PROTECTION OF PERSONAL INFORMATION (INTERNAL) POLICY

PREMIER

honey
INVESTMENT SOLUTIONS

Table of Contents

1. APPLICATION OF THE POLICY

1.1 The Premier Group, as set out in the orginisational organogram as amended from time to time, relates to a group of companies that constitutes a holding company and subsidiaries, referred to hereinafter as "we/our", "the Company" or “the Group”, each possessing their individual set of business practices and risks. To ensure consistency and compliance across our entire organisation, we have developed this comprehensive Policy that applies to all our subsidiary and associate companies, pertaining to all aspects of their operations and business dealings. This Protection of Personal Information Policy (Privacy Policy / Policy) is compiled in terms of the Promotion of Access to Information Act, No 2 of 2000, the Protection of Personal Information Act no 4 of 2013 (POPIA) and the General Data Protection Regulation (GDPR) when applicable.

1.2 The Retirement Funds are distinct legal entities, established and supported This policy outlines how all employees, representatives, contractors, temporary staff and associated persons of the Group and/or the Retirement Funds who handle personal information in any form within the Group, must handle personal information to ensure compliance with POPIA and protect the rights of data subjects.

2. PURPOSE OF THE POLICY

2.1 The Protection of Personal Information Act, 4 of 2013, (“POPIA”), which came into force on 1 July 2021, is a statute that regulates the use and processing of a person and/or legal entity’s personal information.

2.2 The purpose of this policy is to:

2.1.1. Promote a culture of data privacy and security within the organization;

2.1.2. Ensure that personal information is collected, processed, stored, and shared in a lawful, fair, and transparent manner;

2.1.3. Safeguard the confidentiality, integrity, and availability of personal information;

2.1.4. Prevent unauthorized access, disclosure, or misuse of personal information;

2.1.5. Outline the obligations of employees, directors, and trustees in handling personal information; and

2.1.6. Align the Group’s operations with the regulatory requirements of POPIA, FAIS, and the Pension Funds Act.

3. DEFINITIONS

3.1. **Authorities:** means the Prudential Authority as established in terms of section 32 of the Act and the Financial Sector Conduct Authority as established in terms of section 56 of the Act;

3.2 **Compliance Officer:** means the person appointed by the Group as the legal and governance compliance officer;[1]

3.3 **Data subject:** means the person to whom personal information relates;

3.4 **Information officer:** means the head of the juristic entity;[2]

3.5 **Information Regulator:** means an independent body established in terms of POPIA and is amongst others empowered to monitor and enforce compliance by public and private bodies within the provisions of PAIA and POPIA;

3.10 **IT security:** means the appointed service provider responsible for the protection of all electronic data for the Group;

3.11 **Material incident:** means a disruption of a business activity, process or function which has, or is likely to have, a severe and widespread impact on the financial institution's operations, services to its customers, or the broader financial system and economy;

3.12 **Operator:** means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party;

3.13 **Personal information:** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to –

a) information relating to the race, gender, sex, pregnancy status, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of the person;

b) information relating to the education or the medical, financial, criminal or employment history of the person;

c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

d) the biometric information of the person;

e) the personal opinions, views or preferences of the person;

f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

g) the views or opinions of another individual about the person; and

h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

3.16 **POPIA:** means the Protection of Personal Information Act, 2013 (act 4 of 2013) (as amended from time to time);

3.17 **POPIA (data) breach:** means when there is unauthorized access, loss, disclosure, destruction, or alteration of personal information of any nature (regardless of the harm or risk posed to the data subject). Examples include:

[1] The Group appointed Monique Collyer as Compliance Officer.

