INVESTMENTS

PPS House, Boundary Terraces
1 Mariendahl Lane, Newlands, 7700
PO Box 44507, Claremont, 7735
Tel: 0860 468 777 | Fax: +27 (0) 21 680 3680
clientservices@ppsinvestments.co.za
www.pps.co.za/invest

PROFESSIONAL PROVIDENT SOCIETY RETIREMENT ANNUITY FUND

PRIVACY POLICY

Table of Contents

1. Introduction

The right to privacy and access of personal information is endorsed by the Protection of Personal Information Act 4 of 2013 (POPIA) and the Promotion of Access to Information Act 2 of 2000 (PAIA) as amended from time to time. A person's right to privacy entails having control over his/her personal information and being able to conduct his/her affairs free from unwanted intrusions. POPIA aims to promote the protection of privacy through guiding principles that are intended to be applied to the processing of personal information.

It is through the provision of retirement benefits to members of the Professional Provident Society Retirement Annuity Fund ('the Fund') that the Fund is involved in the collection, use and disclosure of certain aspects of personal information of prospective and existing members, employees and other stakeholders. Considering the importance of privacy, the Fund is committed to effectively managing personal information in accordance with POPIA and PAIA.

2. Purpose of this policy

The purpose of this Policy is to protect the Fund and its members by adhering to the protection of personal information which includes to :

- Give effect to the constitutional right to privacy by safeguarding personal information against breaches of confidentiality where personal information of data subjects is shared or disclosed inappropriately through for example data breaches and hacking;
- Prevent reputational damage and financial loss that the Fund may suffer following an adverse data breach incident; and
- Offer choice, where required; as all data subjects have the free will to choose how and for what purpose the Fund uses information relating to them during and after their contractual relationship.

This Policy demonstrates the Fund's commitment to protecting the privacy rights of data subjects by:

- Stating desired behaviour and directing compliance with the provisions of POPIA including best practice;
- Developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information;
- Creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of the Fund;

- By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officers in order to protect the interests of the Fund and data subjects;
- By raising awareness and providing guidance to employees and any other authorised individuals who process personal information when carrying out their duties or in terms of a scope of contract in order to ensure that they act confidently and consistently; and
- Cultivating a culture within the Fund that recognises privacy as a valuable human right.

3. Scope of this policy

This Policy is relevant to the Fund, specifically:

- The board of trustees, principal officer, deputy principal officer, and all other fund officials;
- The sponsor and its staff;
- Members of the Fund and their beneficiaries;
- Services providers to the Fund, such as the s13B administrators, external auditor, actuary, fidelity cover insurer, investment manager, tracing agents and external counsel that may be appointed for expert opinion.

POPIA does not apply in situations where the processing of personal information is concluded in the course of purely household or personal activities; or where the personal information has been de-identified (anonymised data).

4. Policy statement

The Fund is committed to protecting the data subjects' privacy and ensuring their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

5. Key definitions in this policy:

"**Biometrics**" means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprint, DNA analysis, retinal scanning and voice recognition;

"Child" means a person under the age of 18 years;

"**Consent**" means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;

"**Data subject**" means the natural or juristic person to whom personal information relates, such as an individual member, employee or an entity that provides the Fund with products or services;

"**De-identify**" in relation to personal information of a data subject, means to delete any information that—

a) identifies the data subject;

b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or can be linked by a reasonably foreseeable method to other information that identifies the data subject, and ''de-identified'' has a corresponding meaning;

"**Deputy Information Officer**" means the person to whom any power or duty conferred or imposed on an Information Officer in terms of POPIA has been delegated;

"**Filing system**" means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria;

"**Information Officer**" means the Principal Officer of the Fund. Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer;

"**Information Regulator**" means the Regulator established in terms of section 39 of POPIA;

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

"Processing" means any operation or activity or any set of operations, whether by automatic means or not, concerning personal information, including-

a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

b) dissemination by means of transmission, distribution or making available in any other form; or products and legal matters relating to those products; or

c) merging, linking, as well as restriction, degradation, erasure or destruction of information.

"**Person**" means a natural person or a juristic person;

"**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, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, wellbeing, 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 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.

"Private body" means-

a) natural person who carries on or has a carried on any trade, business or profession, but only in such capacity;
b) a partnership which carries on or has carried on any trade, business or profession;
c) any former or existing juristic person but excludes a public body.

"**Public body''** means-

a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or
b) any other functionary or institution when-
    (i) exercising a power or performing a duty in terms of the Constitution ; or
    (ii) exercising a public power or performing a public function in terms of any legislation.

"**Record**" means any recorded information-

a) regardless of form or medium, including any of the following;
   (i) writing of any material;
   (ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
   (iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
   (iv) book, map, plan, graph or drawing;
   (v) photograph, film, negative, tape or other device in which one or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced;
b) in the possession or under the control of a responsible party;
c) whether or not it was created by a responsible party and regardless of when it came into existence.

