PPS GROUP

EXTERNAL PRIVACY STANDARD

Contents

1. Introduction

1.1 In this PPS Group External Privacy Standard (the Privacy Standard), references to PPS includes, Professional Provident Society Holdings Trust (PPS Holdings Trust), PPS Insurance Company Limited and all its subsidiaries. Any reference to "PPS" or "we" or "us" or "our" included in this document means any such entity. Any reference to "you" or "your" in this Privacy Standard will include related data subject persons with the necessary amendments. We respect the right to privacy and confidentiality of personal information we encounter in conducting our business.

PPS may change this Privacy Standard from time to time if the law or business practices require it.

The Protection of Personal Information Act, 4 of 2013 (POPIA) describes personal information as information that identifies and relates to you or other individuals (such as your dependents).

1.2 Who does this Standard apply to?

All persons external to PPS providing information to PPS, all persons external to PPS requesting and making use of information obtained by PPS by rightful consent and/or lawful processing.

2. Key definitions in this standard

"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, policyholder 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
c) 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;

"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
d) 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-

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

"**Public body**'' means-

- any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or
- any other functionary or institution when-
  - exercising a power or performing a duty in terms of the constitution in terms of the constitution; or

- exercising a public power or performing a public function in terms of any legislation.

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

- 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
- the criminal behaviour of a data subject to the extent that such information relates to-
  - the alleged commission by a data subject of any offence; or
  - any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

Our aim is to handle personal information responsibly, balancing the benefits of activities such as fulfilment of the contractual relationship, research, data analytics with our other commitments, including reliability, transparency and non-discrimination. This Privacy Standard describes how we handle personal information that we collect through:

- The PPS website, the software applications made available by us for use on or through computers, mobile devices or other Internet-connected devices (the Apps), our social media pages; and
- Other means (for example, from your application and claim forms, telephone calls, e-mails and other communications with us, as well as from claim investigators, medical professionals, witnesses or other third parties involved in our business dealings with you).

3. Personal information that we collect

3.1 General identification and contact information

This includes but is not limited to:

- your name;
- address;
- e-mail and telephone details;
- gender;
- marital status;
- family status;
- date of birth;
- passwords;
- educational background;
- physical attributes;
- activity records, such as driving records;
- photos;
- employment history, skills and experience;
- professional licenses and affiliations;
- relationship to the policyholder, insured or claimant; and date and cause of death, injury or disability.

3.2 Medical and health information

This includes but is not limited to:

- your current or former physical or mental or medical condition;
- health status;
- injury or disability information;
- medical procedures performed;
- personal habits (for example, smoking or consumption of alcohol);
- prescription information; and medical history.

3.3 Financial information and account details

This includes but is not limited to:

- your payment card number;
- bank account number and account details;
- credit history and credit score;
- assets;
- income; and
- other financial information.

3.4 Identification numbers issued by government bodies or agencies

This includes but is not limited to:

- Identity number;
- passport number;
- tax number; or
- driver's or another license number.

3.5 Telephone recordings

This includes but is not limited to recordings of telephone calls to our representatives and call centres.

3.6 Information to investigate crime, including fraud and money laundering

Financial Service Providers may share information about their previous dealings with clients and claimants for this purpose.

3.7 Information enabling us to provide financial products and services

This includes but is not limited to:

- location and identification of property insured (for example, property address, vehicle license plate or identification number);
- travel plans;
- age categories of individuals you wish to insure;
- policy and claim numbers; coverage/peril details;
- cause of loss;
- prior accident or loss history;
- your status as director or partner, or other ownership or management interest in an organisation; and
- other insurance you hold.

3.8 Other sensitive information

In certain cases, we may receive sensitive information about your trade union membership, religious beliefs, political opinions, family medical history or genetic information. In addition, we may obtain information about your criminal record or civil litigation history in the process of preventing, detecting and investigating fraud. We may also obtain sensitive information if you voluntarily provide it to us (for example, if you express preferences regarding medical treatment based on your religious beliefs).

3.9 Marketing preferences and customer feedback

You may let us know of your marketing preferences, enter a contest or prize draw or other sales promotion or respond to a voluntary customer satisfaction survey.