[2] Honey Investment Solution's (prev. Premier Product Solutions) appointed IO is Chad Menton. Premier Benefits' appointed IO is the director. The Retirement Funds appointed the principal officer as its IO.

a) Accidental or unlawful disclosure of personal information

b) Loss or theft of devices containing personal information

c) Cyberattacks or hacking incidents

d) Employee negligence leading to unauthorized data exposure

when there are reasonable grounds to believe that any unauthorized person has accessed or acquired personal information under the control of the Group, or if data has been intentionally or accidentally lost, shared or destroyed. Data breaches may occur in different ways, including but not limited to hacking, theft, accidental loss and unauthorized use of personal information. Remember that a data breach can take place through either physical or electronic means. This means that the theft of a laptop containing potentially personal information of your clients, will constitute a data breach in terms of POPIA**.**

3.18 **Responsible party:** means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

3.19 **Retirement funds** means the Honey (previously Premier) Retirement Annuity Fund, registration number 12/8/38196; the Honey (previously Premier) Preservation Fund, registration number 12/8/38197; the Prime Pension Fund, registration number 12/8/37068; and the Prime Provident Fund, registration number 12/8/37069;

3.20 **Senior Management**: means –

(a) the chief executive officer or the person who is in charge of the Group; or

(b) a person, other than a director or a head of a control function-

(i) who makes or participates in making decisions that-

(aa) affect the whole or a substantial part of the business of the Group; or

(bb) have the capacity to significantly affect the financial standing of the Group; or

(ii) who oversees the enforcement of policies and the implementation of strategies approved, or adopted by the governing body;

3.21 **Sponsor** means the entity who established and/or supports the Retirement funds, noted within each set of fund rules.

3.22 **Supporting documentation:** means all documentation used in the computer system in the construction, clarification, implementation, use or modification of the Software or data.

4. EMPLOYEE RESPONSIBILITIES

Employees are responsible for:

4.1 Understanding and complying with POPIA and this policy.

4.2 Processing personal information only for lawful and authorised purposes.

4.3 Keeping personal information confidential and secure.

4.4 Reporting any suspected data breaches immediately.

4.5 Completing required POPIA training provided by the Company.

5. TYPES OF INFORMATION COLLECTED AND PROCESSED

5.1 **General information:**

5.1.1 Identifying information: the Data subject's name and/or date of birth or identification number of any kind;

5.1.2 Contact information: the Data subject's phone or mobile number and/or email address;

5.1.3 Address information: the Data subject's physical and/ or postal address;

5.1.4 Demographic information: the Data subject's gender and /or marital status.

5.2 **Sensitive personal information:**

5.2.1 Financial information: the Data subject's bank account details;

5.2.2 Sensitive demographic information: the Data subject's race and ethnicity;

5.2.3 Medical information: information about the Data subject's physical and /or mental health;

5.2.4 Criminal information: information about a charge or alleged charge of any offence and / or about any related legal proceedings; or

5.2.5 Employment information: the Data subject's membership of a trade union.

5.3 **Application Information:** If the Data subject's submit an application to become a client, member or investor or are already one, the Group may collect the following from him/her:

5.3.1 the Data subject's name and surname or your company name, company registration number and VAT number;

5.3.2 the Data subject's date of birth and / or age and /or proof of identification in the form of copies of his/her passport, driving license or other identity documents;

5.3.3 the Data subject's postal and /or street address;

5.3.4 financial information, including the Data subject's bank account information, the amount he/ she is looking to invest, and any monthly payments he/ she may wish to make, his/her investment selection(s) and bank details for any relevant income or redemption payments to be made;

5.3.5 personal information and contact information which the Data subject's provide in correspondence with the Group, whether by email, written letter, or telephone call or through our online enquiry system (this will be information volunteered by the Data subject's, it could include the reasons why he /she has decided to invest, or where investment money has come from, by way of example); and/or

5.3.6 information relating to the Data subject's use of our service and products.

5.4 **Website use information:** When you interact with our website:

5.4.1 where the Data subject has an account, financial information such as portfolio and account numbers, as well as login information, including username and password encryption key;

5.4.2 where the Data subject applies for employment, such information may include education and qualification details, training and professional memberships and accreditations, date of birth; and/or

5.4.3 technical information about our products and services and how the Data subject uses them;

5.4.4 The Group may collect certain information from the Data subject's web browser, including Internet usage information when visiting our website:

a) The Group may place small text files called 'cookies' on the Data subject's device when visiting our website. These files do not contain personal information, but they do contain a personal identifier allowing us to associate the Data subject's Personal information with a certain device. These files serve several useful purposes for the Data subject, including:

i. tailoring our website's functionality to you personally by letting us remember your preferences;

ii. improving how our website performs;

iii. allowing third parties to provide services to our website

b) The Data subject's internet browser accepts cookies automatically, but you can often change this setting to stop accepting them. You can also delete cookies manually. However, no longer accepting cookies or deleting them will prevent you from accessing certain aspects of our website where cookies are necessary. Many websites use cookies, and you can find out more about this in our **Cookie Policy**.