"**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.

"**Special personal information**" means personal information concerning -

a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or
b) the criminal behaviour of a data subject to the extent that such information relates to-
   (iii) the alleged commission by a data subject of any offence; or
   (iv) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

6. Principles

All employees and persons acting on behalf of the Fund will always be subject to, and act in accordance with, the following principles:

Principle 1: Accountability and open communication

The Fund upholds and maintains an approach of transparency of operational procedures that controls its collection and processing of personal information. The Fund is committed to complying with all applicable regulatory requirements related to the collection and processing of personal information. Reasonable

measures will be taken to ensure that data subjects are notified (are at all times aware) that their personal information is being collected (directly from the data subject or from an external source e.g. media). The Fund is responsible for ensuring that the data subjects are aware that-

- Their personal information is being collected; and
- The Fund is the responsible party collecting the personal information by providing the necessary details; including specific reasons for the collection of such information.

The Fund will establish and maintain a platform for data subjects who want to:

- Enquire whether the Fund holds related personal information; or
- Request the Fund to update or correct related personal information; or
- Make a complaint concerning the processing of personal information.

Principle 2: Processing limitation

The Fund will ensure that personal information under its control is processed:

- In a fair, lawful and non-excessive manner; and
- In a reasonable manner that does not infringe the privacy of the data subject.

The Fund will inform the data subject of the reasons for collecting his/ her or its personal information and obtain written consent, where required, prior to processing personal information.

Where applicable, the data subject will be informed of the possibility that their personal information will be shared with other entities acting on behalf of the Principal Fund and be provided with reasons for doing so.

Principle 3: Purpose specification

The Fund will process personal information only for specific, explicitly defined and legitimate reasons. Data subjects will be informed of these reasons when collecting or recording the data subject's personal information.

Principle 4: Further processing limitation

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose. Therefore, where the Fund seeks to process personal information it holds for

purpose other than the original purpose for which it was collected, and where this secondary purpose is not compatible with the original purpose, the Fund will first obtain consent from the data subject.

Principle 5: Information quality

The Fund undertakes to take reasonable steps to ensure that personal information collected is complete, up to date, accurate and not misleading. This means that it may be necessary to request data subjects from time to time to update their information and confirm that it is still relevant.
Where personal information is collected or received from third parties, the Fund will take reasonable steps to confirm that the information is correct by requesting the third party to confirm the accuracy of the information.

Principle 6: Security safeguards

The Fund undertakes to secure the integrity and confidentiality of personal information in its possession as personal information is at great risk of loss, breach of confidentiality, corruption, hacking or theft when it is accessed or used. The Fund will provide the necessary reasonable security of data and keep it in accordance with prescribed legislation.

The Fund will manage the security of its filing system to ensure that personal information is adequately protected and to this end, security controls will be appropriate to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction. The Fund will regularly review its security controls which will include regular testing of protocols and measures implemented to combat cyber-attacks on the Fund's IT network. All hardcopy and electronic records comprising of personal information will be securely stored and made accessible only to authorised persons.

The Fund's operators are required to enter into service level agreements with the Fund where both parties pledge their mutual understanding and commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

Principle 7: Processing of personal information

Personal Information will only be used for the purpose for which it was collected and agreed upon. This may include, but not limited to:

- Provide retirement products or services to members or their beneficiaries and to carry out the

transactions requested;

- Provide services to members and beneficiaries to carry out the services requested, to maintain and constantly improve the relationship;
- For underwriting purposes, where applicable;
- Assess and process claims;
- Conduct credit reference searches or verification, where necessary;
- Confirm, verify and update member and beneficiary details;
- For purposes of claims history;
- For the detection and prevention of fraud, crime, money laundering or any other misconduct;
- For market or customer satisfaction research;
- For audit and record keeping purposes;
- In connection with legal proceedings; and
- In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

Personal Information that is received via a third party for further processing, this further processing must be compatible with the purpose for which the data was initially collected.

Principle 8: Data subject participation

A data subject may request the correction or deletion of his, her or its personal information held by the Fund. They may contact the Fund for such requests.

7. Rights of data subjects

Where appropriate, the Fund will ensure that data subjects are made aware of the rights conferred upon them as data subjects. The Fund will ensure that it gives effect to the following rights:

7.1 The right to access personal information

The Fund recognises that a data subject has the right to establish whether the organisation holds personal information related to him or her, including the right to request access to that personal information.

In addition, data subjects have the right to:

- Request what personal information the Fund holds about them and why;
- Be informed on how to keep their personal information up to date.

Access to information requests can be made by email and the prescribed form, addressed to the Information Officer.

7.2 The right to have personal information corrected or deleted

A data subject has the right to request the correction or deletion of personal data that is inaccurate, incomplete, unnecessary, and excessive or where the Fund is no longer authorised to retain personal information.

