PRIVACY POLICY

Ausvogar Investment Management Pty Ltd

ACN 617 714 324

1. We respect your privacy

1.1. Ausvogar Investment Management Pty Ltd respects your right to privacy and is committed to safeguarding the privacy of our customers and website visitors. We adhere to the Australian Privacy Principles contained in the *Privacy Act* 1988 (Cth). This policy sets out how we collect and treat your personal information.

1.2. "Personal information" is information we hold which is identifiable as being about you.

2. Collection of personal information

2.1. Ausvogar Investment Management Pty Ltd will, from time to time, receive and store personal information you enter onto our website, provided to us directly or given to us in other forms.

2.2. You may provide basic information such as your name, phone number, address and email address to enable us to send information, provide updates and process your product or service order. We may collect additional information at other times, including but not limited to, when you provide feedback, when you provide information about your personal or business affairs, change your content or email preference, respond to surveys and/or promotions, provide financial or credit card information, or communicate with our customer support.

2.3. Additionally, we may also collect any other information you provide while interacting with us.

3. How we collect your personal information

3.1. Ausvogar Investment Management Pty Ltd collects personal information from you in a variety of ways, including when you interact with us electronically or in person, when you access our website and when we provide our services to you. We may receive personal information from third parties. If we do, we will protect it as set out in this Privacy Policy.

4. Use of your personal information

4.1. Ausvogar Investment Management Pty Ltd may use personal information collected from you to provide you with information, updates and our services. We may also make you aware of new and additional products, services and opportunities available to you. We may use your personal information to improve our products and services and better understand your needs.

4.2. Ausvogar Investment Management Pty Ltd may contact you by a variety of measures including, but not limited to telephone, email, sms or mail.

5. Disclosure of your personal information

5.1. To enable us to maintain a successful business relationship with you, we amy disclose your personal information to:

5.1.1. Organizations that provide products or services used by us, your employer/s or referees, your guarantors, your professional advisors, your bank and any other organization that may have or is consideration having an interest in your loan, or in our business;

5.1.2. Companies and contractors who we retain to provide service for us, such as IT contractors, lawyers, accountants and auditors, who will need to have access to your personal information to provide those services

5.1.3. Other individuals or companies authorized by you.

5.2. We may from time to time need to disclose personal information to comply with a legal requirement, such as a law, regulation, court order, subpoena, warrant, in the course of a legal proceeding or in response to a law enforcement agency request.

5.3. We may also use your personal information to protect the copyright, trademarks, legal rights, property or safety of Ausvogar Investment Management Pty Ltd, www.ausvogar.com.au, its customers or third parties.

5.4. Information that we collect may from time to time be stored, processed in or transferred between parties located in countries outside of Australia.

5.5. If there is a change of control in our business or a sale or transfer of business assets, we reserve the right to transfer to the extent permissible at law our user databases, together with any personal information and non-personal information contained in those databases. This information may be disclosed to a potential purchaser under an agreement to maintain confidentiality. We would seek to only disclose information in good faith and where required by any of the above circumstances.

5.6. By providing us with personal information, you consent to the terms of this Privacy Policy and the types of disclosure covered by this Policy without obtaining your consent on a case by case basis. Where we disclose your personal information to related parties or third parties, we will request that the third party follow this Policy regarding handling your personal information.

6. Security of your personal information

6.1. Ausvogar Investment Management Pty Ltd is committed to ensuring that the information you provide to us is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure information and protect it from misuse, interference, loss and unauthorised access, modification and disclosure.

6.2. The transmission and exchange of information is carried out at your own risk. We cannot guarantee the security of any information that you transmit to us, or receive from us. Although we take measures to safeguard against unauthorised disclosures of information, we cannot assure you that personal information that we collect will not be disclosed in a manner that is inconsistent with this Privacy Policy.

7. Access to your personal information

7.1. You may request details of personal information that we hold about you in accordance with the provisions of the *Privacy Act* 1988 (Cth). A small administrative fee may be payable for the provision of information. If you would

like a copy of the information, which we hold about you or believe that any information we hold on you is inaccurate, out of date, incomplete, irrelevant or misleading, please email us at info@ausvogar.com.