3.10 Information concerning race or ethnic origin

Race and ethnic origin information will be processed if such information is needed to identify data subjects and only when this is essential for that purpose; or to comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

4. Sources from which personal information will be collected

We will endeavour to collect personal information directly from you, for lawful processing relating to our business or possible employment. Should this not be feasible, we will then collect such personal information if the following circumstances apply:

- You have consented thereto;
- A person legally authorised by you, the law or a court, has consented thereto;
- It is necessary to conclude or perform under a contract we have with you;
- The law requires or permits it;
- It is required to protect or pursue your, our or a third party's legitimate interest; and/or
- You are a child, and a competent person (such as a parent or guardian) has consented thereto on your behalf.

We will also collect personal information from other sources as indicated under Annexures A and B, respectively.

5. Notification to data subject when collecting personal information

During collection of your personal information, we will take reasonably practicable steps to ensure that you are aware of-

- the information being collected and where the information is not collected from you, the source from which it is collected;
- the name and address of the responsible party/ies;
- the purpose for which the information is being collected;
- whether or not the supply of the information by you is voluntary or mandatory;
- the consequences of failure to provide the information;

- any particular law authorising or requiring the collection of the information;
- the fact that, where applicable, the responsible party intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation.

6. When will we process your special personal information?

We may process your special personal information in the following circumstances:

- If you have consented to the processing;
- If the processing is needed to create, use or protect a right or obligation in law;
- If the processing is for statistical or research purposes, and all legal conditions are met;
- If the special personal information was made public by you;
- If the processing is required by law;
- If racial information is processed and the processing is required to identify you; and/or
- If health information is processed, and the processing is to determine your insurance risk, or to comply with an insurance policy, or to enforce an insurance right or obligation.

7. When and how we will process the personal information of children

A child is a person who is defined as a child by a country's legislation, and who has not been recognised as an adult by the courts, in South Africa it is a person under 18 years. We process the personal information of children if the law permits this. We will only process the personal information of children if any one or more of the following applies:

- A person with the ability to sign legal agreements has consented to the processing, being the parent or guardian of the child;
- The processing is needed to create, use or protect a right or obligation in law, such as where the child is an heir in a will, a beneficiary of a trust, a beneficiary of an insurance policy or an insured person in terms of an insurance policy;
- The child's personal information was made public by the child, with the consent of a person who can sign legal agreements;
- The processing is for statistical or research purposes and all legal conditions are met;
- Where the child is an heir in a will, if required to give effect to the will;
- Where the child is a beneficiary of a trust, if required to give effect to the trust deed;
- Where the child is legally old enough to sign a document as a witness without the assistance from their parent or guardian;
- Where the child benefits from a bank account such as an investment or savings account; and/or
- Where the child is an insured person or beneficiary of an insurance policy, if required to give effect to the policy.

8. How we process information about persons related to a juristic person

If you are a juristic person, such as a company or close corporation, we may collect and use personal information relating to the juristic person's directors, officers, employees, beneficial owners, partners, shareholders, members, authorised signatories, representatives, agents, payers, payees, customers, guarantors, spouses of guarantors, sureties, spouses of sureties, other security providers and other persons related to the juristic person. These are related persons.

If you provide the personal information of a related person to us, you warrant that the related person is aware that you are sharing their personal information with us, and that the related person has consented thereto. We will process the personal information of related persons as stated in this Privacy Standard.

9. Personal information of other individuals

If you provide personal information to PPS regarding other individuals, you agree to:

- Inform the individual about the content of this Privacy Standard; and
- Obtain any legally required consent for the collection, use, disclosure, and transfer (including cross-border transfer) of personal information about the individual in accordance with this Privacy Standard.

10. Reasons we need to process your personal information

Personal Information may be obtained to, reasons listed below is not exhaustive:

- Assess our insurance risks;
- Enable us to deliver goods, documents or notices to you;
- Carry out your instructions and requests;
- Conclude or perform in terms of a contract, or for the implementation of pre-contractual measures requested by you;
- Communicate with you and others as part of our business;
- Send you important information regarding changes to our policies, other terms and conditions, the website and other administrative information.
- Open, manage and maintain your membership or relationship with us;
- To disclose and obtain personal information from credit bureaux regarding your credit history;
- Make decisions about whether to provide insurance; provide insurance and assistance services, including claim assessment, processing and settlement; and, where applicable, manage claim disputes;
- For insurance underwriting and administration;
- For customer satisfaction feedback;
- Assess your eligibility for membership and process your premium and other payments;
- Provide improved quality, training and security (for example, with respect to recorded or monitored phone calls to our contact numbers);
- Prevent, detect, investigate and report crime, including fraud, financing of terrorism and money laundering, and analyse and manage other commercial risks.

