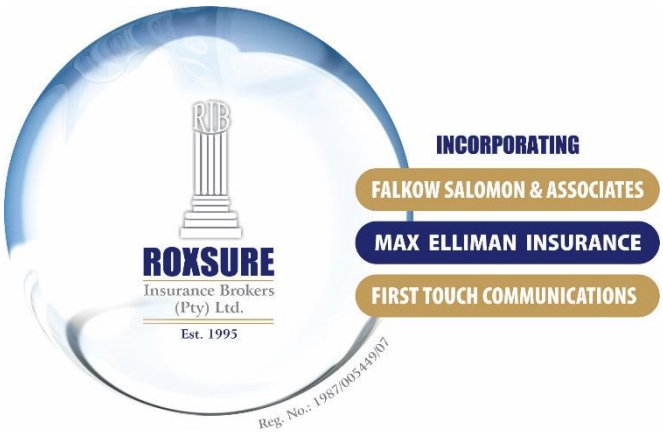

Protection of Personal Information Act ("POPI") & Data Management Policy

Purpose	Personal Information as defined by POPI may be required by the Company to provide a customer or prospective customer with financial services. The purpose of this Policy is to ensure that such Personal Information is protected so that the Company's customers do not suffer any prejudice as a result of this information ending up in the wrong hands. This policy describes how this personal data must be collected, handled and stored to meet the Company's data protection standards – and comply with the law.
Audience	This document is a guide to the Board of Directors, Management, staff, Business Partners who handle Personal Information ("Operators'), and any entity that processes Personal Information on behalf of the Company to ensure awareness of data protection issues, risks and responsibilities.
Prescribed forms	1. Form 1 – Objection to the processing of personal information 2. Form 2 – Request for correction/deletion of personal information/destruction/deletion of record of personal information 3. Form 3 – Application for Issuing code of conduct 4. Form4 – Request for data subject's consent to process personal information (Direct marketing) 5. Form 5 – Submission of complaint 6. Form 6 – Regulator acting as conciliator during investigation 7. Form 7 – Conciliation certificate 8. Form 8 – Pre-investigation proceeding of Regulator 9. Form 9 – Settlement of complaints 10. Form 10 – Settlement certificate 11. Form 11 – Assessments 12. Form 12 – Regulator to notify of decision made/action taken 13. Form 13 – Informing parties -enforcement notice will not be issued 14. Form 14 – Informing parties – complaint referred to the enforcement Committee 15. Form 15 – Informing parties – enforcement notice has been served 16. Form 16 – Informing parties – enforcement notice has been cancelled/varied 17. Form 17 – Informing parties – an appeal has been lodged against enforcement notice 18. Form 18 – Informing parties – an appeal against enforcement notices has been allowed 19. Form 19 – Informing parties – appeal has been dismissed
Version History	01/07/2021 (Unchanged – reviewed) 31/03/2021 09/10/2020 01/07/2020 (Unchanged – reviewed) 20/05/2020 01/01/2020 01/07/2019 (Unchanged – reviewed) 01/07/2018 (Unchanged – reviewed) 05/08/2016 20/06/2016

1. **Definitions – POPI**

Act	means the Protection of Personal Information Act, 2014;
Data	means all information stored relating to the Company business, its customers and policies that is not personal information;
Data Subjects	means any person to whom personal information relates
De-identify	means to delete any information that: 1. identifies the data subject; 2. can be used or manipulated by a reasonably foreseeable method to identify the data subject; or 3. can be linked by a reasonably foreseeable method to other information that identifies the data subject;
Legitimate Purpose	means any act which is necessary in order to negotiate, conclude, maintain and administer the insurance policy in favour of the insured, including but not limited to acts such as the settling of claims, even after termination of the policy. The legitimate purpose further extends to the processing of personal information for audit, storage and back up purposes and the storage of personal information beyond expiry of the insurance contract for a period of 5 years, in order to meet Company obligations in terms of Financial Advisory and Intermediary Services Act ("FAIS") and to address potential litigation disputes;
Operator	means any person or organisation who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party, and includes all business partners;
Process	means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including: 1. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; 2. dissemination by means of transmission, distribution or making available in any other form including written and printed; or 3. merging, linking, as well as blocking, degradation, erasure or destruction of information;
Personal Information	means any information relating to an identifiable, living natural person or juristic person (companies, CC's etc.) and includes, but is not limited to: 1. Contact details: email, telephone, address etc.; 2. Identity number, asset information and company registration numbers 3. Demographic information: age, sex, race, birth date, ethnicity etc.; 4. History: employment, financial, educational, criminal, medical history; 5. Biometric information: blood type etc.;

	6. Opinions of and about the person; and 7. Private correspondence etc.
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.

