PROTECTION OF PERSONAL INFORMATION POLICY

010 141 6859
info@raminfinancial.com
www.raminfinancial.co.za
Norwich Place West 2nd floor Cnr 5th and Norwich Sandown Sandton, Gauteng.

2021/675398/07
Ramin is an authorized FSP registered with the FSCA with FSP No. 51897

Table of Contents

1. Introduction

At Ramin Financial Services, our utmost priority is safeguarding the privacy and confidentiality of our clients' personal information. This Privacy Policy delineates our procedures for collecting, utilizing, disclosing, and securing your personal data in alignment with pertinent privacy laws and regulations.

The right to privacy stands as a fundamental human entitlement enshrined in both the South African Constitution and the Protection of Personal Information Act 4 of 2013 ("POPIA"). POPIA is designed to bolster privacy protection by furnishing guiding principles for the handling of personal information in a contextually sensitive manner.

In the course of delivering high-quality goods and services, our organization inevitably engages in the collection, utilization, and disclosure of certain facets of personal information pertaining to clients, customers, employees, and other stakeholders.

An individual's right to privacy encompasses the ability to exercise control over their personal information and conduct their affairs with a degree of autonomy, free from undue intrusions.

Recognizing the paramount importance of privacy, our organization is steadfast in its commitment to effectively manage personal information in full compliance with the provisions delineated in POPIA.

2. Definitions

2.1 Personal Information

Personal information encompasses any data capable of identifying an individual. This includes, but is not limited to:

- Demographic details like race, gender, or age
- Information regarding health, education, finances, or employment
- Contact particulars such as addresses, phone numbers, or email addresses
- Biometric data
- Personal opinions or correspondence of a private nature
- Views or opinions held about the individual
- Any additional information that, when combined, can lead to identification.

2.2 Data Subject

A data subject refers to the individual or entity to whom the personal information pertains, whether it's a client, customer, or supplying company.

2.3 Responsible Party

The responsible party is the entity requiring personal information for specific purposes and determining its processing methods. In this context, the organization assumes this responsibility.

2.4 Operator

An operator processes personal information on behalf of a responsible party under contract or mandate, without direct authority. For instance, third-party service providers engaged by the organization for tasks such as document shredding.

2.5 Information Officer

The Information Officer ensures the organization's compliance with POPIA. In the absence of an appointed officer, the organization's head assumes these duties. Registration with the South African Information Regulator is mandatory prior to commencing duties, with the option of appointing Deputy Information Officers for support.

2.6 Processing

Processing encompasses all activities involving personal information, including collection, storage, retrieval, dissemination, alteration, or destruction.

2.7 Record

Any recorded information regardless of format, including written documents, electronic data, photographs, and recordings.

2.8 Filing System

Structured sets of personal information accessible based on specific criteria, regardless of whether they're centralized or decentralized.

2.9 Unique Identifier

An identifier assigned by a responsible party to uniquely identify a data subject for operational purposes.

2.10 De-Identify

To remove any information that can identify a data subject or can be used, in conjunction with other data, to identify them.

2.11 Re-Identify

To resurrect or manipulate de-identified information to identify the data subject.

2.12 Consent

Voluntary, informed permission for the processing of personal information.

2.13 Direct Marketing

Approaching data subjects, whether in person, by mail, or electronically, for the promotion of goods or services or solicitation of donations.

2.14 Biometrics

Identification techniques based on physical, physiological, or behavioral characteristics, such as fingerprinting or voice recognition.

3. Scope

This notice applies to Ramin Financial Services as well as its (future) subsidiaries. The company offers solutions that are financial and non-financial in nature. These solutions include financial advice, investment, and insurance goods and services. This policy applies to any product, service or goods offered Ramin Financial Services, whether financial or non-financial in nature.

4. Policy Statement

- This policy constitutes an integral component of the internal business processes and procedures of the policy owner.
- Any mention of the "organization" shall encompass the "policy owner."
- The governing body of the organization, along with its employees, volunteers, contractors, suppliers, and any other individuals representing the organization, are obligated to acquaint themselves with the stipulations of this policy and commit to adhering to the outlined processes and procedures.
- Risk owners and control owners are tasked with supervising and upholding control procedures and activities.

