SANLAM ALLIANZ GENERAL INSURANCE GHANA LTD ("SAZ GI")

DATA PRIVACY POLICY

SAZ GI DATA PRIVACY POLICY	
Type of Policy:	SAZ GI
Entities subject to this Policy:	SAZ GI
Governance Area Addressed:	Compliance
Approving Authority:	SAZ GI Board
Exco Sponsor:	SAZ GI Compliance Manager
Responsible Person:	SAZ GI Compliance Manager
Date of First Approval:	2024
Frequency of review or update:	Annual Review
Date of next review	2025
Version number:	2024.1
Related Policies	• SAZ GI Governance Policy • SAZ GI IT Policy • SAZ GI Information and Data Policy • SAZ GI Digital Behaviour (User) Policy • SAZ GI Cyber and Information Security Policy

1. Purpose of the Policy

1.1. The primary objective of this Policy is to ensure that the SAZ GI Processes Personal Information in a responsible manner that demonstrates its commitment to upholding the right to privacy of Data Subjects, subject to justifiable limitations that are aimed at balancing the right to privacy of Data Subjects against:

1.1.1. the right of access to information; and
1.1.2. the interests of other stakeholders, including the free flow of information across international borders.

1.2. This Policy:

1.2.1. specifies minimum requirements that are to be adhered to with regard to the Processing of Personal Information by SAZ GI entities.

1.2.2. creates a mechanism for the development of binding corporate rules (BCRs) and binding corporate agreements (BCAs) to enable the sharing of information (including Personal Information) by SAZ GI with SanlamAllianz JV (for purposes of enabling it to comply with its obligations as the Controlling Company of the SanlamAllianz JV) and with one another, where there is a legitimate reason to do so.

1.2.3. sets high level standards for SAZ GI, which entities shall formulate, document and implement detailed procedures, processes and systems to proactively ensure compliance with these standards, having due regard to the specific business environment and any relevant applicable laws or regulations of the jurisdiction in which they are located or operate.

2. Scope

2.1. This Policy:

2.1.1. is a SAZ GI Policy and shall apply to all SAZ GI Companies in the manner foreseen in the SAZ GI Governance Policy.

2.1.2. is applicable to the Processing of Personal Information throughout the information life cycle, from the point of first collection of Personal Information until the time that such information is destroyed; and

2.1.3. does not apply to:
2.1.3.1. the Processing of Personal Information in the course of a purely personal or household activity; or
2.1.3.2. Personal Information which has been De-Identified.

3. Policy Statement

3.1. The SAZ GI is committed to:

3.1.1. ensuring that all Personal Information will be Processed in a responsible manner that does not unjustifiably infringe the privacy of any Data Subjects.
3.1.2. securing the integrity and confidentiality of Personal Information of any Data Subjects that comes into its possession or under its control; and
3.1.3. complying with its obligations in accordance with all applicable and relevant laws including, but not limited to, Data Protection Laws.

4. SAZ GI Data Privacy Principles

Where a SAZ GI is the Responsible Party, all Processing of Personal Information by the Company shall be informed by the following key principles:

4.1. **Accountability** - SAZ GI is accountable for ensuring that the provisions of applicable Data Protection Laws and the requirements outlined in this Policy are complied with through implementing appropriate practices, policies and procedures. In addition, SAZ GI must be in a position to demonstrate such compliance.

4.2. **Processing Limitation / Minimisation** – SAZ GI must ensure that Personal Information under its control is Processed only where a Legitimate Basis exists, in a fair, lawful, and non-excessive manner. Personal Information should not be retained for longer than is necessary to achieve the purpose for which it is Processed unless authorised or required by applicable laws. Personal Information must be collected directly from a Data Subject unless collection from another source is permitted under applicable laws.

4.3. **Transparency** - All of a SAZ GI's Processing must be informed by the principle of transparency toward Data Subjects. This includes taking reasonable steps to ensure that Data Subjects are aware of the Processing and that all necessary disclosures as required by applicable Data Protection Laws and this Policy are made.

4.4. **Purposes Specification** - SAZ GI must Process Personal Information only for specific, explicitly defined and legitimate reasons.

4.5. **Further Processing Limitation** - Personal information must not be Processed for a secondary purpose, unless that secondary purpose is compatible with the original purpose or authorised by Data Protection Laws.

4.6. **Information Quality** – SAZ GI must take reasonable steps to ensure that all Personal Information collected and processed is complete, accurate and up to date, and not misleading, considering the purpose for which such information is Processed.

4.7. **Security Safeguards** – SAZ GI must take all reasonable precautions, with regard to the nature of the Personal Information and the risks of the Processing, to preserve the security and confidentiality of the Personal Information and, in particular, prevent its alteration, loss and damage, or access by non-authorised persons. This includes adhering to any SAZ GI information security policies.