7.3 The right to object to the processing of personal Information

The data subject has the right, on reasonable grounds to object to the processing of his, her or its personal information. In such circumstances, the Fund will give due consideration to the request and the requirements of POPIA. The Fund may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual recordkeeping requirements, also approve the destruction of the personal information.

7.4 The right to object to direct marketing

The data subject has the right to object to the processing of his, her or its personal information for purposes of direct marketing by means of unsolicited electronic communications.

7.5 The right to complain

The data subject has the right to submit a complaint to the Fund and to the South African Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his/her or its personal information.

7.6 The right to be informed

The data subject has the right to be notified that his, her or its personal information is being collected by the Fund where reasonable. Furthermore, the data subject has the right to be notified in any situation where the Fund has reasonable grounds to believe that the personal information of the data subject has been accessed by an unauthorised person.

8. Personal information of a child

The Fund undertakes to ensure that lawful processing of the personal information of a child takes place

where the child is under the age of 18 and such processing is limited to the extent that consent is given or authorised by the holder of parental responsibility over the child, or other competent person or where a lawful reason exists.

9. Special Personal Information

The Fund undertakes to maintain processes in place to:

- Identify special personal information held or requested, on information technology systems or other documents;
- Ensure that special personal information is processed only when:
    - the data subject has consented to the processing;
    - a competent person has consented to the personal information relating to a child;
    - processing is necessary for the establishment, exercise or defence of a right;
    - the information has deliberately been made public by the data subject; or
    - processing is necessary to comply with an obligation of international public interest.

10. Information officer

The Fund will appoint Information Officer/s and where necessary, Deputy Information Officer/s to assist the Information Officers. The Information Officers and their deputies are responsible for ensuring compliance with POPIA and PAIA which include attending to requests for personal information, related queries and complaints made to the Fund in accordance with the PPS Group Information and Privacy Standard by data subjects and the Information Regulator. Once appointed, the Information Officers will register with the South African Information Regulator established under POPIA.

11. Complaints procedure

Data subjects have the right to complain in the event where any of their rights in terms of POPIA have been infringed. The Fund takes all complaints in a serious light and will address all personal information/ privacy related complaints in accordance with its documented procedure.

12. Publication of the Privacy Policy

The Policy is published internally and will be made available to all members via the PPS website.

13. Accountabilities and responsibilities for compliance

The Board of Trustees of the Fund will continually be responsible for ensuring the safeguarding, protection and avoidance of any unauthorised disclosure or breach of personal information in the execution of their duties.

13.1 The Board of Trustees

Accountabilities

The Board is ultimately responsible for ensuring that the Fund meets its legal obligations in terms of POPIA, regulations, directives, supervisory requirements and internal policies and supporting standards relating to the protection of personal information.

Roles and responsibilities

- To approve and adopt this Policy;
- To promote a culture of personal information protection and compliance;
- Ensure that the risk of unlawful processing of personal information and data breaches are assessed and considered as part of the Fund's risk assessment and strategic plans; and
- Monitor management's reports on processing of personal information and data breach risks, policies, and control activities, which include obtaining assurance that the controls are effective. The Board should also establish mechanisms to ensure it is receiving accurate and timely information from the administrator, sponsor, external auditor, actuary, insurer, asset managers and other stakeholders regarding potential data breach occurrences.

13.2 Information Officers and Deputy Information Officers

Accountabilities

- Assists the Board in ensuring compliance with the conditions of lawful processing of personal information and data breach risk management across the Board in Fund; and
- Information Officers and Deputy Information Officers will be appointed according to the legal and regulatory requirements and will fulfil their regulatory obligations.

Roles and responsibilities

- Take steps to ensure the Fund's compliance with the provisions of POPIA;
- Review the Fund's information protection procedures and related policies;
- Ensure that privacy notices for internal and external purposes are developed and published;
- Ensure that the Fund makes it possible for data subjects to update their personal information or submit POPIA related complaints to the Fund;
- Address members and beneficiaries' POPIA related questions;
- Provide direction when appointed;
- Address all POPIA related requests and complaints made by data subjects;
- Oversee the awareness training of all individuals involved in the processing of personal information on behalf of the Fund;
- Liaising and working with the Information Regulator in relation to ongoing investigations, arising issues, reporting and any other related matter:;
- Review and recommend this Policy to the Board for review.
- Review reports on non-compliance with established policies and procedures and ensure that appropriate plans for corrective action are put in place.
- Obtain feedback on progress made against action plans and ensure delivery.
- Encourage compliance with conditions for the lawful processing of personal information.
- Ensure that personal information impact assessments are done to ensure that adequate measures and standards exist within the Fund ,
- Ensure that a PAIA and POPIA Standard is developed, implemented and maintained;
- Ensure that adequate IT and operational systems are in place and well-maintained to process requests for access to information.

POLICY ADOPTED BY THE BOARD OF TRUSTEES ON 22 JUNE 2021.