5. Policy adoption

By signing this document, I grant authorization for the policy owner to approve and implement the processes and procedures detailed herein.

Name & Surname	Rulich Pretorius
Capacity	Key Individual
Signature	
Date	2024-04-19

Version	4
Publishing Date	April 2024
Last Review Date	n/a
Frequency of Review	Annually
Next Review Date	April 2025
Policy Owner	Willem van Staden

6. Collection of Personal Information

We may collect personal information from clients and prospective clients in various ways, including: Personal Information request form *Annexure A*

- Information provided directly by you when you apply for our products or services, such as your name, contact details, date of birth, identification documents;
- Marital status (married, single, divorced); national origin; age; language; birth; education;
- Financial history (e.g. income, expenses, obligations, assets and liabilities or buying, investing, lending, insurance, banking and money management behaviour or goals and needs;
- Employment history and current employment status;
- Information collected automatically when you use our website or other digital platforms, including IP address, browsing history, and cookies (please refer to our Cookie Policy for more information);
- Information obtained from third parties, such as credit reporting agencies or other financial institutions, with your consent or as permitted by law.

The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as the organisation's PAIA Policy as required by the Promotion of Access to Information Act (Act No 2 of 2000).

The legal duty to comply with POPIA's provisions is activated in any situation where there is:

- A **processing** of…...…
- ……**personal information**…….
- ……entered into a **record**…….
- ……..……..by or for a **responsible person**……
- who is **domiciled** in South Africa.

POPIA does not apply in situations where the processing of personal information:

- is concluded in the course of purely personal or household activities, or
- where the personal information has been de-identified.

7. Use of Personal Information

We may use your personal information for the following purposes:

- To provide you with the products and services you have requested, including processing applications, managing accounts, and facilitating transactions;
- To communicate with you regarding your accounts, inquiries, or requests for information;
- To personalize your experience and improve our products and services;
- To comply with legal and regulatory requirements, including anti-money laundering laws, tax reporting obligations, and fraud prevention;
- To analyze and understand market trends, customer preferences, and demographics to develop and enhance our offerings.

8. Disclosure of Personal Information

We may disclose your personal information to third parties in the following circumstances:

- To our affiliates, partners, or service providers who assist us in delivering our products and services, such as IT providers, payment processors, and professional advisors.
- To regulatory authorities, law enforcement agencies, or other government bodies as required by law or in response to legal requests or obligations.
- With your consent or as otherwise permitted or required by law.

9. Security of Personal Information

We take reasonable measures to safeguard your personal information from unauthorized access, use, or disclosure. These measures include physical, technical, and organizational safeguards designed to protect the confidentiality and integrity of your information.

10. Retention of Personal Information

We will retain your personal information only for as long as necessary to fulfill the purposes for which it was collected or as required by law. When no longer required, we will securely dispose of or anonymize your information in accordance with our retention policies.

11. Your Rights and Choices

You may have certain rights regarding your personal information, including the right to access, correct, or delete your information, as well as the right to object to or restrict certain processing activities. Please contact us using the details provided below to exercise your rights or discuss any concerns you may have about your personal information.

12. Updates to Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, legal requirements, or industry standards. We will notify you of any material changes to this policy by posting a revised version on our website or through other appropriate channels.

For more guidance and updates on privacy regulations, please contact the Information Regulator (South Africa) at:

- *www.inforegulator.org.za*
- *(+27)10 023 5200*

13. Information Officers

The organization may opt to designate an Information Officer and, if deemed necessary, appoint a Deputy Information Officer to provide support. The Information Officer is entrusted with ensuring adherence to POPIA regulations.

Although POPIA does not legally mandate the appointment of an Information Officer, it is widely regarded as a prudent business practice, especially for larger organizations. In the absence of an appointed Information Officer, the organization's head assumes this role. Regular assessments will be conducted to consider the re-appointment or replacement of the Information Officer and any Deputy Information Officers.