5.5 **Regulatory and Compliance use:** In addition to the above, the Group collects the following information from the Data subject when required:

5.5.1 tax residency and/or nationality;

5.5.2 personal information which we obtain from identity verification agencies;

5.5.3 information about employment status (including whether the Data subject is employed, retired, or receive benefits) and regarding the source of wealth; and/or

5.5.4 to secure online validation facility, the answers to security verification questions, and / or username.

6. CONSENT TO PROCESS PERSONAL INFORMATION

6.1 Where consent is required for processing a Data subject's Personal information, employees must ensure that such consent is obtained lawfully. The Data subject has the right to withdraw their consent at any time. However, in cases where the processing is based on legitimate grounds other than consent, such withdrawal will not affect the continued lawful processing of Personal information.

6.2 If a Data subject wishes to withdraw their consent, employees must facilitate the process by directing the Data subject to info@honeyinvestments.co.za.

6.3 Employees must rely on consent in the following instances:

6.3.1 When a Data subject explicitly requests that their Personal information be shared with a third-party;

6.3.2 Where a Data subject has opted-in to receiving marketing communication; and/or

6.3.3 When a Data subject voluntarily provides Personal information in correspondence, which is necessary to respond to their inquiry, and only where lawful to do so.

6.4 Employees must acknowledge that a Data subject has the right to withdraw consent at any time, however such withdrawal will not invalidate any processing undertaken prior to the withdrawal.

6.5 Employees must recognize that where another lawful basis exists for processing a Data subject's Personal information—such as contractual necessity or legal compliance—withdrawal of consent will not affect the processing of information for those purposes.

6.6 If a Data subject chooses not to provide voluntary Personal information, employees must inform them that this may impact the quality of service provided.

6.7 Employees must take reasonable steps to ensure that Personal information collected remains accurate and up to date. Data subjects must be encouraged to review and update their Personal information through designated channels. Employees must verify a Data subject's identity before making any corrections to their Personal information to safeguard data security.

6.8 Employees must not knowingly collect or process the Personal information of children without the verified consent of a parent or legal guardian. If a Data subject is under 18 years of age, their Personal information must only be processed with the necessary consent.

7. SHARING OF PERSONAL INFORMATION

7.1 Employees may only share a Data subject's Personal information with third-parties where it is necessary for business operations, regulatory compliance (regulators and authorities), or with the Data subject's consent.

7.2 Employees must inform Data subjects of the third-parties with whom their Personal information is shared upon request.

7.3 Employees must comply with legal obligations requiring the disclosure of Personal information to third-parties (e.g., tax authorities, regulators). Where third-parties are contracted to assist in business operations or fund administration, employees must ensure that appropriate agreements and safeguards are in place to protect Personal information.

7.4 Employees must not sell, rent, or trade Personal information of Data subjects.

7.5 Employees may share Personal information with regulators, governmental authorities, and law enforcement agencies for compliance, crime prevention, and other legal obligations.

7.6 Where applicable, employees must ensure compliance with jurisdictional requirements that mandate disclosure of certain Personal information to regulatory bodies, exchanges, or authorities for market transparency.

7.7 Employees must acknowledge that once Personal information is shared with another data controller, the Data subject may need to exercise their data rights directly with that third-party.