4.8. **Data Subject Participation** - SAZ GI must, upon request of a Data Subject and subject to

Data Protection Laws and any other applicable laws relevant to access to information or any legitimate considerations on the part of the SanlamAllianz JV, facilitate access to (and where justified, deletion or correction) of that Data Subject's Personal Information. SAZ GI must ensure that its Data Subjects (including, but not limited to, employees, clients, intermediaries, suppliers and other persons in respect of whom Personal Information is Processed) are made aware of the rights conferred upon them as Data Subjects under Data Protection Laws.

5. Information Officers

5.1. SAZ GI shall appoint an Information Officer.

5.2. SAZ GI shall, to the extent required by Data Protection Laws, appoint a SAZ GI Information Officer or equivalent under the relevant Data Protection Laws. Any such appointments must comply with the requirements of applicable laws.

5.3. The SAZ GI Information Officer's role will be a first-line management responsibility and not a second-line assurance provider responsibility.

5.4. The AZGH Information Officer is responsible for ensuring that this Policy is implemented throughout all SAZ GI entities.

5.5. The SAZ GI Information Officer must engage with SanlamAllianz JV to ensure that a Statutory Information Officer is appointed. The SAZ GI Information Officer may also consider registering as the Statutory Information Officer for a SAZ GI to the extent possible.

5.6. The Chief Executive Officer of:

5.6.1. SAZ GI shall be responsible for appointing and authorising the SAZ GI Information Officer.

5.6.2. SAZ GI shall be responsible for formally appointing and authorising the Company Information Officer.

5.7. The SAZ GI Information Officer is responsible for, inter alia –

5.7.1. Where relevant, ensuring that documented processes and procedures for compliance with Data Protection Laws are developed or updated, monitored, maintained, and made available, including as may be prescribed by Data Protection Laws.

5.7.2. Ensuring that Personal Information impact assessments are done to ensure that adequate measures and standards exist to comply with the conditions for the lawful processing of Personal Information.

5.7.3. Continually assessing SAZ GI's Personal Information Processing procedures and aligning them with Data Privacy Laws, adopted industry codes of conduct and best practices (relevant to the industry and jurisdiction of the SAZ GI operating within SanlamAllianz JV). This will include reviewing all information protection procedures and related policies which are relevant to the SAZ GI.

5.7.4. Taking steps to ensure SAZ GI's compliance with the provisions of Data Protection Laws including by developing, implementing, monitoring and maintaining a compliance framework.

5.7.5. Keeping SAZ GI updated about the Personal Information protection responsibilities under Data Protection Laws including informing and advising Business Entities of their obligations under Data Protection Laws.

5.7.6. Ensuring compliance with the conditions required for the lawful Processing of Personal Information and the principles contained in this Policy.

5.7.7. Organising and overseeing the awareness training of Staff and other individuals involved in the Processing of Personal Information on behalf of SAZ GI.

5.7.8. Ensuring that all requests and complaints related to Data Protection Laws made by SAZ GI's Data Subjects and/or the Supervisory Authority are addressed.

5.7.9. Working with all relevant regulators, SanlamAllianz JV GTI, the SAZ GI Risk and Compliance Office and SanlamAllianz JV in relation to any ongoing investigations.

5.8. The SAZ GI Information Officer may designate a Deputy Information Officer to assist with fulfilling his/her responsibilities and may delegate his/her responsibilities to a Deputy Information Officer, provided that any such delegation:

5.8.1. Must be in writing.

5.8.2. Does not prohibit the person who made the delegation from exercising the power concerned or performing the duty concerned himself or herself.

5.8.3. May at any time be withdrawn or amended in writing by the delegator.

6. Privacy Information Disclosures

6.1. To ensure effective compliance with the principle of transparency referred to in paragraph 4.3 above, SAZ GI must, where required by Data Protection Laws, ensure that they publish privacy notices or privacy statements ("Privacy Disclosures") to enable Data Subjects to clearly understand why and for what purpose their Personal Information is being collected and Processed by the SAZ GI.

6.2. The Privacy Disclosures should, at a minimum, include the following details:

6.2.1. the Personal Information being collected and the source of the Personal Information (if not collected from the Data Subject).
6.2.2. the name and address of the SAZ GI.
6.2.3. the purpose for which the Personal Information is being collected.
6.2.4. whether or not the supply of the Personal Information by the Data Subject is voluntary or mandatory.
6.2.5. the consequences of failure to provide the Personal Information.
6.2.6. any particular law authorising or requiring collection of the Personal Information.

6.2.7. where applicable, that the SAZ GI intends to transfer the Personal Information to a foreign country/ies and the level of protection afforded to the Personal Information

by the recipient in the foreign country.