2. Policy

2.1. The Company relies on business partners ("operators") to record, store and access Personal Information relating to facility holders. IT system requirements, Data and Personal Information requirements are set out in the agreements concluded with all business partners and governed by the Company's BCM Governance Policies. These agreements are reviewed and checked by the Company on a regular basis and the Company considers regular Information Technology ("IT") Governance reports provided by its business partners.

2.2. The Company ensures that all Data and Personal Information is stored and accessed on IT systems, which guarantees confidentiality, integrity of data and authenticity of system information.

2.3. The Company's BCM governance policies, as well as its POPI policy are applied to all Personal Information relating to customers, business partners and facility holders, which is entered onto a record and filed, including all other Data, which is stored and kept by the Company, or on behalf of the Company. The Company shall secure the integrity and confidentiality of Personal Information in its possession or under its control by taking appropriate, reasonable, technical and organisational measures.

2.4. This policy exists to ensure that the Company:

2.4.1. Complies with data protection laws and follows good practice

2.4.2. Protects the rights of customers, staff and business partners

2.4.3. Is transparent about how it stores and processes data

2.4.4. Protects itself from the risks of a data breach

2.4.5. Has access, at all times, as and when required, to data that is up- to-date, accurate, reliable, secure and complete and includes data in intermediary systems.

3. Data

3.1. It is the Company's policy to ensure that all Data is handled in a secure manner, so as not to compromise integrity or confidentiality. The Company shall ensure, by reviewing reports of operators,

that Data is accurate and of a good quality. The Company shall use secure systems to ensure its own data is protected.

3.2. Operators that manage Company Data are responsible for all information related processes and must adhere to the Company's BCM Governance policies in respect of handling Company Data.

4. Personal Information

4.1. The Company is a Responsible Party in terms of POPI and processes Personal Information. The Company contracts with operators which may process Personal Information of customers. The purpose of all processing is solely related to non-life insurance policies underwritten by the Company and in accordance with the Legitimate Purpose as detailed in this Policy.

4.2. Personal Information may need to be further processed from time to time in order for the Responsible Party and operator to properly execute and manage the non-life insurance policy. Where the further processing of Personal Information is required other than for the Legitimate Purposes of the insurance policy, consent will be obtained from the Data Subject to which the Personal Information relates. Personal Information is not used for marketing, comparative or public purposes.

5. Legitimate Purpose

5.1. The Company shall:

5.1.1. Only collect Personal Information required for the following purposes:

5.1.1.1. Underwriting;

5.1.1.2. Assessing and processing claims;

5.1.1.3. Conducting credit reference searches or verification;

5.1.1.4. Confirming and verifying an individual's identity;

5.1.1.5. Confirming claims history; and

5.1.1.6. Detecting and preventing fraud, corruption and theft.

5.1.2. Only use Personal Information for what it is intended;

5.1.3. Only retain Personal Information as long as is necessary;

5.1.4. Apply adequate security measures to safeguard Personal Information;

5.1.5. Ensure that the customer's Personal Information is up to date;

5.1.6. Only hold as much information as is required for the aforementioned purposes; and

5.1.7. Destroy or de-identify Personal Information if it is no longer required, but subject to legislative provisions such as FAIS and the Financial Intelligence Centre Act ("FICA") that require the Company to keep records for specified periods of time.

6. Data Access and Sharing

6.1. Where the Company has outsourced the processing of any data, it must ensure that it has access to the data at any time and as and when required, and must also be able to interrogate information on all policy, claims, communication and complaints data (both current and historical data).