This may include the processing of special personal information, such as alleged criminal behaviour or the supply of false, misleading or dishonest information when obtaining financial services/ products with us, or avoiding liability by way of deception;

- Enforce and collect on any agreement when you are in default or breach of the terms and conditions of the agreement, such as tracing you; or to institute legal proceedings against you;
- Develop, test and improve our products and services for you;
- Carry out market research and analysis, including satisfaction surveys;
- Provide marketing information to you (including information about other products and services offered by selected third-party partners) in accordance with preferences you have expressed;
- Personalise your experience on online platforms by presenting information and advertisements tailored for you;
- Identify you to anyone to whom you send messages through the PPS website and Apps;
- Allow you to participate in contests, prize draws, competitions and similar promotions, and to administer these activities. Some of these activities have additional terms and conditions, which could contain additional information about how we use and disclose your Personal Information, as a result, we suggest that you read these carefully;
- Manage our infrastructure and business operations, and comply with internal policies and procedures, including those relating to auditing; finance and accounting; billing and collections; IT systems; data and website hosting; business continuity; and records, document and print management;
- Process payment instruments (such as a cheque) and payment instructions (such as a debit order);
- Resolve complaints, and handle requests for data access or correction;
- Fulfil reporting requirements and information requests;
- Comply with applicable laws and regulatory obligations (including laws**,** directives, sanctions and rules outside your country of residence), such as those relating to anti-money laundering and anti-terrorism; comply with legal process; and respond to requests from public and governmental authorities (including those outside your country of residence);
- Establish and defend legal rights; protect our operations or those of any of our group companies or insurance business partners and associates; our rights, privacy, safety or property, and/or that of PPS, you or others; and pursue available remedies or limit our damages;
- For security and identity verification, and to check the accuracy of your personal information;
- For any related purposes.

11. Marketing preferences

We may use your personal information to market financial, insurance, investments and other related PPS products and services to you. We may do this in person, by post, telephone, or electronic channels such as SMS and email. We will provide you with

regular opportunities to tell us your marketing preferences, including in our communications to you. You can also contact us by e-mail at memberservices@pps.co.za to tell us your marketing preferences and to opt-out.

If you no longer want to receive marketing-related communications from PPS going-forward, you may opt-out of receiving these marketing-related communications at any time.

We aim to comply with your opt-out request(s) within a reasonable time period. Please note that if you opt-out as described above, we will not be able to immediately remove your personal information from the databases of third parties with whom we have already shared your personal information (e.g. those to whom we have already provided your personal information as of the date on which we respond to your opt-out request). Please also note that if you do opt-out of receiving marketing communications from us, we may still send you other important administrative communications from which you cannot opt-out.

If you are not our member and/or policyholder, or in any other instances where the law requires, we will only market to you by electronic communications with your consent.

12. Security

We will take appropriate and reasonable technical, physical, legal and organisational measures, which are consistent with applicable privacy and data security laws. This includes the following:

- Keeping our systems secure (such as monitoring access and usage);
- Storing our records securely;
- Controlling the access to our buildings, systems and/or records; and
- Safely destroying or deleting records.

Unfortunately, no data transmission over the Internet or data storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of any personal information you might have with us has been compromised), please immediately notify us at memberservices@pps.co.za or call us directly on telephone 0860 123 777.

When we provide personal information to a service provider, the service provider will be selected carefully and required to use appropriate measures to protect the confidentiality and security of the Personal Information.

13. International (cross border) transfer of personal information

Due to the presence of our business activities in other countries, for the purposes set out above we may transfer Personal Information to parties located in Namibia and Australia and other countries that have a different data protection regime than is found in the country where you are based. For example, we may transfer Personal Information in order to assist you in obtaining comprehensive financial planning. We may transfer information

internationally to our group companies, service providers, business partners and governmental or public authorities. The transfer will be relevant and not excessive.

During any such international transfer of your personal information, we will take reasonably practical steps to ensure that you are aware of our intention to transfer the information to a third party country, including the level of protection afforded to the information by that third country or international organisation.

14. Retention of personal information

We take reasonable steps to ensure that the personal information we process is reliable for its intended use, and as accurate and complete as is necessary to carry out the purposes described in this Privacy Standard. We will retain personal information for the period necessary to fulfil the purposes outlined in this Privacy Standard unless a longer retention period is required or permitted by other applicable law. We will keep your personal information for as long as:

- The law requires us to keep it;
- A contract between you and PPS requires us to keep it;
- You have consented to us keeping it;
- We are required to keep it to achieve the purposes listed in this Privacy Standard;
- We require it for statistical or research purposes, we will then de-identify the personal information where necessary; and/or
- We require it for our lawful business purposes.