6.2.8. any other relevant information as may be required by Data Protection Laws.

7. Legitimate Bases

7.1. The SAZ GI may only Process Personal Information where a Legitimate Basis exists. SAZ GI must identify and record the Legitimate Basis it is relying on for Processing Personal Information in each relevant instance.

7.2. Where Consent is the Legitimate Basis, such Consent must be:

7.2.1. obtained prior to the Processing.

7.2.2. clear and unambiguous.

7.2.3. obtained in a recorded manner.

7.2.4. capable of being withdrawn by the Data Subject freely.

7.3. When relying on the SAZ GI ’s legitimate interests as a Legitimate Basis, an LIA must be conducted, and the outcome recorded to ensure that the SAZ GI can demonstrate that it considered whether there were less intrusive means to achieve the purpose of Processing.

8. Special Personal Information

8.1. Special Personal Information are categories of Personal Information that are afforded a higher level of protection by Data Protection Laws. Particular care should be taken in protecting Special Personal Information from loss, damage, unauthorised use, disclosure or access.

8.2. Subject to any other justifications under Data Protection Laws which may exist in relation to Special Personal Information (or a certain category of Special Personal Information), Special Personal Information should only be Processed and disclosed to third parties with the Consent of the Data Subject (or a competent person in respect of a Child).

9. Staff Obligations

9.1. It is a condition of employment that Staff abide by this Policy and procedures, guidelines or rules that may be applicable to them from time to time. This Policy therefore applies to all Staff and may be amended at any time and reissued.

9.2. Staff will, during the course of the performance of their duties and/or services, gain access to and become acquainted with the Personal Information of certain Data Subjects including, but not limited to, employees, clients, intermediaries, suppliers and other stakeholders of SAZ GI or SanlamAllianz JV. In this regard:

9.2.1. All Staff are required to treat Personal Information as a confidential business asset and to respect the privacy of Data Subjects.

9.2.2. Staff may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, any Personal Information which has come into their possession as a consequence of their employment with SAZ GI , unless such information is already publicly known or the disclosure is necessary in order for the relevant Staff member to perform his or her duties.

9.2.3. If a Staff member is unsure about any aspect related to the protection of a Data Subject's Personal Information, such Staff member must request assistance from their line manager, the SAZ GI Information Officer or SAZ GI Deputy Information Officer (where applicable).

9.2.4. Staff must follow all procedures and utilise technologies which the SAZ GI, have implemented to maintain the security of all Personal Information from the point of collection to the point of destruction. This includes complying with SAZ GI's Information Security policies and processes, including, but not limited to the SAZ GI IT Policy, SAZ GI Digital Behaviour (User) Policy, SAZ GI Cyber and Information Security Policy and SAZ GI Information and Data Policy.

9.3. Except to the extent expressly and duly authorised, Staff will under no circumstances –

9.3.1. Process or access Personal Information where such Processing or access is not a requirement to perform their respective work-related tasks or duties.

9.3.2. save copies of Personal Information directly to their own private computers, laptops or other mobile devices like tablets or smart phones, or otherwise copy, print or

reproduce in any form any Personal Information, except as is necessary to fulfil their work-related tasks or duties.

9.3.3. share Personal Information through unsecure methods.

9.3.4. transfer Personal Information to a third party (not being part of the SanlamAllianz JV) in a foreign country.

9.4. Where a Staff member requires access to Personal Information which is not readily available, such Staff Member shall request access to Personal Information from the relevant line manager, the SAZ GI Information Officer or the SAZ GI Deputy Information Officer (as applicable).

9.5. Where a Staff member becomes aware or suspicious of any Security Event such as any unauthorised access, interference, modification, destruction or the unsanctioned disclosure of Personal Information, he or she must immediately report this event or suspicion to the SAZ GI Information Officer and/or SAZ GI Deputy Information Officer (as applicable). The SAZ GI may prescribe a form for notifying Security Events to SAZ GI Information Security.

10. Intra-Group Sharing

10.1. As the Controlling Company, SanlamAllianz JV requires SAZ GI to provide to SanlamAllianz any such information as may be prescribed from time to time (including Personal Information) which is needed to enable SanlamAllianz to comply with its obligations in terms of the South African Insurance Act, No. 18 of 2017 or any other law governing the SanlamAllianz JV as a financial conglomerate or insurance group. SAZ GI shall be bound by any BCRs imposed by SanlamAllianz or BCAs entered into between SanlamAllianz and SAZ GI from time to time in order to give effect to this requirement, which BCRs and BCAs shall be consistent with the provisions of this Policy insofar as they relate to the provision of Personal Information to SanlamAllianz for purposes of SanlamAllianz fulfilling its obligations as the Controlling Company.

