

# HARBOUR ADVISORY (PTY) LTD

## Protection of Personal Information Policy

### 1. Scope

This policy applies to everyone with access to Personal Information available to them due to their relationship with Harbour Advisory (Pty) Ltd.

It addresses the rights of Data Subjects, being the various categories of people whose personal information we have access to.

Personal Information broadly means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly to a specific natural or juristic person / Data Subject.

This policy must be read together with Harbour Advisory (Pty) Ltd Records Management, Cyber Security and Business Continuity Policies.

### 2. Purpose

This Policy aims to ensure Harbour Advisory (Pty) Ltd compliance with various laws and regulations addressing Personal Information and sets out how Harbour Advisory (Pty) Ltd handles their Data Subjects' Personal Information and additionally lists the purpose(s) said information is used for.

### 3. Policy

Harbour Advisory (Pty) Ltd is committed to protecting the privacy of Data Subjects and to ensuring that their Personal Information is used appropriately, transparently, securely and in accordance with applicable laws.

We subscribe to the Protection of Personal Information Act Principles and will:

1. Obtain and process information fairly.
2. Keep information only for one or more specified, explicit, and lawful purposes.
3. Use and disclose information only in ways compatible with these purposes.
4. Keep information safe and secure.
5. Keep information accurate, complete, and up to date.
6. Ensure that information is adequate, relevant, and not excessive.
7. Retain information for no longer than is necessary for the purpose or purposes.
8. Provide a copy of personal data kept to the Data Subject on request.

### 4. Procedures

#### 4.1 Personal Information Collected

Harbour Advisory (Pty) Ltd will generally collect some of the following personal information from our Data Subjects:

- Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, colour, age, physical or mental health, well-being, disability, language, and birth.
- Information relating to the education, medical, financial, criminal or employment history.
- Identifying number, name, symbol, e-mail address, physical address, telephone number, location information.
- Biometric information (employees).
- Correspondence sent/received that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence.
- The views or opinions of another individual about our Data Subject.

We have agreements in place with all our product suppliers, and third-party service providers to ensure that there is a mutual understanding with regards to the protection of Personal Information.

We may also supplement the information provided with information we receive from other providers to offer a more consistent and personalised experience in clients' interaction with us.

#### **4.2 How Personal Information is used**

Personal Information will only be used for the purpose for which it was collected and agreed. This may include:

- Providing a product / service to a Data Subject;
- As part of employee on-boarding or any other internal human resources function;
- Conducting credit reference searches or verification;
- Confirming, verifying, and updating contact details;
- For the detection and prevention of fraud, crime, money laundering or other malpractice;
- For audit and record keeping purposes;
- In connection with legal proceedings;
- Providing our services to a Data Subject to carry out the services requested and to maintain and constantly improve the relationship;
- Providing communications in respect of Harbour Advisory (Pty) Ltd and regulatory matters that may affect Data Subjects;
- In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law;
- To carry out the transaction(s) requested;
- For underwriting purposes;
- Assessing and processing claims;
- For purposes of claims history; and or
- Conducting market or customer satisfaction research.

In terms of the provisions of the Protection of Personal Information Act, Personal Information may only be processed if certain conditions are met, which are listed below, along with supporting information for Harbour Advisory (Pty) Ltd processing of Personal Information:

- When Data Subject consents to the processing – consent only required where the information will be used for something other than the intended use for which the information is supplied.
- The processing is necessary.
- Processing complies with an obligation imposed by law on Harbour Advisory (Pty) Ltd
- Processing protects the legitimate interest of the Data Subject.
- Processing is necessary for pursuing the legitimate interest of Harbour Advisory (Pty) Ltd or of a third party to whom information is supplied.

#### **4.3 Disclosure of Personal Information**

We will only disclose a Data Subject's Personal Information for a reason it was not intentionally supplied for where we have a duty or a right to disclose in terms of the law or where it is necessary to protect our rights.

We have agreements in place to ensure compliance with confidentiality and privacy conditions.

We may also share client Personal Information with, and obtain information about, clients from third parties for the reasons already discussed above.

