Bellwether Financial Group Pty Ltd

Privacy Policy

Obligation

As an Australian Financial Services Licensee and a holder of personal information about our clients, it is our objective to ensure that Bellwether Financial Group Pty Ltd and its representatives 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 APPs require Bellwether Financial Group Pty Ltd to take reasonable steps to protect the 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. In addition, the NDB Scheme applies to entities that have an obligation under APP 11 of the Privacy Act to protect the personal information they hold.

Adherence to the Bellwether Financial Group Pty Ltd Privacy Breach Policy and Data Response Plan (The Policy) is expected and will be monitored to ensure that personal information is secured adequately and breaches, both suspected and actual, are treated appropriately as per the guidelines set by the Office of the Australian Information Commissioner (OAIC).

Expectation

The OAIC'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 if their information is compromised.

Bellwether Financial Group 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 NDB Scheme (under Part IIIC of the Act)

Commitment

Bellwether Financial Group Pty Ltd is committed to providing you with the highest levels of client service. Bellwether Financial Group Pty Ltd recognises that your privacy is very important to you. As such, the organisation is committed to providing a privacy program that ensure the correct management of personal information, identification of breaches or suspected breaches of the Policy and utilising the breach Response Plan to ensure we are able to respond quickly to suspected data breaches, and take appropriate steps as required under the NDB Scheme.

Bellwether Financial Group Pty Ltd 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 acting to prevent future breaches.

Refer Appendix A; comprehensive information on how this company will undertake its NDB Scheme.

Further information on privacy in Australia may be obtained by visiting the website of the Office of the Australian Information Commissioner at www.oaic.gov.au.

Bellwether Financial Group Pty Ltd believes that this Privacy Policy discloses the purpose, and how the personal information you provide to us and our representatives, is collected, used, held, disclosed and disseminated.

As a Licensee, Bellwether Financial Group Pty Ltd ensures that there are adequate resources in place to develop, implement and maintain the privacy program and response plan. All representatives of Bellwether Financial Group Pty Ltd are made aware of the privacy program and are encouraged to identify privacy issues and notify directly to Bellwether Financial Group Pty Ltd.

Bellwether Financial Group Pty Ltd is required to meet legislative and regulatory requirements. The information that we seek to collect about you will depend on the products or services that we provide. If you provide inaccurate or incomplete information, we may not be able to provide you with the services you requested.

We encourage you to check our website regularly for any updates to our Privacy Policy.

Your Personal Information

When you apply for our products or services, we may ask for identification information. This could include your name, address, contact details and date of birth. We may also collect your tax file number if we are authorised to collect it and if you choose to supply it.

How Bellwether Financial Group Pty Ltd Collects Personal Information

We collect personal information directly from you or from third parties once authorisation has been provided by you. You have a right to refuse us authorisation to collect information from a third party.

How Bellwether Financial Group Pty Ltd Uses Your Personal Information

Primarily, your personal information is used in order to provide you with products or services. We may also use the information that is related to the primary purpose and it is reasonable for you to expect the information to be disclosed.

From time to time, we may provide you with direct marketing material. This will include articles and newsletters that may be of interest to you. We may only use sensitive information about you for direct marketing once we have obtained your consent.

Bellwether Financial Group Pty Ltd maintains details of the source of your personal information used for direct marketing and you have the right to request these details. We will endeavour to meet your request within two (2) weeks. A record is maintained for those individuals not wanting direct marketing material.

When Bellwether Financial Group Pty Ltd Discloses Your Personal Information*

In line with modern business practices common to many financial institutions and to meet your specific needs we may disclose your personal information to the following organisations:

- superannuation fund trustees, insurance providers, fund managers and other product providers in order to manage or administer your product or service;
- compliance consultants;
- temporary staff to handle workloads during peak periods;
- mailing houses;
- your professional advisers, including your solicitor or accountant as authorised by you;
- information technology service providers;
- Government and regulatory authorities, as required or authorised by law
- another authorised representative of Bellwether Financial Group Pty Ltd if necessary;
- a potential purchaser/organisation involved in the proposed sale of Bellwether Financial Group Pty Ltd's business for the purpose of due diligence, corporate re-organisation and transfer or all or part of the assets of the business. Disclosure will be made in confidence and it will be a condition of that disclosure that no personal information will be used or disclosed by them;
- a new owner of the business that will require the transfer of your personal information.

