PPS Group
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.

In this PPS Group Privacy Policy (Policy), references to PPS includes, Professional Provident Society Holdings Trust (PPS Holdings Trust), PPS Insurance Company Limited and all its subsidiaries.

It is through the rendering or provision of financial services and other related services that PPS 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, PPS 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 PPS 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 PPS 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 PPS uses information relating to them during and after their contractual relationship.

This Policy demonstrates PPS' 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 PPS;
- 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 PPS 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 PPS that recognises privacy as a valuable human right.

3. Scope of this policy

This Policy is relevant to PPS specifically all:

- Branches, business units, divisions and subsidiaries within PPS;
- Employees, independent contractors and volunteers;
- Members;
- Clients; and
- Suppliers and any other persons acting on behalf of PPS.

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).
The Policy applies to the entities set out in Annexure A.

4. Policy statement

PPS 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 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 PPS 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;

"**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 head of a private body. 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;

"**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;

"**Head**" in relation to, a private body means-

a) in the case of a natural person, that natural person or any person duly authorised by that natural person;
b) in the case of a partnership, any partner of the partnership or any person duly authorised by the partnership;
c) in the case of a juristic person:
    (i) the chief executive officer or equivalent officer of the juristic person or any person duly authorised by that officer; or
    (ii) the person who is acting as such or any person duly authorised by such acting person;

"**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 e.g. a third party service provider that has contracted with PPS to shred documents containing personal information.

"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.

"**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.

"**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 or has a carried on any trade, business or profession, but only in such capacity;

b) a partnership which carries or has carried 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 in terms of the constitution; or
   (ii) exercising a public power or performing a public function in terms of any legislation.

"**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 PPS will always be subject to, and act in accordance with, the following principles:

Principle 1: Accountability and open communication

PPS upholds and maintains an approach of transparency of operational procedures that controls its collection and processing of personal information. PPS 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). PPS is responsible for ensuring that the data subjects are aware that-

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

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

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

Principle 2: Processing limitation

PPS 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.

PPS 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. Alternatively, where services or transactions are concluded over the phone or electronic video feed, PPS will maintain a voice recording of the stated purpose for collecting the personal information followed by the data subject's subsequent consent, where required.

Where applicable, the data subject will be informed of the possibility that their personal information will be shared with other entities within the PPS and be provided with reasons for doing so.

Principle 3: Purpose specification

PPS 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 PPS 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, PPS will first obtain consent from the data subject.

Principle 5: Information quality

PPS 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, PPS 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

PPS 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. PPS will provide the necessary reasonable security of data and keep it in accordance with prescribed legislation.

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

All employees' employment contracts contain contractual terms for the use and storage of employee information. Confidentiality clauses are included to reduce the risk of unauthorised disclosures of personal information for which PPS is responsible.

PPS' operators are required to enter into service level agreements with PPS 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 financial products or services to members and clients and to carry out the transactions requested;
- Provide financial services to members and clients to carry out the services requested, to maintain and constantly improve the relationship;
- For underwriting purposes;
- Assess and process claims;
- Conduct credit reference searches or verification;
- Confirm, verify and update members and client 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 PPS. The

process described in the PPS Group Information and Privacy Standard will be provided for data subjects who want to request the correction or deletion of their personal information.

7. Rights of data subjects

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

7.1 The right to access personal information

PPS 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 PPS 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 PPS 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 process of his, her or its personal information. In such circumstances, PPS will give due consideration to the request and the requirements of POPIA. PPS 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. Objecting to processing of personal information may in some instances lead to the cancellation of financial products.

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 PPS 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 PPS where reasonable. Furthermore, the data subject has the right to notified in any situation where PPS 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

PPS 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

PPS 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 officers

PPS will appoint Information Officers and where necessary, Deputy Information Officers 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 PPS 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. PPS 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 PPS Group Privacy Policy

The Policy is published internally and made available to all employees on the PPS intranet. The policy is

available to the public on written request to PPS through the website www.pps.co.za. Such written request can be in electronic form.