TAKE NOTE: We may keep your personal information even if you no longer have a relationship with us, if the law permits.

15. Your duties and rights regarding the personal information we have about you

You must provide proof of identity when enforcing the rights below. You must inform us when your personal information changes.

Refer to PPS Group PAIA Standard (PAIA Standard) in terms of the Promotion of Access to Information Act 2 of 2000 (PAIA) and this Standard for further information on how you can give effect to the rights listed below. The PAIA Standard is located on the PPS website www.pps.co.za.

You have the right to request access to the personal information we have about you by contacting us. This includes requesting:

- Confirmation that we hold your personal information;
- A copy or description of the record containing your personal information; and
- The identity or categories of third parties who have had access to your personal information.

We will attend to requests for access to personal information within a reasonable time. You may be required to pay a reasonable fee to receive copies or descriptions of records,

or information about, third parties. We will inform you of the fee, if applicable, before attending to your request.

Please note that the law may limit your right to access information. You have the right to request us to correct or delete the personal information we have about you if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, obtained unlawfully, or if we are no longer authorised to keep it, under certain circumstances. You must inform us of your request in writing, and complete the attached Form 2.

Please refer to our PAIA and POPIA Standards for further information in this regard, such as the process you should follow to give effect to this right. It may take up to 30 business days for the change to reflect on our systems. We may request documents from you to verify the change in personal information.

A specific agreement that you have entered into with us may determine how you must change your personal information provided at the time when you entered into the specific agreement. Please adhere to these requirements.

If the law requires us to keep the personal information, it will not be deleted upon your request. The deletion of certain personal information may lead to the termination of your business relationship with us.

You may object on reasonable grounds to the processing of your personal information. We will not be able to give effect to your objection if the processing of your personal information was and is permitted by law, you have provided consent to the processing, and our processing was conducted in line with your consent; or the processing is necessary to conclude or perform under a contract with you. For any objection to the processing of personal information, complete the attached Form 1.

You must inform us of any objection in writing. Please refer to our PAIA and POPIA Standard for further information in this regard, such as the process you should follow to give effect to this right.

Where you have provided your consent for the processing of your personal information, you may withdraw your consent. If you withdraw your consent, we will explain the consequences to you. We may proceed to process your personal information, even if you have withdrawn your consent, if the law permits or requires it. It may take up to 30 business days for the change to reflect on our systems. During this time, we may still process your personal information. The withdrawal of your consent may lead to the termination of your business relationship with us.

You have a right to file a complaint with us or the Information Regulator by email at POPIAComplaints@inforegulator.org.za and PAIAComplaints@inforegulator.org.za about an alleged interference with the protection of your personal information. We request that you address your compliant to us first at privacy@pps.co.za to provide us with an opportunity to respond to you, prior to you approaching the Information Regulator.

16. Complaints procedure

You have the right to complain in the event where any of your 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 the following procedure:

- Where the complaint has been received by any person other than Information Officer and/or the Deputy Information Officer, that person shall ensure that full details of the complaint reach the Information Officer or Deputy Information Officer as soon as possible;
- You will receive a written acknowledgement of receipt;
- The Information Officer and/or the Deputy Information Officer will carefully consider the complaint and address the complaint's concerns in an amicable manner and in accordance with the principles of POPIA;
- The Information Officer and/or the Deputy Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred, and which may have a wider impact on the data subjects of PPS;
- Where the Information Officer and/or the Deputy Information Officer has reason to believe that your personal information has been accessed or acquired by an unauthorised person, the Information Protection Committee must be consulted and the affected data subjects and the Information Regulator must be informed of the breach;
- The Information Officer and/or the Deputy Information Officer will revert to you with a proposed solution with the option of escalating the complaint to the Information Protection Committee within 7 working days upon receipt of the complaint. In all instances, PPS will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines;
- A response to you may comprise any of the following:
    - A recommendation or remedy for the complaint;
    - A dismissal of the complaint with reasons as to why it was dismissed; or
    - An apology (if applicable) with appropriate action against any persons involved.
- Where you are not satisfied with the outcome or handling of the complaint, you have the right to complain to the Information Regulator; and
- The Information Officer and/or the Deputy Information Officer will regularly review the complaints process and procedure to assess its effectiveness. A root cause analysis of the complaints will be done to avoid reoccurrences that give rise to POPIA related complaints.

