach discovered	
Number of individuals affected	
Potential harm to the affected individuals	
How was the data breach contained? (containment and remedial action)	
Detail any steps taken to mitigate future data breaches	

Assessment	
Assessment date	
Nature of potential harm	☐ 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 bully or marginalisation
Has remediation actioned prevented the likely risk of serious harm?	☐ Yes ☐ No
Other entities affected	☐ Yes ☐ No Name and contact details of other entity:
Final assessment (is the risk of serious harm more probable than not)	☐ Yes – Eligible data breach requiring notification ☐ No – Not an eligible data breach requiring notification Include details:
Any additional remediation or mitigation actions required	☐ Yes ☐ No Include details:
Do any law enforcement agencies or regulators need to be notified?	☐ Yes ☐ No Include details:
Notification plan	☐ Notify all affected individuals ☐ Notify a subset of affected individuals. Include details ☐ Public notification as unable to notify individuals
OAIC notification date:	
Individual notification date:	
Public notification date:	