#### **4.4 Safeguarding Personal Information**

We will adequately protect the Personal Information we hold and avoid unauthorised access and use of Personal Information. We will continuously review our security controls and processes to ensure that personal Information is secure.

When we contract with third parties, we impose appropriate security, privacy, and confidentiality obligations on them to ensure that Personal Information is kept secure.

We may need to transfer (electronic) Personal Information to another country for processing or storage. We will ensure that anyone to whom we pass personal information agrees to treat Personal Information with a similar level of protection as afforded by ourselves.

#### **4.5 Access and correction of Personal Information**

Data Subjects have the right to access the Personal Information we hold about them. Data Subjects also have the right to request us to update, correct or delete their Personal Information on reasonable grounds. Once a Data Subject objects to the processing of their Personal Information, Harbour Advisory (Pty) Ltd may no longer process said Personal Information. We will take all reasonable steps to confirm our Data Subject's identity before providing details of their Personal Information or making changes to their Personal Information. Harbour Advisory (Pty) Ltd Information Officer will be responsible for managing this process.

#### **4.6 Sharing personal information**

We will disclose your personal information to service providers, affiliates or third parties including Investment Managers, Custodians, Linked Investment Services Platforms, Insurers for everyday business purpose e.g. to facilitate transactions and maintain your accounts or in response to court orders or legal investigations.

We have a mutual understanding with all our product suppliers and third-party service providers mutual understanding with regards to the protection of Personal Information.

Due to the nature of our infrastructure information may also be shared with:

- Microsoft Corporation

#### **4.7 Monitoring of communications**

We record and monitor telephone conversations and electronic communications with you for the purposes of (i) ascertaining the details of instructions given, the terms on which any transaction was executed or any other relevant circumstances, (ii) ensuring compliance with our regulatory obligations; and / or (iii) detecting and preventing the commission of financial crime.

#### **4.8 Data breaches**

Even though Harbour Advisory (Pty) Ltd will take every precaution to prevent a data breach, a breach may still occur.

A personal data breach is a breach of security leading to a:

- Confidentiality breach – an accidental or unauthorised disclosure of, or access to, personal data.
- Availability breach – an accidental or unauthorised loss of access to, or destruction of, personal data and/or
- Integrity breach – an accidental or unauthorised alteration of personal data.

##### **4.8.1 Notification to the Information Regulator ("IR")**

The Information Regulator must be notified of the breach if it is likely to result in a risk to the rights and freedoms of data subjects i.e., if, for example, it could result in:

- loss of control over their data
- limitation of their rights
- discrimination
- identity theft
- fraud
- damage to reputation
- financial loss
- unauthorised reversal of pseudonymisation
- loss of confidentiality
- any other significant economic or social disadvantage.

Where a breach is reportable, the Company must notify the Information Regulator without undue delay and, where feasible, no later than **72 hours** after becoming aware of the breach. If our report is submitted late, it must also set out the reasons for our delay.

The notification must at least include:

- a description of the nature of the breach including, where possible, the categories and approximate number of affected data subjects and the categories and approximate number of affected records;
- the name and contact details of the **Information Officer**;
- a description of the likely consequences of the breach; and
- a description of the measures taken, or to be taken, by the Company to address the breach and mitigate its possible adverse effects.

#### 4.8.2. Communication to affected Data Subjects

Where the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, Harbour Advisory (Pty) Ltd also needs to communicate the breach to the affected data subjects without undue delay, i.e., as soon as possible.

Reporting to Data Subjects may however be delayed if reporting may lead to an increased risk to the Data Subject.

In clear and plain language, Harbour Advisory (Pty) Ltd must provide affected Data Subjects with:

- a description of the nature of the breach;
- the name and contact details of Harbour Advisory (Pty) Ltd's Information Officer and CEO;
- a description of the likely consequences of the breach;
- a description of the measures taken, or to be taken, by Harbour Advisory (Pty) Ltd to address the breach and mitigate its possible adverse effects;
- practical advice on how to limit the damage, e.g., resetting their passwords; and
- Data subjects will be contacted individually, by e-mail, unless that would involve Harbour Advisory (Pty) Ltd in disproportionate effort such as where contact details have been lost as a result of the breach or were not known in the first place, in which case we will use a public communication, such as a notification on our website.