7.8 Employees must ensure that Personal information is shared only with authorized individuals or organizations, including:

- 7.8.1 Internal employees and management with a legitimate need to process the information;
- 7.8.2 Legal, professional advisors, and auditors;
- 7.8.3 Governmental and regulatory authorities such as financial or tax regulators;
- 7.8.4 Overseas tax authorities where required by law;
- 7.8.5 Service providers under contractual agreements, such as IT service providers, document storage providers, auditors, and compliance consultants;
- 7.8.6 Prospective buyers or managers in case of business restructuring;
- 7.8.7 Identity verification agencies;
- 7.8.8 Market research organizations engaged to improve business services;
- 7.8.9 Successors in the event of business transfers; and/or
- 7.8.10 Law enforcement or other legal bodies when required by a valid legal instrument.

7.9 Employees must ensure that before transferring a Data subject's personal information outside the country, written consent is obtained where required, and appropriate safeguards are in place. This includes contractual obligations that require the recipient to maintain equivalent levels of data protection or adherence to recognized international data-sharing frameworks.

8. PROCESSING OF PERSONAL INFORMATION

8.1. Personal information includes information the Group collects:

8.1.1. automatically when visiting our website or on completion of applications;

8.1.2. on registration;

8.1.3. on submission; and

8.1.4. optional information provided voluntarily;

8.2. Personal information **excludes:**

8.2.1. information that has been made **anonymous** so that it does not identify a specific person;

8.2.2. permanently **de-identified** information that does not relate, or cannot be traced back, to you specifically;

8.2.3. **non-personal statistical** information collected and compiled by us; and

8.2.4. information that you have provided voluntarily in an open**, public** environment or forum including any blog, chat room, community, classifieds, or discussion board (because the information has been disclosed in a public forum, it is no longer confidential and does not constitute personal information subject to protection under this Policy).

8.3. The Group may use or process any products or services information, or voluntary / optional information provided to us for the purposes indicated when the data subject agreed to provide it to us. Processing includes:

8.3.1. gathering personal information;

8.3.2. disclosing it, and

8.3.3. combining it with other personal information.

8.4. Employees must adhere to the following principles when processing personal information:

8.4.1. **Lawfulness, Fairness, and Transparency:** Information must be collected and processed lawfully:

a) Most of this information is necessary for the Group to comply with our legal obligations, to enter into an agreement with you, or for legitimate business purposes.

8.4.2. **Purpose Limitation:** the Group needs to use some personal information to provide the Data subject with our service and to fulfil our contract with him /her. Information must only be used for the purposes for which it was collected. The Group collects and processes personal information for various purposes, including:

a) **products or services purposes** – such as collecting applications or requests for and providing our products or services;

b) **marketing purposes** – such as pursuing lawful related marketing activities;

c) **business purposes** – such as internal audit, accounting, business planning, and joint ventures, disposals of business, or other proposed and actual transactions; and

d) **legal purposes** – such as handling claims, complying with regulations, or pursuing good governance.

We may use the Data subject's website usage information for the purposes described above and to:

a) remember the Data subject's information so that he/she does not have to re-enter it during his/her visit or the next time accessing the website or applications;

b) monitor website and application usage metrics such as total number of visitors and pages accessed; and

c) track the Data subject's entries, submissions, and status in any promotions or other activities in connection with his/her usage of the website or applications.

The Group may send administrative messages and email updates to the Data subject about the products and services he/she subscribed to. In some cases, we may also send him/her primarily promotional messages. The Data subject can choose to opt-out of promotional messages and unsubscribe from email updates. The Group will not send you promotional messages unless the Data subject has chosen to opt into them.

8.4.3. **Data Minimization:** Only necessary data should be collected and retained:

Personal information must not be retained for longer than is necessary for the lawful purposes for which it is processed. To achieve this, each category of Personal information processed by or on behalf of the Group shall be subject to a retention period which can be justified by reference to those lawful grounds. Retention periods shall be monitored and upon their expiry, the relevant Personal information must be deleted or anonymised, so that it is no longer possible to identify the Data Subject to whom the Personal information relates.

8.4.4. **Accuracy:** Ensure that information is correct and up to date.

8.4.5. **Security:** Protect information from unauthorised access and breaches:

We implement appropriate technical and organizational measures which seek to ensure that personal data is appropriately protected against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or unauthorized access.

8.4.6. **Accountability:** Employees are accountable for complying with POPIA.