13. Accountabilities and responsibilities for compliance

All employees and management of PPS 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 PPS Boards

Accountabilities

The PPS Boards are ultimately responsible for ensuring that PPS meets its legal obligations in terms of POPIA, regulation, 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 PPS' 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 PPS Boards also should establish mechanisms to ensure it is receiving accurate and timely information from management, employees, internal and external auditors, and other stakeholders regarding potential data breach occurrences.

13.2 Risk Committee

"Risk Committee", for the purposes of this Policy includes the Audit & Risk Committee in respect of any relevant PPS subsidiary.

Accountabilities

Ensure the protection of personal information.

Roles and responsibilities

- Review this Policy and recommend its approval to the PPS Boards;
- Monitor compliance with the protection of personal information;
- Receive reports on unlawful processing of personal information and data breach activities; and
- Ensure that appropriate plans for corrective action are put in place following the detection or reporting

of unlawful processing of personal information and data breach activities.

13.3 Chief Executive Officer (CEO) of PPS

Accountabilities

Ensures the lawful processing of personal information. The CEO is accountable to the PPS Boards for the effective operation of compliance with POPIA.

Roles and responsibilities

- Appoints Information Officers and where relevant Deputy Information Officers;
- Ensure that there is liaison and co-operation with the Information Regulator in relation to investigations;
- Ensure that an overall compliance framework is developed, implemented and monitored for the protection of personal information;
- Ensure that adequate IT and operational systems are in place and well-maintained to protect and process requests for access to information; and
- Review reports on compliance status and deficiencies and ensure that corrective action is taken.

13.4 PPS Chief Information Officer

Accountabilities, roles and responsibilities

- Ensure that PPS ’s IT infrastructure, filing systems and any other devices used for processing of persona information meet acceptable standards;
- Ensure that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services;
- Ensure that servers containing personal information are sited in a secure location, with access security;
- Ensure that all electronically stored personal information is backed-up and tested regularly;
- Ensure that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious hacking attempts;
- Ensure that all personal information being transferred electronically is encrypted;
- Ensure that all servers and computers containing personal information are protected by relevant up to date security software;
- Arrange regular IT audits to ensure that security of PPS ’s hardware and software systems are functioning properly;
- Investigate and report to the Committee any suspected data breaches;
- Set and recommend any IT policies relating to how PPS collects, holds, shares, uses, discloses, destroys and processes personal information;

- Arrange regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons; and
- Establish a process for a proper due diligence review prior to contracting with operators or any other third party service providers to process personal information on behalf of PPS.

13.5 Information Protection Committees of PPS

Accountabilities

An Information Protection Committee (Committee) is established and will convene on an ad hoc basis as and when required or when any issues of non-compliance and data breach activity is reported or suspected or to discuss any compliance requirement or process.

Roles and responsibilities

- The Committee oversees the implementation of the Policy.
- The Committee has the primary responsibility for the investigation of all suspected data breaches and acts of non-compliance as defined in the Policy. The Committee will ensure that the investigation is performed by a skilled forensic expert in collaboration with the relevant business area.
- Within the scope of their investigation as set out above, members of the Committee will have:
    - Free and unrestricted access to all records, employees and premises, whether owned or rented; and
    - The authority to examine, copy, or remove all or any portion of the contents of files, desks, cabinets, and other PPS facilities without prior knowledge or consent of any individual who might use or have custody of any such items.
    - The Committee must receive a Report from the investigation expert which should address at least the following:
        - Details of the complaint received or data breach identified;
        - Details of the manner in which the investigation was conducted;
        - Summary of the evidence found and an assessment of the strength/validity of the evidence;
        - Details of any process or other relevant shortcomings identified during the investigations and proposed mitigating action; and
        - Proposal to the Committee on proposed action to be taken.

- The Committee should evaluate the Report and decide on the most appropriate course of action.
- If the investigation substantiates that a data breach has occurred or personal information has been compromised, the Committee will make an assessment, in terms of the PPS Information Security Incident Management Policy and relevant standards, and where relevant will notify the following persons:

    - The Information Regulator;
    - Appropriate designated personnel within PPS ; and

- Chairman of Risk Committee.