10.2. The BCRs and/or BCAs, as applicable, shall also incorporate provisions which allow for sharing of Personal Information amongst SanlamAllianz Group Companies (and Sanlam and initially also Allianz, where applicable and while on Allianz infrastructure) where there are Legitimate Bases for sharing, subject always to applicable Data Protection Laws.

10.3. Where a SanlamAllianz Group Company acts as an Operator on behalf of another SanlamAllianz Group Company, which acts as a Responsible Party, the relevant SanlamAllianz Group Companies shall ensure that there is an Operator Agreement in place between them which shall incorporate provisions required by Data Protection Laws (including any applicable security requirements). The Operator Agreement need not be a standalone agreement and may be incorporated under a broader agreement between the SanlamAllianz Group Companies.

11. Authorised Third Parties

11.1. Where a SanlamAllianz Group Company is the Responsible Party, it is required to ensure that there are Operator Agreements in place with all Authorised Third Parties to ensure that they Process Personal Information in accordance with this Policy and applicable Data

Protection Laws. An Operator Agreement need not be a standalone agreement and may be incorporated under a broader agreement between the SanlamAllianz Group Company and Authorised Third Party.

11.2. Where circumstances warrant (including where the nature of the services to be provided by an Authorised Third Party will involve large scale Processing of Personal Information or Processing of Special Personal Information) the SAZ GI must carry out a due diligence of such Authorised Third Parties. Such due diligence shall be conducted prior to commencement of the services and should be undertaken at least annually thereafter. Such due diligence may include conducting a risk assessment, auditing the facilities, security procedures and policies of such Authorised Third Parties.

11.3. The detail of the Operator Agreement should take into account the nature of the Authorised Third Party's services and exposure to SAZ GI's Personal Information. The SAZ GI Information Officer, in consultation with the SAZ GI COO (and GTI), may set minimum requirements for clauses to be included in Operator Agreements.

11.4. All Authorised Third Parties who Process Personal Information must strictly adhere to a level of security commensurate with the security requirements set forth in SAZ GI's Security policy(ies) (including the SAZ GI Information Security Requirements for Operators) and shall be required to maintain and where required, upgrade their systems and processes to ensure the appropriate level of security.

11.5. The Operator Agreement shall:

11.5.1. include a right for the SAZ GI to audit the facilities and premises of the Authorised Third Parties (and subcontractors to the Authorised Third Party) to ensure adherence to the security policies; and

11.5.2. provide adequate recourse to SAZ GI, including a right to terminate, indemnification for breach and/or appropriate insurance cover for cyber security breaches, to the AZGHGI where the Authorised Third Party is not complying with the requirements set forth in the Processor Agreement.

11.6. Authorised Third Parties must, as part of the Operator Agreement, be required to immediately inform the SAZ GI (via the office of the SAZ GI Information Officer) of any actual or suspected Security Event or compromise to Personal Information in its possession.

11.7. Authorised Third Parties may be required to notify the affected Data Subject(s) and/or the Supervisory Authority, but this should only be carried out on the SAZ GI instructions, via the office of the relevant SAZ GI Information Officer.

11.8. Authorised Third Parties, including data storage and Processing providers, may from time to time also have access to a Data Subject's Personal Information in connection with the storage and retention thereof. SAZ GI must ensure that these Authorised Third Parties only Process the Personal Information in accordance with the instructions of the SAZ GI and relevant provisions of this Policy, all other relevant internal policies of SanlamAllianz and Data Protection Laws.

12. Cross Border Transfers of Personal Information

12.1. The SAZ GI must determine and adhere to all relevant and applicable legal requirements for cross-border transfers of Personal Information in their respective jurisdictions. Furthermore, Company must maintain a record of any cross-border transfers of Personal Information. Such record must document the processes and procedures governing cross-border transfers as well as safeguards and legal justifications the SAZ GIis relying on for such transfers.

12.2. Subject to paragraph 12.1 above, SAZ GI may only transfer Personal Information to a third party in a foreign country in any of the following circumstances:

12.2.1. to another SanlamAllianz Group Company, subject to this Policy, the BCRs and/or BCAs;

12.2.2. to an Authorised Third Party, provided that the Authorised Third Party is bound by an Operator Agreement which complies with the requirements of this Policy;

12.2.3. the Data Subject has Consented to the proposed transfer, after being informed of any potential risks; or

12.2.4. the transfer is necessary for one of the other reasons set out in the Data Protection Laws, including:

12.2.4.1. the performance of a contract between SAZ GI or SanlamAllianz and the Data Subject;

12.2.4.2. the performance of a contract concluded between SAZ GI and a third party in the interest of a Data Subject;

12.2.4.3. where the transfer is for the benefit of the Data Subject provided that it is not reasonably practicable to obtain the Data Subject's Consent to the transfer and if it were reasonably practicable to obtain such Consent, the Data Subject would be likely to give it; and

12.2.4.4. in some limited cases, for the legitimate interest of SAZ GI or SanlamAllianz.