9. SECURITY MEASURES

9.1. The Company has implemented various security measures to protect personal information, including:

9.1.1 Password protection and access control mechanisms.

9.1.2 Secure storage and encryption of electronic data.

9.1.3 Restriction of access to personal information on a need-to-know basis.

9.1.4 Regular audits to ensure compliance with this Policy.

9.2. Personal data must be disposed of securely in a way that protects the rights and privacy of Data Subjects and ensures the permanent erasure of the data. This includes shredding, disposal of confidential waste and secure electronic deletion.

9.3. The Group's operators and third-party service providers will be required to enter into service level agreements with the Group where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

9.4. Where data is stored on:

Paper	**Electronically**
it must be kept in a secure place, when not in use, such that an unauthorized person cannot access the information. e.g. should be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated. This also applies to data stored electronically which has been printed to hard copy.	it must be kept in a secure place, when not in use, such that an unauthorized person cannot access the information. e.g. electronic storage media, should be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated.
Employees should ensure that paper and printouts are not left in places where unauthorized persons can gain access, e.g., on a printer or an employee's desk.	it must be protected from unauthorized access, accidental deletion, or risk of exposure to malicious hacking attempts:
All unwanted paper must be shredded.	it should be protected by strong passwords that are changed regularly and never shared between employees;
A Clean Desk / clear screen Policy reduces the risks of unauthorized access, loss of and damage to information during and outside normal working hours. All employees must clear their desks or all personal information when leaving them for any length of time and at the end of the day.	if stored on removable media such as a DVD, USB, or any other type of removeable media these must always be locked away securely when not in immediate use;
Safes or other forms of secure storage facilities might also protect information stored therein against disasters such as a fire, earthquake, flood, or explosion.	All data may only be stored on designated servers and may only be uploaded to approved cloud computing services;

	Data will be backed up frequently in accordance with backup protocols. Such backups will be tested regularly in line with the company's standard backup procedures and protocols under the direction of the IT Manager;
	Personal data may not be saved directly to laptops or other mobile or removable devices, such as tablets or smart phones or removable USB drives;
	In exceptional circumstances, where personal data must be saved to a laptop hard drive to work offline, this may only be done where the laptop has been protected with hard drive encryption;
	All servers and computers containing data will be protected by approved security software, and one or more firewalls under the direction of the IT Manager.

10. DATA BREACH MANAGEMENT

In the event of a data breach:

10.1 Employees must report the breach immediately to the Information Officer at info@honeyinvestments.co.za with the subject matter: POPIA BREACH.

10.2 The Company will assess the impact of the breach and take remedial actions.

10.3 Where required, the Information Regulator and affected individuals will be notified.

Step		**Accountable party**
Identification & Immediate Response	Any employee, contractor or third-party who becomes aware of a potential or actual data breach must immediately report it to the Information Officer using the **Data Breach Report Form** (see Annexure A1).	All employees and/or contractors, third-parties (Operators) where applicable
	If feasible, the individual discovering the breach must take immediate action to contain it (e.g., retrieving emails sent in error, isolating affected systems, or securing lost documents by sending an	

	email to the unintended recipient with a request to delete and not distribute /share the personal information further -refer to Annexure A2).	
Assessment & Classification	The Information Officer / Deputy IO / Group Compliance Officer will assess the incident based on the following criteria: • **Nature of the breach** (e.g., accidental vs. malicious) • **Types of personal data involved** • **Number of data subjects affected** • **Potential risk and harm to data subjects**	Information Officer /deputy Information Officer
Containment & Mitigation	IT Security and relevant departments will implement containment measures, such as revoking access credentials, recovering lost data, or applying security patches, remotely wipe the laptop, or track such or enable encryption.	IT Security company[3]
	Legal and Compliance teams will evaluate regulatory obligations and potential liabilities.	Compliance Officer
Notification to Affected Parties & Regulator	If the breach poses a risk to Data subjects, they must be notified[4] as soon as possible, providing details of: • The nature of the breach • Potential consequences of the breach • Steps taken by the Responsible party to mitigate risks	Compliance Officer

[3] Accelerate is the current appointed IT security company.