7.2. We reserve the right to refuse to provide you with information that we hold about you, in certain circumstances set out in the Privacy Act.

8. Complaints about privacy

8.1. If you have any complaints about our privacy practices, please feel free to send in details of your complaints to Suite 3604, Level 36 201 Elizabeth Street, Sydney, New South Wales, 2000. We take complaints very seriously and will respond shortly after receiving written notice of your complaint.

9. Changes to Privacy Policy

9.1. Please be aware that we may change this Privacy Policy in the future. We may modify this Policy at any time, in our sole discretion and all modifications will be effective immediately upon our posting of the modifications on our website or notice board. Please check back from time to time to review our Privacy Policy.

10. Website

10.1. *When you visit our website*

When you come to our website (www.ausvogar.com.au) we may collect certain information such as browser type, operating system, website visited immediately before coming to our site, etc. This information is used in an aggregated manner to analyse how people use our site, such that we can improve our service.

10.2. *Cookies*

We may from time to time use cookies on our website. Cookies are very small files which a website uses to identify you when you come back to the site and to store details about your use of the site. Cookies are not malicious programs that access or damage your computer. Most web browsers automatically accept cookies but you can choose to reject cookies by changing your browser settings. However, this may prevent you from taking full advantage of our website. Our website may from time to time use cookies to analyses website traffic and help us provide a better website visitor experience. In addition, cookies may be used to serve relevant ads to website visitors through third party services such as Google Adwords. These ads may appear on this website or other websites you visit.

10.3. *Third party sites*

Our site may from time to time have links to other websites not owned or controlled by us. These links are meant for your convenience only. Links to third party websites do not constitute sponsorship or endorsement or approval of these websites. Please be aware that Ausvogar Investment Management Pty Ltd is not responsible for the privacy practises of other such websites. We encourage our users to be aware, when they leave our website, to read the privacy statements of each and every website that collects personal identifiable information.

11. Code of Conduct

11.1. Protecting our client's privacy and ensuring the highest level of information security is integral to our continued business growth and success and our principles of integrity and honesty.

11.2. Our client's confidentially and interests remain paramount and as such, any client information entrusted to us will not be unlawfully disclosed to any none related party, unless where disclosure is required under the law.

11.3. All client material and information entrusted to our company, will be handled wit the highest degree of care and stored securely.

11.4. Our Privacy Policy outlines our commitment to ensure how the National Privacy Principles are practiced in our organization.

12. Application Form Information

12.1. Our reference checking process is consistent with our obligations under the *Privacy Act 1988* (Cth) (Privacy Act) for the handling of personal information. (Further information regarding the Privacy act can be found at www.oaic.gov.au).

We will need to collect private information about you from third parties, including referees as well as current/previous Organizations for this purpose.

We may engage an agent to conduct background checks to verify some or all of the information you have provided. Any agent we engage to act on our behalf will be required to handle personal information in a manner which is consistent with our obligations under the Privacy Act.

To facilitate the reference checking process, we need to obtain your informed and your direction for us to collect, use, disclose and store personal information about you from third parties for the purpose of verifying your experience and qualifications and to assist us in assessing your application.

We will send a signed copy of your Consent Form and Direction Form to your current/previous Organizations as part of our reference checking process. We may disclose relevant factual information that we have collected to prospective Organizations who ask us for this information together with other information including dates of appointment, position(s) held, and compliance reviews. You may gain access to the information collected about you and/or correct this information (if necessary) while it is being stored. We will securely store this information and will destroy the information when it is no longer required for the purposes set out above.

13. Privacy Breach Policy and Data Breach Response Plan

13.1. Our objective is to ensures that Ausvogar Investment Management Pty Ltd comply with all relevant aspects of the Australian Privacy Principles (APPs), as set out in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, and with the Notifiable Data Breach Scheme (NDB Scheme). The detailed Privacy Breach Policy and Data Breach Response Plan is attached in the **Appendix 1**.