Bellwether Financial Group Pty Ltd's employees and the outsourcing companies/contractors are obliged to respect the confidentiality of any personal information held by Bellwether Financial Group Pty Ltd.

The Corporations Act has provided the Australian Securities and Investments Commission (ASIC) with the authority to inspect certain personal information that is kept on Bellwether Financial Group Pty Ltd's files about you.

Bellwether Financial Group Pty Ltd takes its obligations to protect your information seriously, this includes if/when Bellwether Financial Group Pty Ltd operates throughout Australia and overseas, as part of its operations. Some uses and disclosures of your information may occur outside your State or Territory and/or outside of Australia. In some circumstances we may need to obtain your consent before disclosure of your information outside Australia occurs.

How Bellwether Financial Group Pty Ltd Stores and Secures Your Personal Information

Bellwether Financial Group Pty Ltd keeps your personal information in your client files or electronically. These files are accessible to authorised personnel only and are appropriately secured and subject to confidentiality requirements.

Personal information will be treated as confidential information and sensitive information will be treated highly confidential.

It is a legislative requirement that Bellwether Financial Group Pty Ltd keeps all personal information and records for a period of seven (7) years. Should you cease to be our client, we will maintain your personal information on or off site in a secure manner for seven (7) years. After this period, the information will be destroyed.

Ensure Your Personal Information Is Correct

Bellwether Financial Group Pty Ltd takes all reasonable precautions to ensure that the personal information collected, used and disclosed is accurate, complete and up to date. To ensure that we can maintain this level of accuracy and completeness, it is recommended you:

- inform us of any errors in your personal information; and
- update us with any changes to your personal information as soon as possible.

Unsolicited Information

Bellwether Financial Group Pty Ltd does not usually collect unsolicited personal information. Where we receive unsolicited personal information, it will be determined whether or not it would have been permissible to collect that personal information if it had been solicited. If Bellwether Financial Group Pty Ltd determines that collection would not have been permissible, to the extent permitted by law, the personal information will be destroyed or de-identified as soon as practicable.

Access to Your Personal Information

You have a right to access your personal information, subject to certain exceptions allowed by law. We ask that you provide your request for access in writing (for security reasons) and we will provide you with access to that personal information. Access to the requested personal information may include:

- providing you with copies;
- providing you with the opportunity for inspection; or
- providing you with a summary.

If charges are applicable in providing access to you, these charges will be disclosed to you prior to providing the information.

Some exceptions exist where Bellwether Financial Group Pty Ltd will not provide you with access to your personal information if:

- providing access would pose a serious threat to the life or health of a person;
- providing access would have an unreasonable impact on the privacy of others;
- the request for access is frivolous or vexatious;
- the information is related to existing or anticipated legal proceedings between Bellwether Financial Group Pty Ltd and the client and would not be discoverable in those proceedings;
- providing access would reveal Bellwether Financial Group Pty Ltd's intentions in relation to negotiations with you in such a way as to prejudice those negotiations;
- providing access would be unlawful;
- denying access is required or authorised by or under law;
- providing access would be likely to prejudice certain operations by or on behalf of an enforcement body or an enforcement body requests that access not be provided on the grounds of national security.

Should we refuse you access to your personal information, a written explanation for that refusal will be provided.

Using Government Identifiers

Although in certain circumstances Bellwether Financial Group Pty Ltd is required to collect Government identifiers such as your tax file number, Medicare number or pension card number, Bellwether Financial Group Pty Ltd does not use or disclose this information other than when required or authorised by law or unless you have voluntarily consented to disclose this information to any third party.