6.2. Where data is maintained by an outsourced party, it is the Company's duty to ensure that it is easily accessible within reasonable timelines.

6.3. The data that the Company collects and maintains, should be easy to understand, yet comprehensive enough to facilitate informed decisions and will adhere to the data standards and definitions as approved by FSCA.

7. Access to Personal Information

7.1. It is the Company's policy to make available all Personal Information to a Data Subject, where this is requested by the Data Subject in terms of the Company's Promotion of Access to Information Manual.

7.2. The Company shall ensure the following information is disclosed to a Data Subject:

7.2.1. Personal Information being collected;

7.2.2. details of the Responsible Party;

7.2.3. purpose for which the Personal Information is being collected;

7.2.4. whether the supply of Personal Information is mandatory or voluntary;

7.2.5. consequences of failure to provide the Personal Information;

7.2.6. any law authorising or requiring the collection of the Personal Information;

7.2.7. the existence of rights of access to and rectification of the Personal Information collected; and

7.2.8. any further information which is reasonably necessary to enable Processing.

8. Trans-border Personal Information Flows

8.1. The Company shall not transfer any Personal Information of a Data Subject to a third party that is situated in a foreign country, unless:

8.1.1. the recipient of the information is subject to a law or binding code of conduct or contract which upholds the principles for reasonable processing of the information, as according to POPI, this policy and the Company's BCM Governance Policies, and includes provisions which protects the further transfer of such information from the recipient to another third party in a foreign country; or

8.1.2. the Data Subject further consents to the transfer of information, which is relevant to the insurance policy; or

8.1.3. the transfer is necessary for the performance of a contract between the Data Subject and the Responsible Party or for implementation of pre-contractual measures in response to the Data Subjects request; or

8.1.4. the transfer is necessary for the performance of a contract in the interest of the Data Subject between a third party and the Responsible Party, the transfer is for the benefit of the Data Subject and it is not reasonably practical to obtain the consent of the Data Subject, who would likely consent if it were reasonably practical to obtain his or her consent.

9. Incident Management Strategy

9.1. The Company's incident management strategy, which is documented below, shall be communicated to the Data Subject, upon a security breach. Such communication shall set out the details of security breaches and procedures to be followed in accordance with the Company's BCM Governance Policies and Procedures. The incident management strategy shall include the:

9.1.1. Notification procedures to Data Subjects whose Personal Information has been compromised;

9.1.2. Manner of notification to Data Subjects and to the Regulator;

9.1.3. Details of the breach;

9.1.4. Actual information that has been compromised;

9.1.5. Identity of person responsible for the breach;

9.1.6. Remedies that are available to the Data Subject whose information has been breached; and

9.1.7. Where the Data Subject objects to the processing of Personal Information, he must do so according to the procedure for lodging a complaint, in terms of the Company's Complaints Resolution Policy and on the prescribed forms. The Company will consider whether the grounds for objections are reasonable and if so, shall discontinue the Processing of Personal Information.

10. Information Officer / Data Protection Officer (IO/DPO)

10.1. The person responsible for fulfilling the tasks of the IO/DPO in respect of the Company are the Key Individuals employed by the Company.

10.2. Best practice dictates that, irrespective of circumstances, the Company should appoint an individual as IO/DPO to lead on ensuring that data protection obligations are met. The minimum tasks of the IO/DPO are:

10.2.1. To inform and advise the organisation and its employees about their obligations to comply with POPI and any other regulatory requirements;

10.2.2. To monitor compliance with POPI and other data protection laws, including managing internal data protection activities, such as having access, as and when required, to data that is up-to-date, accurate, reliable, secure and complete;

10.2.3. To comply with all relevant legislation relating to confidentiality, privacy, security and retention of data;

10.2.4. To comply with any regulatory reporting requirements;

10.2.5. Advise on data protection impact assessments;

10.2.6. Train staff and conduct internal audits;

10.2.7. To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.)

11. Records

11.1. Personal Information belonging to Data Subjects, once obtained, shall be protected in accordance with the Company's BCM Governance policies in order to reduce the risk of any Data breaches.

12. Adoption and Approval

12.1. This Policy has been formally adopted by the Board of Directors.