14. Email and Internet Use Procedures

14.1. *Sending Emails*

Email sent to multiple external recipients (e.g. Newsletters) must be addressed

using the Bcc (Blind Copy) address block unless the privacy of recipients is not a consideration (e.g. members of a working group).

Staff should always ensure emails messages protect other's rights to privacy and confidentiality.

Appendix 1

Privacy Breach Policy and Data Breach Response Plan

Obligation

As a corporate authorised representative, Ausvogar Investment Management Pty Ltd aims to comply all relevant aspects of the Australian Privacy Principles (APPs), as set out in the Privacy Amendment (Enhancing Privacy Protection) Act 2012, and with the Notifiable Data Breach Scheme (NDM Scheme).

All Australian Financial Services Licensees that hold personal information are subject to the APPs and are required to take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure under APP11 – Security of Personal Information. Licensees who trade in personal information have additional obligations under the remaining APPs. All Licensees holding personal information are expected to implement a Privacy Policy in compliance with the APPs.

The NDB scheme applies to entities that have an obligation under APP 11 of the Privacy Act to protect the personal information they hold. Known as 'APP entities', these include businesses with an annual turnover of more than $3 million.

Small business operators are not considered APP entities. However, some businesses of any size are APP entities, including businesses that trade in personal information. A small business operator (SBO) is an individual (including a sole trader), body corporate, partnership, unincorporated association, or trust that has not had an annual turnover of more than $3 million in any financial year since 2001 (s 6D).

Small business operators who do not trade in personal information are caught under NDB if they hold tax file numbers (under TFN rule 15) and/or if they hold personal information for the purpose of AML reporting. Business collecting TFNs and/or holding AML reporting information, are required only to identify and respond to data breaches of TFN and/or AML information.

Note:

Ausvogar Investment Management Pty Ltd is:

- A small business operator who does not trade in personal information, who:
    - Holds Tax File Numbers under TFN rule 15 -and/or-
    - Holds personal information for the purpose of AML reporting

Adherence to the Ausvogar Investment Management Pty Ltd Policy Breach and Data Response Plan is expected and will be monitored to ensure that personal information is secured adequately and breaches, both suspected and actual, are treated appropriately per the guidelines set by the Office of the Australian Information Commissioner.

Expectation

The Office of the Australia Information Commissioner's focus of the Privacy Act and NDB Scheme obligations is to increase protection levels across the board and keep individual's personal information more secure. It's the responsibility of APP entities to secure and protect the personal information they hold and prevent breaches from occurring. The NDB Scheme provides a framework that requires businesses to respond swiftly and with transparency to mitigate the damage potentially caused by a breach. This ultimately gives consumers more confidence that their personal information is being appropriately safeguarded and that they will be made aware in the event that their information is compromised.

Ausvogar Investment Management Pty Ltd as an organisation has undertaken to ensure that its privacy program embraces the principles established by the APPs under the Privacy Act and abides by the requirements of the NDB Scheme.

Privacy Act 1988 (Privacy Act)

Australian Privacy Principles

APP 1 — Open and transparent management of personal information
APP 2 — Anonymity and pseudonymity
APP 3 — Collection of solicited personal information
APP 4 — Dealing with unsolicited personal information
APP 5 — Notification of the collection of personal information
APP 6 — Use or disclosure of personal information
APP 7 — Direct marketing
APP 8 — Cross-border disclosure of personal information
APP 9 — Adoption, use or disclosure of government related identifiers
APP 10 — Quality of personal information
APP 11 — Security of personal information
APP 12 — Access to personal information
APP 13 — Correction of personal information

The Notifiable Data Breaches (NDB)- scheme (under Part IIIC of the Act)

Commitment

Ausvogar Investment Management Pty Ltd as an organisation is committed to the development and implementation of its privacy program including maintaining an up-to-date APP Privacy Policy about how it manages personal information, identifying breaches or suspected breaches of the Policy and developing and relying on a breach Response Plan to ensure they are able to respond quickly to suspected data breaches, and take appropriate steps as required under the NDB Scheme.