12.3. A risk assessment should be undertaken when using cloud-based services that involve the Processing of Personal Information. Such risk assessment should be conducted in line with any other applicable policies regulating the use of cloud services by SanlamAllianz Group Companies including SAZ GI, and shall take into account, at a minimum:

12.3.1. The location of the servers where the Personal Information will be stored and any data residency requirements;

12.3.2. The jurisdictions to which the Personal Information will be transferred, and the level of protection to Personal Information afforded in each such jurisdiction;

12.3.3. The level of security implemented by the service provider considered in the context of the sensitivity of the Personal Information; and

12.3.4. The legislative requirements applicable to the third party in countries where the Personal Information will be hosted, particularly where countries have rights to

seize or otherwise access Personal Information hosted by the third party.

13. Procedure to Request Access to Personal Information

13.1. Data Subjects have the right to:

13.1.1. request information about Personal Information that SAZ GI holds about them as well as request the reasons for SAZ GI, as the case may be, holding it;

13.1.2. request access to their Personal Information; and

13.1.3. be informed of how to keep their Personal Information up to date.

13.2. SAZ GI shall develop an access request procedure, which will apply to Data Subject access requests under Data Protection Laws. Such procedure must be documented, made available to Staff within SAZ GI and describe the end-to-end process from the initiation of an access request by a Data Subject, to the execution of such request.

13.3. Where Data Protection Laws prescribe forms for access requests, SAZ GI must ensure that such forms are placed on their websites and are readily available via all client-facing channels.

14. Disclosure of Information required by Competent Authorities

14.1. Where SAZ GI is required to disclose Personal Information to local and/or international tax authorities; to regulatory authorities or government institutions; or pursuant to an order by a court of law (collectively “Competent Authorities”), the SAZ GI shall verify the veracity of any such request from a Competent Authority before making any disclosures and will take reasonable care to ensure that only the Personal Information that is legally required, and nothing more, is provided to the Competent Authority.

15. Security Safeguards

15.1. To ensure effective compliance with the principle of security safeguards referred to in paragraph 4.7 above SAZ GI shall:

15.1.1. adopt a risk-based approach to continually improving its information security safeguards by implementing and maintaining appropriate information security policies and controls applicable to both management and to end-users. Due regard must be had of the SAZ GI Cyber and Information Security Policy with its underlying policies, as well as the SAZ GI Digital Behaviour (User) Policy;

15.1.2. implement measures to monitor compliance with its security policies and procedures and verify the implementation of security controls through accepted methods, such as audits;

15.1.3. create and maintain awareness amongst its Staff about its information security policies and procedures through on-boarding processes and security awareness drives;

15.1.4. ensure that all Personal Information leaving secure environments is adequately protected by using appropriate technologies, like encryption or physical controls.

15.1.5. exercise due care in the disposal or destruction of Personal Information in order to prevent unauthorised access; and

15.1.6. ensure that any Authorised Third Party that Processes Personal Information on its behalf has security safeguards in place which are at least commensurate with those referred to in this Policy.

15.2. SAZ GI shall ensure that appropriate incident management measures are in place to monitor, detect, assess and respond to any Security Event involving Personal Information in its possession or under its control. Such incident management measures shall be aligned with any standard(s) on data breach reporting issued under his Policy.

15.3. Where there are reasonable grounds to believe that a Security Event has occurred and to the extent required by applicable laws, the SAZ GI will notify the Supervisory Authority and the affected Data Subjects (unless the identity of the Data Subjects cannot be established) as soon as reasonably possible.

15.4. Any notifications to a Supervisory Authority and/or affected Data Subjects shall be undertaken in consultation with the SAZ GI Information Officer and comply with the requirements of applicable laws (including Data Protection Laws).

15.5. The SAZ GI Information Officer may prescribe a form for notifying Security Events to SanlamAllianz Information Security.

16. Data Storage and Retention

16.1. SAZ GI and/or Authorised Third Parties must ensure that Personal Information, including Special Personal Information which they Process, is Processed, (including captured, used, disclosed, stored and destroyed) in a secure and confidential manner appropriate to the classification of the information, in accordance with SanlamAllianz's data retention and destruction policy and / or relevant provisions of Data Protection Laws.