Upon appointment, the organization will proceed to register the Information Officer with the South African Information Regulator established under POPIA before commencement of duties. A sample "Information Officer Appointment Letter" is available in Annexure F for reference.

14. POPIA Audit

The organization's Information Officer will arrange regular POPIA Audits. These audits serve several purposes:

- Identifying processes involved in the collection, recording, storage, dissemination, and disposal of personal information.
- Mapping the flow of personal information across the organization, including various business units, divisions, branches, and associated entities.
- Reviewing and refining the purposes for collecting and processing personal information.
- Ensuring processing parameters remain appropriately restricted.
- Informing new data subjects about the processing of their personal information.
- Justifying any further processing when information is obtained through third parties.
- Assessing the quality and security of personal information.
- Monitoring compliance with POPIA and organizational policies.
- Evaluating the effectiveness of internal controls established to manage POPIA-related compliance risks.

During POPIA Audits, Information Officers will collaborate with line managers to pinpoint areas within the organization that are particularly vulnerable to unlawful processing of personal information. They will have direct access to and receive support from line managers and the organization's governing body in carrying out their responsibilities.

15. POPIA Complaints procedure

Data subjects hold the right to lodge complaints if they believe their rights under POPIA have been violated. The organization treats all complaints with utmost seriousness and follows this procedure for addressing POPIA-related grievances:

- Complaints regarding POPIA must be submitted in writing to the organization. If necessary, the Information Officer will furnish the data subject with a "POPIA

Complaint Form." *Annexure B*

- If a complaint is received by someone other than the Information Officer, that individual will ensure that the complete details of the complaint reach the Information Officer within 1 working day.
- The Information Officer will acknowledge receipt of the complaint in writing within 2 working days.
- The Information Officer will carefully review the complaint and address the concerns of the complainant in a respectful manner, striving to resolve it fairly and in line with POPIA principles.
- Additionally, the Information Officer will determine whether the complaint pertains to an error or breach of confidentiality that may impact the organization's data subjects on a broader scale.
- If the Information Officer suspects unauthorized access or acquisition of personal information of data subjects, they will consult with the organization's governing body. Subsequently, affected data subjects and the Information Regulator will be notified of the breach.
- Within 7 working days of receiving the complaint, the Information Officer will respond to the complainant with a proposed solution. Should the complainant wish to escalate the matter, they may approach the organization's governing body. In all instances, the organization will provide explanations for any decisions made and communicate any expected deviations from specified timelines.
- The Information Officer's response to the data subject may include:
    - Suggested remedies for the complaint,
    - Dismissal of the complaint along with reasons for dismissal,
    - Apology (if applicable) and any disciplinary actions taken against involved employees.
- If the data subject remains dissatisfied with the Information Officer's proposed remedies, they retain the right to lodge a complaint with the Information Regulator.
- The Information Officer will periodically review the complaints process to assess its effectiveness and make improvements where necessary. Additionally, reasons for complaints will be examined to prevent future occurrences leading to POPIA-related grievances.

16. Conclusion

By using our products and services, you consent to the collection, use, and disclosure of your personal information as described in this Privacy Policy. We are committed to protecting your privacy and will handle your information with care and respect. Thank you for entrusting us with your financial needs.

ANNEXURE A : PERSONAL INFORMATION REQUEST FORM

PERSONAL INFORMATION REQUEST FORM

Please submit the completed form to the Information Officer:	
Name	
Contact Number	
Email Address:	

Please be aware that we may require you to provide proof of identification prior to processing your request. There may also be a reasonable charge for providing copies of the information requested.

A. Particulars of Data Subject	
Name & Surname	
Identity Number:	
Postal Address:	
Contact Number:	
Email Address:	

B. Request	
I request the organisation to:	
(a) Inform me whether it holds any of my personal information	☐
(b) Provide me with a record or description of my personal information	☐
(c) Correct or update my personal information	☐
(d) Destroy or delete a record of my personal information	☐

C. Instructions

D. Signature Page
Signature
Date

ANNEXURE B : POPIA COMPLAINT FORM

POPIA COMPLAINT FORM

We are committed to safeguarding your privacy and the confidentiality of your personal information and are bound by the Protection of Personal Information Act.