The Licensee is committed to all stages of the NDB Scheme and the reporting of data breaches from identification of a breach/potential breach including containment, evaluation, notification and review of the breach including taking action to prevent future breaches.

As a corporate authorised representative Ausvogar Investment Management Pty Ltd ensures that there are adequate resources in place to develop, implement and maintain the privacy program and response plan.

Implementation

Ausvogar Investment Management Pty Ltd demonstrates commitment to the privacy program by implementing best practices and adherence to privacy standards and compliance with the NDB Scheme:

- Ausvogar Investment Management Pty Ltd Privacy Policy
- Data Breach Response Plan

Ausvogar Investment Management Pty Ltd takes reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure. Should a breach be suspected or occur, Ausvogar Investment Management Pty Ltd follows a documented plan covering strategy, assessment, treatment, and review of data breaches.

Management Responsibility

The Response Team will have the overall responsibility for overseeing the Privacy Policy and Data Breach Response Plan. Both the internal and external resources will be engaged as required to assist in the management of this function. The responsibilities of this role include but are not limited to:

- Ensuring all staff and representatives and staff are fully trained and aware of their privacy responsibilities;
- Dealing with privacy breaches, including under the NDB Scheme;
- Identifying issues which may lead to privacy breaches;
- Maintaining a detailed level of knowledge in relation to privacy issues i.e. regulatory and industry changes.

Identification of Breaches

Ausvogar Investment Management Pty Ltd has an Induction Program which actions will be in accordance with its policy, including the identification of privacy breaches.

As a small business and holder of tax file numbers (under TFN rule 15) and/or personal information for the purpose of AML reporting, Ausvogar Investment Management Pty Ltd is required only to identify and respond to data breaches of TFN and/or AML information.

Notification

When Ausvogar Investment Management Pty Ltd is aware of reasonable grounds to believe an eligible data breach has occurred, they are obligated to promptly notify affected individuals of the likely risk of serious harm. The Commissioner must also be notified as soon as practicable through a statement about the eligible data breach.

Record Keeping

The following records are to be maintained with regard to privacy issues:

- Minutes of compliance meetings where privacy breaches are discussed

- Copies of evidence of a privacy breach
- Documents supporting steps of the Response Plan as followed:
    - Preliminary breach assessment
    - Notification to individuals
    - Notification to OAIC
    - Breach risk assessment
    - Review of breach incident outcomes and recommendations to prevent future breaches

Review and prevention

In the case of a breach, Ausvogar Investment Management Pty Ltd, led by the Response Team, will review the incident and take action to prevent future breaches.

What Constitutes a Data Breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information an entity holds. A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. Data breaches can be caused by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harms to individuals, agencies and organisations.

What is a 'data breach'?

- ***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).
- ***Unauthorised disclosure*** occurs when an entity, whether intentionally or unintentionally, makes personal information accessible or visible to others outside the entity, and releases that information from its effective control in a way that is not permitted by the Privacy Act. This includes an unauthorised disclosure by an employee of the entity.
- ***Loss*** refers to the accidental or inadvertent loss of personal information held by an entity, in circumstances where is it is likely to result in unauthorised access or disclosure.

What is an eligible data breach?

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

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds;
- this is likely to result in serious harm to one or more individuals; and
- the entity has not been able to prevent the likely risk of serious harm with remedial action.

Notifiable Data Breaches Scheme

The Notifiable Data Breaches (NDB) scheme establishes requirements for entities in responding to data breaches. Entities have data breach notification obligations when a data breach is likely to result in serious harm to any individuals whose personal information is involved in the breach.

Identifying 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 (APP11).

Small business operators who hold TFNs and/or hold AML reporting information, are required only to identify and respond to data breaches of TFN and/or AML information respectively.