Complaints will be handled in line with the PPS Group Complaints Management Standard and Policy, read with the PPS Group Personal Information Breaches Management Standard.

Complaints referred to the Information Regulator, are dealt with as follows:

On receiving a complaint, the Information Regulator may-

- conduct a pre-investigation;
- act, at any time during the investigation and where appropriate, as conciliator in relation to any interference with the protection of your personal information;
- decide to take no action on the complaint or, as the case may be, require no further action in respect of the complaint;
- conduct a full investigation of the complaint;
- refer the complaint to the Enforcement Committee; or
- take such further action.

17. Minimality

Personal information will only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.

18. Who to contact about your personal information?

Access to information requests can be made by email and in the prescribed form, addressed to the Information Officer. Once the request is received, the Information Officer and/or the Deputy Information Officer will verify the identity of the data subject prior to handing out /disclosing any personal information. All requests will be processed and considered against the PAIA Standard. The Information Officer and/or the Deputy Information Officer will process all requests within a reasonable time.

If you have any queries about our use of your Personal Information you can e-mail: memberservices@pps.co.za or privacy@pps.co.za and/or refer to the PAIA Standard on the PPS website for further information regarding requests for personal information and related complaints.

19. Information Officers and Deputy Information Officers

Information Officers and Deputy Information Officers in PPS are appointed according to the legal and regulatory requirements and will fulfil their regulatory obligations to protect personal information in PPS.

An Information Officer is the custodian of any activity relating to the processing of personal information and if any of the provisions of POPIA is breached, he or she could ultimately be held liable for that transgression. For accountabilities, roles and responsibilities of the Information Officer and his/ her Deputy, kindly refer to the PPS Group Privacy Policy.

20. Information Protection Committees of PPS

An Information Protection Committee is established and will convene on an ad hoc basis as required or when any issues of non-compliance and personal information breach activity is reported or suspected.

The Committee consists of the following individuals:

- Information Officer;
- Deputy Information Officer(s);
- Relevant IT executive;
- Executive: Human Resources or equivalent role for subsidiaries as applicable or his/her representative;
- Head of Group Legal and Compliance or equivalent role for subsidiaries, as applicable;
- Relevant Investigator; and
- Relevant manager /team leader.

A summary of Other Information is included in this External Privacy Standard as Annexure A below.

21. Standard Administration

Approved and Issued by:

PPS Group Executive Committee

Person responsible for the Standard Administration
Leon Du Plessis, Group Executive: Legal and Compliance
+27 11 644 4491

Valid from: July 2021

Next update required: September 2023

Annexure A: Other information we collect

We and our third-party service providers may collect Other Information in a variety of ways, including:

- **Through your internet browser:** Certain information is collected by most websites, such as your IP address (i.e., your computer's address on the internet), screen resolution, operating system type (Windows or Mac) and version, internet browser type and version, time of the visit and the page(s) visited. We use this information for purposes such as calculating PPS website usage levels, helping diagnose server problems, and administering the website.

- **Using cookies**: Cookies are pieces of information stored directly on the computer you are using. Cookies allow us to recognise your computer and to collect information such as internet browser type, time spent on the website, pages visited, language preferences, etc. We may use the information for security purposes, to facilitate navigation, to display information more effectively, to personalise your experience while visiting the website, or to gather statistical information about the usage of the Site. Cookies further allow us to present to you the advertisements or offers that are most likely to appeal to you. We may also use cookies to track your responses to our advertisements and we may use cookies or other files to track your use of other websites.

  You can refuse to accept other cookies we use by adjusting your browser settings. However, if you do not accept these cookies, you may experience some inconvenience in your use of the website and some online financial products/services.

- **Using pixel tags, web beacons, clear GIFs or other similar technologies:** These may be used in connection with some website pages and HTML-formatted e-mail messages to, among other things, track the actions of website users and e-mail recipients, measure the success of our marketing campaigns and compile statistics about website usage and response rates.

- **From you**: Some information (for example, your location or preferred means of communication) is collected when you voluntarily provide it. Unless combined with personal information, this information does not personally identify you.

- **By aggregating information**: We may aggregate and use certain information (for example, we may aggregate information to calculate the percentage of our users who are in a certain area).

Annexure B: Collecting and sharing of personal information about you

PPS may collect and share Personal Information available to PPS. Access to personal information within PPS is restricted to those individuals who have a need to access the information for our business purposes.