- Any documentation produced following the Committee's decisions, should be authorised by the Committee or its nominated delegate;
- Decisions to report, laying of criminal charges or referral of the investigation results to the appropriate law enforcement and/or regulatory authorities will be made by the Committee. The committee should at all times consider PPS' zero tolerance for data breaches in making their decision;
- The Committee will assist in the administration, revision, interpretation and application of this Policy;
- The Committee is required to ensure that losses or damages suffered by PPS as a result of all reported acts committed or omitted by an employee or any other person are recovered from such an employee or other person if he or she is found to be liable after due process has been followed. Such recoveries should be conducted in accordance with HR policy and after due consultation with HR, in conjunction with legal remedies as appropriate; and
- Ensure that the content of this Policy is communicated to all employees, and other relevant persons, and are part of appropriate training programmes of employees.

13.6 Information Officers and Deputy Information Officers

Accountabilities

- Assists the CEO and the PPS Boards in ensuring compliance with the conditions of lawful processing of personal information and data breach risk management across the PPS; 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 PPS' compliance with the provisions of POPIA;
- Review PPS' information protection procedures and related policies;
- Ensure that privacy notices for internal and external purposes are developed and published;
- Ensure that PPS makes it possible for data subjects to update their personal information or submit POPIA related complaint to PPS;
- Address employees' POPIA related questions;
- Provide direction when appointed;
- Address all POPIA related requests and complaints made by data subjects;
- Oversee the awareness training of employees and other individuals involved in the processing of personal information on behalf of PPS;
- Liaising and working with the Information Regulator in relation to ongoing investigations, arising issues, reporting and any other related matter, in consultation with Group Compliance or subsidiary company compliance department;
- Review and recommend this Policy to the Risk Committee 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 PPS ,
- 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.

13.7 Business Unit Management of PPS

Accountabilities, roles and responsibilities

- Ensure that compliance requirements of this policy are incorporated in business processes;
- Establish and maintain a protection of personal information compliance culture (tone at the top), in conjunction with the rest of management in the business unit. This includes promoting a culture of risk and control relating to protection of personal information by communicating the requirements set out in this Policy to employees, and tracking adherence with those requirements;
- Ensure that employees within the business unit are adequately trained on the requirements of this Policy;
- Ensure that regular, risk-based compliance monitoring is conducted;
- Report on any incidents to the compliance champion and Group Compliance or Subsidiary Compliance;
- Take action to address such incidents; and
- Confirm compliance with this policy when required.

13.8 Compliance and subsidiary companies Compliance Officers

Accountabilities, roles and responsibilities

- Oversee compliance across PPS;
- Set and recommend this Policy and the Privacy Standard for approval.
- Give guidance and advice to business on the legislative requirements;
- Evaluate effectiveness of procedures and controls adopted to accommodate any legislative changes;
- Accountable for statutory reporting requirements;
- Assist with implementing procedures for reporting compliance breaches;
- Develop systems for monitoring compliance;
- Conduct regular, risk-based compliance monitoring to ensure appropriate levels of compliance are maintained; including assessment of how PPS collects, holds, shares, uses, discloses, destroys and processes personal information;
- Keep a record of all monitoring conducted;
- Report to the risk committee, executive committee and applicable regulators;

- Ensure recommendations from the PPS Boards, risk committee, management and applicable regulators are attended to; and
- Liaise and work with the Information Regulator in relation to ongoing investigations, arising issues, reporting and any other related matter, in consultation with Information or Deputy Information Officers.

13.9 PPS Marketing

Accountabilities, roles and responsibilities

- Maintain the protection of personal information statements and disclaimers that are displayed on PPS' website, mobile applications, including those attached to communications such as emails and electronic newsletters;
- Keep record of processing and marketing consents received;
- Address any personal information protection queries from journalists or media outlets; and
- Ensure that marketing initiatives comply with POPIA.

13.10 Employees and other persons acting on behalf of PPS

Accountabilities, roles and responsibilities

- Comply with this Policy and supporting standards.

14. Policy administration

Target audience:

The PPS Boards, all PPS management and employees.

Approved and Issued by:

The PPS Insurance Board

Person responsible for Policy administration:

Leon du Plessis, Head of Legal & Compliance, PPS,
+27 11 644 4491

Version: 1.0

Valid from:

July 2021

Next update required:

July 2024 or when legislative changes require it.

15. Annexure A

PPS Group Entity Organogram