Eligible Data Breach

An eligible data breach arises when a data breach is likely to result in serious harm to one or more individuals and the likely risk of serious harm has not been prevented through remedial action.

Serious Harm

The risk of serious harm is to be assessed, from the perspective of a reasonable person, with 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. 'Serious harm' is not defined in the Privacy Act. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm.

> *NOTE: For the 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. Also refer Chapter B of the OAIC's APP Guidelines.*
>
> *The phrase 'likely to occur' means the risk of serious harm to an individual is more probable than not (rather than possible).*

Refer Appendix 2: Assessing the Risk of Serious Harm

Preventing serious harm with remedial action

If remedial action is taken so that the data breach would not be likely to result in serious harm, then the breach is not an eligible data breach, for example:

> **Example 1:**
> 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.
>
> **Example 2:**

An employee leaves a smartphone on public transport while on their way to work. When the employee arrives at work they realise that the smartphone has been lost and ask their employer's IT support staff to remotely delete the information on the smartphone. Because of the security measures on the smartphone, the IT support staff are confident that its content could not have been accessed in the short period between when it was lost and when its contents were deleted and no data breach occurred.

Data Breach Response Plan

A data breach response plan sets out the roles, responsibilities and steps for managing data breaches including actions to be taken by the response team.

There are four key steps involved in a Data Breach Response Plan:

1. Contain the breach and do a preliminary assessment;
2. Evaluate the risks associated with the breach;
3. Notification of affected individuals and the OAIC; and
4. Prevent future breaches.

Data Breach Response Team

The purpose of having a response team is to ensure that the relevant staff, roles and responsibilities are identified and documented before the data breach happens. Time can be lost if you do not consider how to create a response team until the breach has already occurred.

The make-up of your response team will depend on your business and the nature of the breach. Different skill sets, and staff may be needed to respond to one breach compared to another. Depending on the size of your entity and the nature of the breach, you may need to include external experts in your team, for example for legal advice, data forensics and media management. You should identify the type of expertise you may need and ensure that that expertise will be available on short notice.

You should keep a current list of team members which clearly articulates their roles, responsibilities and authorities as well as their contact details as appropriate. You should ensure contact lists remain updated, particularly in the event of organisational changes. Each role on the team should have a second contact point in case the first is not available. You may wish to consider creating a core team and adding other members as required.

Typical team roles and skills might include:

- a team leader — to lead the team and manage reporting to senior management
- a project manager — to coordinate the team and provide support to its members
- a senior member of staff with overall accountability for privacy and/or key privacy officer — to bring privacy expertise to the team
- legal support — to identify legal obligations and provide advice
- risk management support — to assess the risks from the breach
- information and records management expertise – to assist in reviewing security and monitoring controls related to the breach (for example, access, authentication,

encryption, audit logs) and to provide advice on recording the response to the data breach

- HR support — if the breach was due to the actions of a staff member
- media/communications expertise — to assist in communicating with affected individuals and dealing with the media and external stakeholders.

Data Breach Response Plan

This data breach response plan sets out procedures and reporting lines for Ausvogar Investment Management Pty Ltd and its management, representatives and staff in the event Ausvogar Investment Management Pty Ltd suspects or experiences a data breach.

Suspected or known data breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information an entity holds. A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse.

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

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds;
- this is likely to result in serious harm to one or more individuals; and
- the entity has not been able to prevent the likely risk of serious harm with remedial action.

If remedial action is taken so that the data breach would not be likely to result in serious harm, then the breach is not an eligible data breach.

This plan is subject to annual review by the Response Team.

Representative and staff responsibilities: record and report to management

Immediately notify management of the suspected data breach. Record and report:

- time and date suspected breach was discovered
- type of information involved
- cause and extent of the breach, if known
- context of the affected information, if known

Management responsibilities: assess, escalate to Response Team where appropriate

Assess and determine whether a data breach has occurred.

If management has any suspicion that a breach has occurred, the matter will be escalated the breach to the Response Team to undertake the breach response process.