16.2. In order to comply with Data Protection Laws, SAZ GI –

16.2.1. must keep records of the Personal Information it has collected, correspondence or comments in an electronic or hardcopy file format. Personal information may be Processed for as long as necessary to fulfil the purposes for which that Personal Information was collected and/or as permitted or required by applicable law;

16.2.2. may retain Personal Information for longer periods for statistical, historical or research purposes, and should this occur, the SAZ GI must ensure that appropriate safeguards have been put in place to ensure that: (i) all recorded Personal Information will continue to be Processed in accordance with this Policy and the applicable laws, and (ii) the records of Personal Information shall not be used for any other purposes; and

16.2.3. must, once the purpose for which the Personal Information was initially collected and Processed no longer applies or becomes obsolete, and there is no legitimate

reason for retention of such Personal Information, ensure that it is deleted, destroyed or De-Identified.

16.3. Where a SAZ GI no longer needs Personal Information for achieving the purpose for which it was initially collected or subsequently Processed, but retains such Personal Information for the purposes of proof, the SAZ GI shall not be required to delete or destroy such information, but must restrict the Processing of such Personal Information from further circulation, publication or use and ensure that there are appropriate security safeguards consistent with the requirements of this Policy in respect of such Personal Information.

17. Direct Marketing

17.1. SAZ GI takes cognisance of the rights of Data Subjects regarding Direct Marketing by means of unsolicited electronic communications and will implement all relevant requirements of Data Protection Laws with regard to Direct Marketing and unsolicited electronic communications.

17.2. Under certain Data Protection Laws, Data Subjects have specific rights with regard to unsolicited electronic communications and can object to Direct Marketing at any time. The Processing of the Data Subject's Personal Information for the purposes of Direct Marketing by means of unsolicited electronic communication is prohibited unless:

17.3. the Data Subject has given his/her Consent; or

17.4. the Data Subject is a customer of the Responsible Party subject to the following requirements:

17.4.1. the contact details of the Data Subject were obtained by the Responsible Party in the context of the sale of a product or service;

17.4.2. the Direct Marketing is for the purpose of marketing the Responsible Party's own similar products or services; and

17.4.3. the Data Subject must have been given an opportunity, free of charge and in a manner free of unnecessary formality, to object to receiving electronic communications for Direct Marketing purposes at the time of collection and again on each subsequent communication.

17.5. Where applicable laws require an explicit opt-in, SAZ GI shall make use of an explicit opt- in component for Direct Marketing by means of unsolicited electronic communications.

17.6. Unless applicable laws permit an opt-out approach, only if a Data Subject chooses to opt in to a Responsible Party sharing the Data Subject's Personal Information with the Responsible Party's marketing partners, can the Responsible Party share the Data Subject's Personal Information with their marketing partners.

17.7. A Responsible Party cannot sell Personal Information without the Data Subject's specific opt-in to the sale of their Personal Information.

18. Automated Decision Making

18.1. SAZ GI must ensure that Data Subjects are not made subject to a decision which has legal consequences for him, her or it, or which affects him, her or it to a substantial degree, which is made solely on the basis of the automated Processing of Personal Information intended to provide a profile of such person including his or her performance at work, or his, her or its credit worthiness, reliability, location, health, personal preferences or conduct unless the decision:

18.1.1. has been taken in connection with the conclusion or execution of a contract and:

18.1.1.1. the request of the Data Subject in terms of the contract has been met; or

18.1.1.2. appropriate measures are taken to protect the data subject's legitimate interests; or

18.1.2. is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of Data Subjects.

18.2. If there is no law or code of conduct, the appropriate measures to be taken must:

18.2.1. provide an opportunity for the Data Subject to make representations about the automated decision; and

18.2.2. require the SAZ GI making the decision to provide a Data Subject with sufficient information about the underlying logic of the automated decision-making process in order to enable the Data Subject to make representations.

19. Processing of Personal Information of Staff

19.1. SAZ GI's human resource function ("HR") shall ensure that they comply with this Policy in respect of all the Business Cluster's Staff Personal Information which they Process.

19.2. HR must only collect such Personal Information of Staff as is necessary for their employment relationship with the relevant SAZ GI, to comply with applicable laws or where the Company otherwise has a Legitimate Basis for Processing the Personal Information collected.

19.3. The provisions of this paragraph apply to Personal Information collected in relation to any Staff member (whether before, during or after employment), including from the time that a potential member of Staff applies for a job, during the interview and selection process and if such candidate is successful, all information processed during the course of their employment, on the termination of their employment and where applicable, after termination of employment.

20. Complaints Procedures

20.1. The SAZ GI Information Officer, and the Company must document and implement specific procedures, processes and controls for lodging and handling complaints related to the Processing of Personal Information. Such complaints procedure must, at a minimum, contain the following:

20.1.1. Data Subjects must be encouraged to submit their complaints/ enquiries which relate to the Processing of Personal Information, directly to the relevant SAZ GI

instead of approaching the Supervisory Authority, in order to give the SAZ GI the opportunity to swiftly and efficiently address the complaint/ enquiry internally and outside of the public domain.