Dealing with Bellwether Financial Group Pty Ltd Anonymously

You can deal with us anonymously or by using a pseudonym where it is lawful and practicable to do so. For example, if you telephone requesting our postal address.

Your Sensitive Information

Without your consent Bellwether Financial Group Pty Ltd will not collect information about you that reveals your racial or ethnic origin, political opinions, religious or philosophical beliefs or afflations, membership of professional or trade association, membership of a trade union, details of health, disability, sexual orientation, or criminal record.

This is subject to some exceptions including:

- the collection is required by law; and
- when the information is necessary for the establishment, exercise or defence of a legal claim.

Bellwether Financial Group Pty Ltd's Website

Bellwether Financial Group Pty Ltd's website may provide links to third party websites. The use of your information by these third-party sites is not within Bellwether Financial Group Pty Ltd's control and Bellwether Financial Group Pty Ltd cannot accept responsibility for the conduct of these organisations. Other websites are not subject to Bellwether Financial Group Pty Ltd's privacy standards. You will need to contact or review those websites directly to ascertain their privacy policies.

You may register with Bellwether Financial Group Pty Ltd to receive newsletters and other information. By doing so, your name and email address will be collected and stored on Bellwether Financial Group Pty Ltd's database. We will take care to ensure that the personal information you provide on our website is protected. For example, Bellwether Financial Group Pty Ltd's website has electronic security systems in place, including the use of firewalls and data encryption.

If you do not wish to receive any further information from Bellwether Financial Group Pty Ltd, or you wish to update your registration details, please email your request. We will endeavour to meet your request within five (5) working days.

Our website utilises cookies to provide you with a better user experience. Cookies also allow Bellwether Financial Group Pty Ltd to identify your browser while you are using the site – the cookies do not identify you. If you do not wish to receive cookies, you can instruct your web browser to refuse these cookies.

Complaints Resolutions

Please contact Bellwether Financial Group Pty Ltd's Privacy Officer if you wish to complain about any breach or potential breach of your privacy rights. Your complaint will be responded to within seven (7) days. Bellwether Financial Group Pty Ltd's Privacy Officer will investigate the issue and determine the steps to undertake to resolve your complaint. Bellwether Financial Group Pty Ltd's Privacy Officer will contact you if any additional information from you is required and will notify you in writing of the determination. If you are not satisfied with the outcome of your complaint, you are entitled to contact the Office of the Australian Information Commissioner.

Privacy Officer: The General Manager
Address: Level 20 Exchange Tower 2 The Esplanade Perth WA 6000
Telephone: 08 9225 4462
Email: management@bellwetherfg.com.au

Spam Policy

Spam is a generic term used to describe electronic 'junk mail'- unwanted messages sent to a person's email account or mobile phone. In Australia, spam is defined as 'unsolicited commercial electronic messages.

'Electronic messaging' covers emails, instant messaging, SMS and other mobile phone messaging, but does not cover normal voice-to-voice communication by telephone.

Bellwether Financial Group Pty Ltd complies with the provisions of the Spam Act when sending commercial electronic messages.

Equally importantly, Bellwether Financial Group Pty Ltd makes sure that its practices are in accordance with the Australian Privacy Principles in all activities where Bellwether Financial Group Pty Ltd deals with personal information. Personal information includes Bellwether Financial Group Pty Ltd's clients contact details.

Internal Procedure for Dealing with Complaints

The three key steps Bellwether Financial Group Pty Ltd follows:

Consent – Only commercial electronic messages are sent with the addressee's consent – either express or inferred consent.

Identify – Electronic messages will include clear and accurate information about the person and the Bellwether Financial Group Pty Ltd contact that is responsible for sending the commercial electronic message.

Unsubscribe – Bellwether Financial Group Pty Ltd ensures that a functional unsubscribe facility is included in all its commercial electronic messages and deal with unsubscribe requests promptly.