Ausvogar Investment Management Pty Ltd Data Response Team

Name (include contact details as appropriate)	Role	Responsibility

Compliance Officers Yuwei Joyce Yang T: +61 2 8599 8599	Team Leader	Lead the team and manage reporting to senior management
Compliance Officers Yuwei Joyce Yang T: +61 2 8599 8599	Project Manager	Coordinate the team and provide support to its members
Compliance Officers Yuwei Joyce Yang T: +61 2 8599 8599	Privacy Officer	Provide privacy expertise to the team
Compliance Officers & External Experts as required Yuwei Joyce Yang T: +61 2 8599 8599	Legal	Identify legal obligations and provide advice
Compliance Officers Yuwei Joyce Yang T: +61 2 8599 8599	Risk Management	Assess the risks from the breach
Compliance Officers Yuwei Joyce Yang T: +61 2 8599 8599	IT	Assist in reviewing security and monitoring controls and to provide advice on recording the response to the data breach
Compliance Officers Yuwei Joyce Yang T: +61 2 8599 8599	HR	Assist if the breach was due to the actions of a staff member
Compliance Officers Yuwei Joyce Yang T: +61 2 8599 8599	Media Representative	Assist in communicating with affected individuals and dealing with the media and any external stakeholders

Compliance Officers & External Experts as required Yuwei Joyce Yang T: +61 2 8599 8599	Industry Expert/s	To provide guidance where outside forensic, privacy, or other input is required

Breach Response Process:

1. Contain the breach and do a preliminary assessment

All Ausvogar Investment Management Pty Ltd personnel understand how to identify a breach or suspected breach and how to escalate to management and/or the Response Team.

When a breach has been identified action must be taken immediately to contain it. Where possible, steps are to be taken to stop the unauthorised practice, recover the information, shut down the system that was breached, change computer access codes or correct weaknesses in physical or electronic security. Depending on the type of breach this may include:

- Resetting passwords
- Disabling network access
- Recalling or deleting information
- Installing patches to resolve viruses or technology flaws
- Securing hardcopy files and electronic devices

After prompt collection of information, the Response Team will handle the breach according to the Data Breach Response Plan, starting with the initial breach investigation, assessing:

1. Personal information the breach involves;
    a. Does the breach involve holding of TFN/s?
    b. Does the breach involve holding of personal information for the purpose of reporting to AUSTRAC?
2. Cause of the breach;
3. Extent of the breach;
4. Harms breach could potentially cause to affected persons; and
5. How the breach can be contained.

As a small business covered by the NDB Scheme for holding TFNs and/or holding AML reporting information, Ausvogar Investment Management Pty Ltd is only required to identify and respond to data breaches of TFN and/or AML information. Where this information is involved in the breach next steps are to be taken per the Response Plan. Where the breach involves personal information other than relating to the holding of TFNs or the holding of AML reporting information, the preliminary assessment can be completed with no further action required.

Records will be kept relating to the initial investigation and ongoing breach response process with ongoing updates on key develops provided to management as necessary. Depending on the breach not all steps may be necessary, however all steps taken are to be documented.

2. Evaluate the risks associated with the breach

Ausvogar Investment Management Pty Ltd will take the steps to initiate the assessment, investigate by gathering relevant information and evaluate via an evidence-based decision about whether serious harm is likely.

Ausvogar Investment Management Pty Ltd will also consider the need to respond to media inquiries and/or adopting a media strategy by an agreed upon spokesperson.