20.1.2. A Data Subject must be able to direct a challenge regarding an alleged infringement of their rights to the SAZ GI Information Officer. The SAZ GI Information Officer must therefore establish procedures to receive and respond to enquiries or challenges to its policies and practices relating to the handling of Personal Information. These procedures must be easily accessible and simple to use.

20.2. The SAZ GI must inform Data Subjects of these procedures through their websites, brochures, or other documents, which must be readily available and easy to understand. The complaint resolution process must be explained and contact information for customers to reach the SAZ GI must be provided.

21. Implementation, Enforcement and Reporting of Breaches of this Policy

21.1. All Staff must ensure that they have read, understood and comply with this Policy when Processing Personal Information during the course and scope of their employment with the SAZ GI. Any breach of this Policy may result in disciplinary action and individuals may be subject to a fine under the applicable Data Protection Laws.

21.2. The SAZ GI must ensure compliance with the legal and regulatory requirements relating to the Processing of Personal Information applicable to it, including as may be contained in this Policy and all applicable Data Protection Laws. It may be necessary for SAZ GI to seek advice from local legal practitioners as to the legal and regulatory requirements relating to the Processing of Personal Information currently in force in a particular jurisdiction.

21.3. The responsibility to develop and document detailed policies, processes, actions and procedures to give effect to and implement the principles put forward in this Policy vests primarily with the SAZ GI, provided that the SAZ GI Information Officer shall be responsible for ensuring alignment across the Company. SAZ GI must be able to demonstrate that they have made all necessary efforts to ensure compliance, including conducting assessments to understand the impact of all relevant and applicable Data Protection Laws on SAZ GI and the SanlamAllianz JV.

21.4. The SAZ GI Information Officer, the SAZ GI COO (with GTI), the SAZ GI Riak and Compliance Office and other SAZ GI Exco members may formulate operational standards in terms of this Policy for submission to the SAZ GI Executive Committee for consideration and approval. Once approved, the operational standards will be binding on the SAZ GI in the manner foreseen in the SAZ GI Governance Policy.

21.5. Any non-compliance with the terms of this Policy could have serious legal and reputational repercussions for the SAZ GI and my cause significant reputational- and financial damage to the SAZ GI and its shareholders.

21.6. Should any Staff member become aware of any non-compliance with the terms of this Policy, they are required to immediately report this to their relevant line managers, who in turn should report this to the SAZ GI Information Officer.

21.7. The SAZ GI Risk and Compliance Office will provide clarification on any aspect of the Policy and how it should be incorporated in the activities of SAZ GI.

22. Definitions

In this Policy, the following capitalised terms will have the meanings given to them:

Associates and joint ventures	An investment over which SanlamAllianz exercises significant influence or joint control, which requires the investment to be equity accounted in the SanlamAllianz financial statements. In most cases SanlamAllianz will have a direct or indirect shareholding of more than 20% but less than 50% of the entity's issued share capital. It includes joint ventures that are equity accounted in the SanlamAllianz financial statements. Strategic shareholding of less than 20% into unlisted businesses can also be classified as an associated company or joint venture.
Authorised Third Party	A third party (not being a SanlamAllianz Group Company) who Processes Personal Information on behalf of a SanlamAllianz Group Company or as part of any functions or duties which they carry out in terms of a contract for a SanlamAllianz Group Company.
BCAs	Binding Corporate Agreements which shall be entered into between at least two SanlamAllianz Group Companies (which may be in lieu of, or in addition to, the BCRs) to facilitate the transfer of information (including Personal Information) between: • Sanlam and SanlamAllianz Group Companies; and • SanlamAllianz Group Companies amongst each other.
BCRs	Binding Corporate Rules applicable to SanlamAllianz Group Companies which shall be developed to facilitate the transfer of information (including Personal Information) between: • SAZ GI and SanlamAllianz ; and • SanlamAllianz Group Companies amongst each other.
Child	A natural living person under the age of majority in the relevant jurisdiction in which SAZ GI operates.
Consent	Any voluntary, specific and informed expression of will, in terms of which permission is given for the Processing of Personal Information.