Comply with the Law regarding Viral Messages

Bellwether Financial Group Pty Ltd ensures that Commercial Communications that include a Forwarding Facility contain a clear recommendation that the Recipient should only forward the Commercial Communication to persons with whom they have a relationship, where that relationship means that person could be said to have consented to receiving Commercial Communications.

Comply with the Age Sensitive Content of Commercial Communication

Where the content of a Commercial Communications seeks to promote or inspire interaction with a product, service or event that is age sensitive, Bellwether Financial Group Pty Ltd takes reasonable steps to ensure that such content is sent to Recipients who are legally entitled to use or participate in the product service or event.

Complaints Resolutions

The Spam Act specifies that the person's consent has been withdrawn within five working days from the date that an unsubscribe request was sent (in the case of electronic unsubscribe messages) or delivered (in the case of unsubscribe messages sent by post or other means).

Please contact Bellwether Financial Group Pty Ltd's Privacy Officer if you wish to complain about any breach or potential breach of your privacy rights. Your complaint will be responded to within 7 days.

If you are not satisfied with the outcome of your complaint, you are entitled to contact the Office of the Australian Information Commissioner.

Privacy Officer: General Manager
Address: Level 20 Exchange Tower 2 The Esplanade Perth WA 6000
Telephone: 08 9225 4462
Email: management@bellwetherfg.com.au

APPENDIX A:

Implementation

Bellwether Financial Group Pty Ltd demonstrates commitment to the privacy program by implementing best practices and adherence to privacy standards and compliance with the NDB Scheme with its commitment to:

- Bellwether Financial Group Pty Ltd Privacy Policy and
- Data Breach Response Plan

Bellwether Financial Group 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, Bellwether Financial Group Pty Ltd follows a documented plan covering strategy, assessment, treatment, and review of data breaches.

Response Team

The Bellwether Financial Group Pty Ltd's Senior Management and the Compliance Manager (Response Team) will have the overall responsibility for overseeing the Privacy Policy and Data Breach Response Plan. Both 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

All Bellwether Financial Group Pty Ltd's representatives will be provided with an Induction Program outlining its policies and expectations that all representatives' actions will be in accordance with Licensee policies, including the identification of privacy breaches.

Notification

When Bellwether Financial Group 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 regarding 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 follows:
    - 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, Bellwether Financial Group 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.

Serious Harm

The risk of serious harm is assessed, from the perspective of a *reasonable person*, regarding 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.*
>
> *The phrase 'likely to occur' means the risk of serious harm to an individual is more probable than not (rather than possible).*

Refer Appendix B: Assessment of Risk of Serious Harm

Data Breach Response Plan

This data breach response plan sets out procedures and reporting lines for Bellwether Financial Group Pty Ltd and its management, representatives and staff if they suspect or experience a 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 to the Response Team to undertake the breach response process.

Breach Response Process:

1. **Contain the breach and do a preliminary assessment**

All Bellwether Financial Group 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:

a. Personal information the breach involves;
b. Cause of the breach;
c. Extent of the breach;
d. Harms breach could potentially cause to affected persons; and
e. How the breach can be contained.

Records will be kept relating to the initial investigation and ongoing breach response process with ongoing updates on key developments 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**

Bellwether Financial Group Pty Ltd will take steps to initiate the assessment, investigate by gathering relevant information and evaluate via an evidence-based decision about whether serious harm is likely.
Bellwether Financial Group 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 1: Assessing the Risk of Serious Harm*
    - What harm to individuals could result from the breach?
    - Who is the recipient of the information?
- Risk of other harms
    - Loss of trust o Damage to reputation
    - Legal liability

Where possible, Bellwether Financial Group 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 assist Bellwether Financial Group 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 Bellwether Financial Group 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: Bellwether Financial Group Pty Ltd does not have to report all breaches. 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.

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 act 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.

Appendix B

Assessment of Risk of Serious Harm

This NDB scheme includes a non-exhaustive list of 'relevant matters' that assists Bellwether Financial Group Pty Ltd 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.

In addition, s26WG provides the following information that may assist Bellwether Financial Group Pty Ltd is its assessment of 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.