- **Other insurance and distribution parties**
  In the course of marketing and providing insurance, and processing claims, PPS may collect and make personal information available to third parties such as other insurers; reinsurers; insurance and reinsurance brokers and other intermediaries and agents; appointed representatives; distributors; affinity marketing partners; and financial institutions, securities firms and other business partners.

- **Our service providers**

  External third-party service providers, such as medical professionals, accountants, auditors, actuaries, lawyers and other outside professional advisors, travel and medical assistance providers; call centre service providers; IT Systems, support and hosting service providers; printing, advertising, marketing and market research and analysis service providers; banks and financial institutions that service our accounts; third party claim administrators; document and records management providers; claim investigators and adjusters; construction consultants; engineers; examiners; consultants; translators; and similar third-party vendors and outsourced service providers that assist us in carrying out business activities.

- **Governmental authorities and third parties involved in court action**
  PPS may also collect and share Personal Information with governmental or other public authorities (including, but not limited to, workers' compensation boards, courts, law enforcement, tax authorities and criminal investigations agencies); and third-party civil legal process participants and their accountants, auditors, lawyers and other advisors and representatives as we believe to be necessary or appropriate:

  (a) To comply with applicable law, including laws outside your country of residence;

  (b) To comply with legal process;

  (c) To respond to requests from public and government authorities including public and government authorities outside your country of residence;

  (d) To enforce our terms and conditions;

  (e) To protect our operations or those of any of our companies;

  (f) To protect our rights, privacy, safety or property, and/or that of our companies, you or others; and

  (g) To allow us to pursue available remedies or limit our damages.

- **Other third parties**

  We may collect and share your Personal Information with payees; emergency providers (fire, police and medical emergency services); retailers; medical networks, attorneys, tracing agents, debt collectors and other persons that assist with the enforcement of agreements; organisations and providers; travel carriers; credit bureaus; credit reporting agencies; and other people involved in an incident that is the subject of a claim; as well as purchasers and prospective purchasers or other parties in any actual or proposed reorganisation, merger, sale, joint venture, assignment, transfer or other transaction relating to all or any portion of our business, assets or stock.

  To check information provided, and to detect and prevent fraudulent claims, Personal Information (including details of injuries) may be put on registers of claims and shared with other insurers. We may search these registers when dealing with claims to detect, prevent and investigate fraud. Information may also be shared with industry associations e.g. ASISA.

  Your spouse, dependants, partners, employer, joint applicant or account holder and other similar sources. People you have authorised to share your personal information, such as a person that makes a travel booking on your behalf, or a medical practitioner for insurance purposes.

  If the law requires us to do so, we will ask for your consent before collecting personal information about you from third parties.

- **You**

  We collect information about you:

  - Directly from you;
  - Based on how you engage or interact with us, such as on social media, and through e-mails, letters, telephone calls, and surveys;
  - Based on your use of our products, services, or service channels (such as our websites and applications);

  Personal Information may also be shared by you, on message boards, social media and blogs, and other services to which you are able to post information and materials. Please note that any information you post or disclose through these services will become public information; and may be available to visitors on the website and to the general public. We urge you to be very careful when deciding to disclose your Personal Information, or any other information, on online platforms.

FORM 1

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2017

[Regulation 2(1)]

Note:

1. *Affidavits or other documentary evidence in support of the objection must be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*

Reference Number….

A	**DETAILS OF DATA SUBJECT**
Name and surname of data subject:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number:	
E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name and surname of responsible party *(if the responsible party is a natural)*:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number:	
E-mail address:	

Name of public or private body *(if the responsible party is not a natural person)*:	
Business address:	
	Code ( )
Contact number(s):	
Fax number:	
E-mail address:	

C	**REASONS FOR OBJECTION** *(Please provide detailed reasons for the objection)*

Signed at ..... this ..... day of .....20……...

.....
Signature of data subject (applicant)

FORM 2

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2017

[Regulation 3(2)]

Note:

1. *Affidavits or other documentary evidence in support of the request must be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*

Reference Number….

Mark the appropriate box with an "x".

Request for:

☐ Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.

☐ Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A	**DETAILS OF THE DATA SUBJECT**
Surname:	
Full names:	
Identity number:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number:	
E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name and surname of responsible party*(if the responsible party is a natural person)*:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number:	
E-mail address:	

Name of public or private body *(if the responsible party is not a natural person)*:	
Business address:	
	Code ( )
Contact number(s):	
Fax number:	
E-mail address:	

C	REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT/*DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY. *(Please provide detailed reasons for the request)*

* *Delete whichever is not applicable*

Signed at ..... this ..... day of .....20……...

.....

Signature of Data subject