[4] The notice must be communicated to the data subject concerned in any one of the following ways:

a) By post to the last known physical or postal address of the Data subject;
b) By email to the last known e-mail address of the Data subject;
c) Placed in a prominent position on the website of the Responsible party;

	• Recommendation on mitigating measures to be taken by the Data subject • If known, the identity of the unauthorised person who may have accessed or acquired the personal information • Contact information for further assistance	
	The Information Regulator must be informed[5] **as soon as reasonably possible**.	Information Officer / Deputy IO of the Responsible party
Investigation & Remediation	The Information Officer will conduct a full investigation to determine root causes and implement corrective actions.	Information Officer / Deputy IO of the Responsible party
	Lessons learned will be documented, and security policies, employee training, or technological safeguards will be updated as needed.[6]	
Record Keeping	All breaches, whether reportable or not, must be logged in the **Data Breach Register** for audit and compliance purposes.[7]	Compliance Officer

11. EMPLOYEE RIGHSTS AND OBLIGATIONS

11.1 Employees have the right to:[8]

11.1.1 Request access to their personal information held by the Company.

11.1.2 Request correction or deletion of incorrect or outdated information.

11.1.3 Object to the processing of their personal information under certain conditions.

11.2 Employees must:

11.2.1 Maintain confidentiality of personal data.

11.2.2 Use personal information strictly for authorized purposes.

[5] Follow this link for the specific form and process guidelines: https://inforegulator.org.za/popia-forms/

[6] Regular audits will be conducted to review breach trends and improve data protection measures

[7] All data breaches whether reportable or not, must be recorded in this register and must be maintained for at least 5 years.

[8] Refer to the Data Privacy Notice for more information where the employee is the Data subject.

11.2.3 Follow Company policies and procedures regarding data protection.

12. CONSEQUENCES OF NON-COMPLIANCE

Failure to comply with this policy may result in disciplinary action, including termination of employment, and potential legal consequences.

13. CONTACT INFORMATION

13.1 Contact details of the Information Officer and Compliance Officer:

Email: info@honeyinvestments.co.za (C/O – the Information Officer and the Compliance Officer)

13.2 Should the Data subject wish to lodge a complaint with the information regulator, please ensure that the above data breach steps were followed first.

The contact details of the Information Regulator are as follows:

Physical Address:	**Postal Address:**
JD House, 27 Stiemens Street Braamfontein Johannesburg 2001	P.O Box 31533 Braamfontein Johannesburg 2017
Complaints email:	POPIAComplaints@inforegulator.org.za
General enquiries email:	enquiries@inforegulator.org.za
Website:	https://inforegulator.org.za/contact-us/

14. DOCUMENT REVISION AND APPROVALS

Detailed below is a list of Policy versions and the changes/amendments/additions/ adoptions made to the Policy with each updated version:

DATE	VERSION	CHANGES
January 2022	1.0	Notice established.
20 December 2022	1.0	The Premier Financial Engineering and Premier Investments Distribution Boards adopted the Policy.
August 2024	2.0	The naming convention of the Notice changed to Policy and legislative updates have been made.
31 October 2024	2.0	Board of Prime Financial Engineering approved policy (Resolution 5 of 2025) Board of Premier Product Solutions approved policy (Resolution 6 of 2025) Board of Premier Benefits approved policy (Resolution 6 of 2025) Board of Protected Nominees approved policy (Resolution 6 of 2025)

1 4 February 2025	3.0	Total revision of the policy to make two separate policies -the POPIA policy for internal use (processes and procedures) and the other to serve as a Privacy Notice to clients /customers. A further amendment was to capture the incident management in this policy rather than in a separate Incident Management policy and to include the associated Retirement Funds (Group Sponsored)
3 April 2025	3.0	PFE Board Approved and Adopted the Amended Policy Honey Board Approved and Adopted the Amended Policy PN Board Approved and Adopted the Amended Policy PB Board Approved and Adopted the Amended Policy Premier Retirement Annuity Fund Approved and Adopted the Amended Policy Premier Preservation Fund Approved and Adopted the Amended Policy Prime Pension Fund Approved and Adopted the Amended Policy Prime Provident Fund Approved and Adopted the Amended Policy
1 July 2025	3.1	**Administrative updates applied by Cyd Isdale:** Updates include the revised registered name of Premier Product Solutions (PPS) now known as Honey Investment Solutions, revised registered names of the Premier retirement funds now known as the Honey retirement funds, incorporation of the new company logo, and amendments to email addresses to reflect the updated company identity. **These changes are administrative in nature and do not affect the substance or intent of the policy.**