- Type of information
    - Personal and/or sensitive information?
    - Does the type of information mean a greater risk of harm?
    - What individuals are affected?
- Context of information
    - For what purpose is the affected personal information held?
    - Who has gained unauthorised access to the information?
    - How could the information be used?
- Cause and extent of breach
    - How many individuals are affected by the breach?
    - Is there a risk of further exposure or ongoing breaches?
    - Is there evidence of theft?
    - Is the information encrypted or otherwise protected from unauthorised access?
    - How did the breach occur? (may be lower risk if accidental)
    - Has the information been recovered?
    - What remedial action has been taken to mitigate harm?
    - Is this an isolated incident or a systemic problem?
- Risk of harm to the affected individuals – *refer Appendix 2: Assessing the Risk of Serious Harm*
    - Who is the recipient of the information?
    - What harm to individuals could result from the breach?
- Risk of other harms
    - Loss of trust
    - Damage to reputation
    - Legal liability

Where possible, Ausvogar Investment Management Pty Ltd will take steps to reduce any potential harm to individuals. This may include recovering lost information prior to unauthorised access or changing passwords before unauthorised access can occur. If the remedial action taken is successful in making serious harm no longer likely, then notification is not required, and the response can progress to the final review stage.

Keep records of suspected breach, actions by management and the Response Team. Include steps taken to rectify the situation and decision made. A thorough evaluation of the risks will Ausvogar Investment Management Pty Ltd to determine the course of action to take.

3. Notification

Where serious harm is likely, an entity must prepare a statement for the Commissioner and notify affected individuals notifying them of the contents of this statement.

Statement Notifying Commissioner

When Ausvogar Investment Management Pty Ltd becomes aware of an eligible data breach as soon as practically possible they will:

- Prepare a statement
- Provide a copy to the Commissioner

Statement to address:

- The identity and contact details of the entity
- A description of the eligible data breach that the entity has reasonable grounds to believe has happened
- The kind or kinds of information concerned; and
- Recommendations about the steps that individuals should take in response.

Note: not all breaches are notifiable. The obligation to notify the Commissioner or individuals is avoided where remedial action has been taken before unauthorised access, disclosure or loss result in harm.

The OAIC intends to release an online Data Breach Notification Form which may be used to notify the Commissioner pending availability (refer ww.oaic.gov.au).

Notification to Individuals

As soon as practical after the statement is prepared, using the usual means of communicating with individuals, the entity must notify and provide the prepared statement to:

- Each of the individuals to whom the information relates; or
- Each of the individuals who are at risk

-OR-

If, this is not possible:

- Publish a copy of the statement on the Licensee's website; and
- Take reasonable steps to publicise the contents of the statement.

4. Review to prevent future breaches

Review the incident and take action to prevent future breaches.

- Fully investigate the cause of the breach, including any internal weaknesses that enabled the breach to occur:

- Develop a plan to prevent similar breaches in future:

- Undertake audits to verify the plan has been implemented:

- Update the data security and response plans and update related policies and procedures as appropriate:
- Provide enhanced staff training.

References

Privacy Act 1988 (Privacy Act)

Australian Privacy Principles (APP1 – APP13)

The Notifiable Data Breaches (NDB)- scheme (under Part IIIC of the Act)

Office of the Australian Information Commissioner website: www.oaic.gov.au

OAIC Resources

Entities Covered by The NDB Scheme

Guide to securing personal information

Identifying eligible data breaches

Assessing a suspected data breach

Notifying individuals about an eligible data breach

What to include in an eligible data breach statement

Data breach response summary

Appendix 2

Assessing the Likelihood of Serious 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 s26WG of the Privacy Amendment (Notifiable Data Breaches) Act 2017 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.

Additional information about the information involved in the breach, the circumstances of the breach and the nature of the harm can also assist in the assessment, as follows:

1. The type or types of personal information involved in the data breach

Some kinds of personal information may be more likely to cause an individual serious harm if compromised, for example:

- '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.

2. Circumstances of the data breach

The specific circumstances of the data breach are relevant when assessing whether there is a risk of serious harm to an individual, for example:

- Whose personal information was involved in the breach?
- How many individuals were involved?
- Do the circumstances of the data breach affect the sensitivity of the personal information?
- How long has the information being accessible?
- Is the personal information adequately encrypted, anonymised, or otherwise not easily accessible?
- What parties have gained or may gain unauthorised access to the personal information?

3. The Nature of the Harm

It may be helpful for entities assessing the likelihood of harm to consider various scenarios that would result in serious harm and the likelihood of each, for example:

- 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.