Please submit your complaint to the Information Officer:	
Name	
Contact Number	
Email Address:	

Where we are unable to resolve your complaint, to your satisfaction you have the right to complaint to the Information Regulator.

The Information Regulator: Ms Mmamoroke Mphelo

Physical Address: SALU Building, 316 Thabo Sehume Street, Pretoria

Email: inforreg@justice.gov.za

Website: http://www.justice.gov.za/inforeg/index.html

A. Particulars of Complainant	
Name & Surname	
Identity Number:	
Postal Address:	
Contact Number:	
Email Address:	
B. Details of Complaint	
C. Desired Outcome	
D. Signature Page	
Signature:	
Date	

ANNEXURE C: POPIA NOTICE AND CONSENT FORM

POPIA NOTICE AND CONSENT FORM

We understand that your personal information is important to you and that you may be apprehensive about disclosing it. Your privacy is just as important to us and we are committed to safeguarding and processing your information in a lawful manner.

We also want to make sure that you understand how and for what purpose we process your information. If for any reason you think that your information is not processed in a correct manner, or that your information is being used for a purpose other than that for what it was originally intended, you can contact our Information Officer.

You can request access to the information we hold about you at any time and if you think that we have outdated information, please request us to update or correct it.

Our Information Officer's Contact Details	
Name	
Contact Number	
Email Address:	

Purpose for Processing your Information
We collect, hold, use and disclose your personal information mainly to provide you with access to the services and products that we provide. We will only process your information for a purpose you would reasonably expect, including:

- Providing you with advice, products and services that suit your needs as requested
- To verify your identity and to conduct credit reference searches
- To issue, administer and manage your insurance policies
- To process insurance claims and to take recovery action
- To notify you of new products or developments that may be of interest to you
- To confirm, verify and update your details
- To comply with any legal and regulatory requirements

Some of your information that we hold may include, your first and last name, email address, a home, postal or other physical address, other contact information, your title, birth date, gender, occupation, qualifications, past employment, residency status, your investments, assets, liabilities, insurance, income, expenditure, family history, medical information and your banking details.

Consent to Disclose and Share your Information

We may need to share your information to provide advice, reports, analyses, products or services that you have requested.

Where we share your information, we will take all precautions to ensure that the third party will treat your information with the same level of protection as required by us. Your information may be hosted on servers managed by a third-party service provider, which may be located outside of South Africa.

I hereby authorise and consent to the organisation sharing my personal information with the following persons:
Name & Surname
Signature
Date

ANNEXURE D: EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE

EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE

- "Personal Information" (PI) shall mean the race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; the personal opinions, views or preferences of the person; 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; the views or opinions of another individual about the person whether the information is recorded electronically or otherwise.
- "POPIA" shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.
- The employer undertakes to process the PI of the employee only in accordance with the conditions of lawful processing as set out in terms of POPIA and in terms of the employer's relevant policy available to the employee on request and only to the extent that it is necessary to discharge its obligations and to perform its functions as an employer and within the framework of the employment relationship and as required by South African law.
- The employee acknowledges that the collection of his/her PI is both necessary and requisite as a legal obligation, which falls within the scope of execution of the legal functions and obligations of the employer. The employee therefore irrevocably and unconditionally agrees:
  - That he/she is notified of the purpose and reason for the collection and processing of his or her PI insofar as it relates to the employer's discharge of its obligations and to perform its functions as an employer.
  - That he/she consents and authorises the employer to undertake the collection, processing and further processing of the employee's PI by the employer for the purposes of securing and further facilitating the employee's employment with the employer.
  - Without derogating from the generality of the aforestated, the employee consents to the employer's collection and processing of PI pursuant to any of the employer's Internet, Email and Interception policies in place insofar as PI of the employee is contained in relevant electronic communications.
  - To make available to the employer all necessary PI required by the employer for the purpose of securing and further facilitating the employee's employment with the employer.
  - To absolve the employer from any liability in terms of POPIA for failing to obtain the employee's consent or to notify the employee of the reason for the processing of any of the employee's PI.
  - To the disclosure of his/her PI by the employer to any third party, where the employer has a legal or contractual duty to disclose such PI.
  - The employee further agrees to the disclosure of his/her PI for any reason enabling the employer to carry out or to comply with any business obligation the employer may have or to pursue a legitimate interest of the employer in order for the employer to perform its business on a day to day basis.
  - The employee authorises the employer to transfer his/her PI outside of the Republic of South Africa for any legitimate business purpose of the employer within the international community. The employer undertakes not to transfer or disclose his/her PI unless it is required for its legitimate business requirements and shall comply strictly with legislative stipulations in this regard.
- The employee acknowledges that during the course of the performance of his/her services, he/she may gain access to and become acquainted with the personal information of certain clients, suppliers and other employees. The employee will treat personal information as a confidential business asset and agrees to respect the privacy of clients, suppliers and other employees.
- To the extent that he/she is exposed to or insofar as PI of other employees or third parties are disclosed to him/her, the employee hereby agree to be bound by appropriate and legally binding confidentiality and non-usage obligations in relation to the PI of third parties or employees.
- Employees may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the organisation or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the employee or person to perform his or her duties on behalf of the employer.