ANNEXURE A1

TEMPLATE - NOTIFICATION BY EMPLOYEE OF A POPIA (DATA) BREACH

(To be submitted to the Information Officer immediately after identifying a breach)

Section	Details
Date of Report	*[DD/MM/YYYY]*
Reporter's Name	*[Full Name]*
Department	*[Department Name]*
Contact Details	*[Phone & Email]*
Date & Time of Incident	*[DD/MM/YYYY - HH:MM]*
Location of Incident	*[Physical/Online/System]*
Number of affected Data subjects	
Details of the Data subject	*[Name, surname, ID no, contact details]*
Type of Personal Information Involved	☐ Names ☐ ID Numbers ☐ Financial Details ☐ Contact Information ☐ Other: [Specify]
Description of Incident	*[Provide a brief but detailed explanation]*
How was the breach detected?	*[E.g., internal monitoring, external notification, self-reporting]*
Immediate actions taken	*[Steps taken to contain or recover data]*
Has IT Security been notified?	☐ Yes ☐ No
Has the Data subject been notified (if so, provide the method of notification)?	☐ Yes ☐ No
Has the Information Regulator been notified?	☐ Yes ☐ No
Any suspected cause or responsible party?	*[If known]*
Recommendations for prevention	*[Suggestions to prevent recurrence]*

Reporter's Signature: _____

Date: _____

ANNEXURE A2

TEMPLATE - REQUEST BY EMPLOYEE TO THE UNINTENDED RECIPIENT

Subject: Urgent: Request to Delete Incorrectly Sent Information

Dear xxxx

I hope this message finds you well.

I am reaching out to notify you of an inadvertent error that occurred when I sent you an email containing an attachment.

Unfortunately, the attachment included personal information relating to another client, which was not intended for your review.

In line with the Protection of Personal Information Act (POPIA), we kindly request that you:

1. Immediately **delete the email and the attached document** from your **inbox and any backup systems**; and
2. **Confirm by return email** that you **deleted the e-mail and attachment from your inbox and backup systems** and to **further confirm that you will not share, distribute, or make any use of the information contained in the attachment.**

We sincerely apologize for any inconvenience this may have caused and appreciate your cooperation in assisting us to protect the confidentiality of all parties involved.

Please feel free to reach out should you have any questions.

ANNEXURE B

TEMPLATE - NOTIFICATION TO AFFECTED DATA SUBJECTS

Subject: Important: Security Incident Affecting Your Personal Information

Dear [Data Subject's Name],

We are writing to inform you of a **data breach** that may have affected your personal information.

What Happened?

On [insert date], we identified an incident in which your personal information was unintentionally accessed or disclosed to an unintended recipient.

What Information Was Affected?

[Specify, e.g., "Your name, ID number, and email address."]

Potential Risks:

[Describe, e.g., "There is a risk of identity theft or unauthorised use of your personal data."]

What Actions Have We Taken?

- We have taken immediate steps to contain the breach.
- We are reinforcing our data protection policies.
- We are implementing additional security controls to prevent similar incidents.

What Should You Do?

- **Be cautious of phishing emails** or unexpected messages requesting your personal information.
- **Monitor your financial accounts** for any suspicious activity.
- **Update your passwords** if your credentials were affected.

We sincerely apologise for this incident and any inconvenience it may cause. Protecting your information is our priority, and we are taking all necessary steps to prevent future occurrences.

If you have any concerns or require further information, please contact us at:

📧 info@honeyinvestments.co.za

📞 010 900 5129

Best regards,

Name and surname of Information Officer