However, Harbour Advisory (Pty) Ltd is not required to report the breach to Data Subjects if:

- appropriate technical and organisational protection measures have been implemented, and those measures have been applied to the personal data affected by the breach, in particular those that render the personal data unintelligible to any person who is not authorised to access them, such as state-of-the-art encryption, or
- subsequent measures were taken to ensure that the high risk to the rights and freedoms of Data Subjects is no longer likely to materialise.

Communication to Data Subjects with regards to Data Breaches may under no circumstances be communicated or published without prior approval of Harbour Advisory (Pty) Ltd **Information Officer**.

#### 4.8.3 Data breach register

Harbour Advisory (Pty) Ltd will maintain a register of all personal data breaches, regardless of whether they are notifiable to the Information Regulator. Please see a template register in Annexure A.

#### 4.8.4 Data breach reporting procedure

If anyone knows or suspects that a personal data breach has occurred, they must immediately both advise their line manager and contact the Company's CEO. Evidence in relation to the breach must be retained.

Harbour Advisory (Pty) Ltd will investigate and assess the actual or suspected personal data breach in accordance with the response plan set out below and will determine who should be notified and how.

#### 4.6.5 Response plan

According to Harbour Advisory (Pty) Ltd response plan the **Information Officer** will:

- Make an urgent preliminary assessment of what data has been lost, why and how.
- Take immediate steps to contain the breach and recover any lost data.
- Undertake a full and detailed assessment of the breach.
- Record the breach in the Company's data breach register.
- Notify the Information Regulator where the breach is likely to result in a risk to the rights and freedoms of data subjects.
- Notify affected Data Subjects where the breach is likely to result in a high risk to their rights and freedoms.
- Respond to the breach by putting in place any further measures to address it and mitigate its possible adverse effects, and to prevent future breaches.

Please see Annexure B for more information.

#### 4.9 Information Officer

The Protection of Personal Information Act appoints the highest level of authority in an organisation as the Information Officer. The Information Officer has been tasked with ensuring compliance with data protection and privacy legislation and regulations.

The details of our Information Officer and Deputy Information Officer are as follows:

##### Information Officer

Name and Surname: Eugene Maree

Information Officer Registration Number:

Our Deputy Information Officer is Razina Gareeb, they are both contactable at our Head Office:

Telephone Number: 010 593 3109

Physical Address: 2<sup>nd</sup> Floor, Lacey Oak House, Ballyoaks Office Park, 35 Ballyclare Drive, Bryanston

Email Address: [razina@harbouradvisory.co.za](mailto:razina@harbouradvisory.co.za)

## 5. Consequences of Non-Adherence

Compliance monitoring will be performed regularly, and feedback will be provided to the Deputy Information Officer of Harbour Advisory (Pty) Ltd.

Action will be taken against those that do not adhere to requirements and principles stated in this policy.

## 5. Training and awareness

Relevant staff will receive training on what is required from them.

## 6. Review

This policy shall be reviewed as and when Harbour Advisory (Pty) Ltd compliance management strategy and framework change or the business strategy changes, but at least annually.

## 7. Version control and approval

Version	Date approved	Approved by	Notes
V1	29 June 2021	Razina Gareeb	To be reviewed annually



## Annexure B: Data Breach Response plan for Harbour Advisory (Pty) Ltd

### CONTAIN

- Data breaches must immediately on discovery be reported to the Information Officer who will drive implementation of this plan.
- If the breach took place through an electronic device:
  - Take the device offline immediately, but DO NOT shut it down
  - Change passwords

### ASSESS

- Determine the extent of the breach
  - who was affected
  - which records have been affected
- Determine the impact of the breach
- Determine if the breach should be reported to
  - the Information Regulator
  - Data Subjects

### MANAGE

- Agree what the appropriate actions will be
  - Facilitate technology restoration or recovery if applicable
  - Prepare and submit insurance claim
- Communicate decisions internally
- Prepare (and arrange for authorisation of) and Communicate with Customer(s) / Public
- Take remedial action to prevent similar breaches