ANNEXURE E: SLA CONFIDENTIALITY CLAUSE

SLA CONFIDENTIALITY CLAUSE

- "Personal Information" (PI) shall mean the race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; the personal opinions, views or preferences of the person; 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; the views or opinions of another individual about the person whether the information is recorded electronically or otherwise.
- "POPIA" shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.
- The parties acknowledge that for the purposes of this agreement that the parties may come into contact with, or have access to PI and other information that may be classified, or deemed as private or confidential and for which the other party is responsible. Such PI may also be deemed or considered as private and confidential as it relates to any third party who may be directly or indirectly associated with this agreement. Further, it is acknowledged and agreed by the parties that they have the necessary consent to share or disclose the PI and that the information may have value.
- The parties agree that they will at all times comply with POPIA's Regulations and Codes of Conduct and that it shall only collect, use and process PI it comes into contact with pursuant to this agreement in a lawful manner, and only to the extend required to execute the services, or to provide the goods and to perform their respective obligations in terms of this agreement.
- The parties agree that it shall put in place, and at all times maintain, appropriate physical, technological and contractual security measures to ensure the protection and confidentiality of PI that it, or its employees, its contractors or other authorised individuals comes into contact with pursuant to this agreement.
- Unless so required by law, the parties agree that it shall not disclose any PI as defined in POPIA to any third party without the prior written consent of the other party, and notwithstanding anything to the contrary contained herein, shall any party in no manner whatsoever transfer any PI out of the Republic of South Africa.

ANNEXURE F: INFORMATION OFFICER APPOINTMENT LETTER

INFORMATION OFFICER APPOINTMENT LETTER

I herewith and with immediate effect appoint you as the Information Officer as required by the Protection of Personal Information Act (Act 4 of 2013). This appointment may at any time be withdrawn or amended in writing.

You are entrusted with the following responsibilities:

- Taking steps to ensure the organisation's reasonable compliance with the provision of POPIA.
- Keeping the governing body updated about the organisation's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to POPIA.
- Continually analysing privacy regulations and aligning them with the organisation's personal information processing procedures. This will include reviewing the organisation's information protection procedures and related policies.
- Ensuring that POPIA Audits are scheduled and conducted on a regular basis.
- Ensuring that the organisation makes it convenient for data subjects who want to update their personal information or submit POPIA related complaints to the organisation, to do so. For instance, maintaining a "contact us" facility on the organisation's website.
- Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the organisation. This will include overseeing the amendment of the organisation's employment contracts and other service level agreements.
- Encouraging compliance with the conditions required for the lawful processing of personal information.
- Ensuring that employees and other persons acting on behalf of the organisation are fully aware of the risks associated with the processing of personal information and that they remain informed about the organisation's security controls.
- Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the organisation.
- Addressing employees' POPIA related questions.
- Addressing all POPIA related requests and complaints made by the organisation's data subjects.
- Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

I hereby accept the appointment as Information Officer
Name & Surname
Signature
Date