Controlling Company	Has the meaning given to it in the South African Insurance Act, No. 18 of 2017.
Data Protection Laws	Any data protection or data privacy laws relating to Personal Information, applicable to the activities of a Group Company from time to time, including POPIA, any laws, regulations, guidelines and/or codes of conducts issued by a Supervisory Authority.
Data Subject	A living natural or where applicable, existing juristic, person to whom Personal Information relates.
De-Identify	In relation to Personal Information, means to delete any information that identifies the Data Subject such that the Data Subject cannot be re-identified again (i.e. permanently anonymised/aggregated).
Deputy Information Officers	A person(s) to whom the SAZ GI Information Officer and/or SAZ GI Information Officers have delegated the day-to-day administration of this Policy and related privacy policies and practices.
Direct Marketing	To approach a Data Subject, either in person or by mail or electronic communication, for the direct or indirect purpose of: • promoting or offering to supply, in the ordinary course of business, any goods or services to the Data Subject; or • requesting the Data Subject to make a donation of any kind for any reason.
GTI	Group Technology and Information.
Legitimate Basis	Any legitimate basis for the Processing of Personal Information recognised by applicable Data Protection Laws including where – • the Processing is necessary to carry out actions for the conclusion or performance of a contract to which the Data Subject is a party; or • the Processing complies with an obligation imposed by law on the Responsible Party; or • the Processing protects a legitimate interest of the Data Subject; or • the Processing is necessary for pursuing the legitimate interests of the Responsible Party or of a third party to whom the information is supplied, provided that an LIA has been undertaken; or • the Data Subject, or the parent, legal guardian (or other competent person) where the Data Subject

	is a Child, Consents to the Processing.
LIA	A legitimate interest assessment which should be undertaken by a SanlamAllianz Group Company where such SanlamAllianz Group Company is relying on its (or a third party recipient's) legitimate interests as the Legitimate Basis for Processing. Such LIA should include: • determining the purpose of the Processing, which purpose must be specific, explicitly defined and lawful; • determining whether the Processing is necessary to achieve the purpose identified; and • undertaking a balancing exercise to determine whether the Data Subject's rights and freedoms override the legitimate interests.
Operator	A person who Processes Personal Information for a Responsible Party in terms of a contract or mandate, without coming under the direct authority of that Responsible Party.
Operator Agreement	A written agreement (or clauses within a broader written agreement) to be concluded between: • a SAZ GI and an Authorised Third Party, which regulates the manner in which an Authorised Third Party, acting as an Operator, Processes Personal Information for a SAZ GI, acting as a Responsible Party; or • a SAZ GI and another SanlamAllianz Group Company, which regulates the manner in which one SanlamAllianz Group Company, acting as an Operator, Processes Personal Information for the other SanlamAllianz Group Company, acting as a Responsible Party.

Personal Information	Refers to 'personal data' or 'personal information' as such terms are defined in Data Protection Laws, and for purposes of this Policy, refers to Personal Information Processed in the course of the SanlamAllianz Group carrying out its operations.
POPIA	The South African Protection of Personal Information Act, No. 4 of 2013.
Process / Processing	Any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information, including – • the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; • dissemination by means of transmission, distribution or making available in any other form; or • merging, linking, as well as restriction, degradation, erasure or destruction of information, or any other activity defined to constitute processing in terms of Data Protection Laws.
Responsible Party	Where a SanlamAllianz Group Company, alone or in conjunction with others, determines the purpose of and means for Processing of Personal Information, it will be the Responsible Party. The Responsible Party is ultimately accountable for ensuring that Personal Information is Processed lawfully.
SanlamAllianz Group	Sanlam Allianz Africa (Pty) Ltd (SanlamAllianz) and all SanlamAllianz Group companies comprise the SanlamAllianz Group.
SanlamAllianz Group companies	Subsidiaries, associates and joint ventures collectively comprise SanlamAllianz Group companies. Portfolio Investments are not seen as Group companies.
AZGH Information Officer	The Statutory Information Officer for SAZ GI.
SAZ GI Information Officer	The designated information officer of SAZ GI, tasked with ensuring compliance by Company with Data Protection Laws.
Sanlam Limited Insurance Group	The insurance group designated under the South African Insurance Act, No. 18 of 2017.

Security Event	Where there is reason to believe or to suspect that Personal Information has been acquired, disclosed, used, dealt with in any way whatsoever or accessed by an unauthorised party or is reasonably likely to be acquired, disclosed, used or accessed by an unauthorised party.

Special Personal Information	Refers to 'special personal information' or 'sensitive personal data' as defined in Data Protection Laws and for purposes of this Policy, includes Personal Information relating to a Child.
Staff	In relation to SAZ GI, all employees (whether permanent or temporary), directors, officers, natural persons acting as contractors under the authority of SAZ GI and other staff of such SAZ GI Company.
Statutory Information Officer	Where Data Protection Laws require SAZ GI to register an information officer with a Supervisory Authority, the individual registered as such from time to time.
Subsidiary	An investment where SanlamAllianz exercises such a level of control that requires the investment to be consolidated in the SanlamAllianz accounts (either due to equity holding or material influence). It excludes consolidated portfolio investment funds. In most cases SanlamAllianz will have a direct or indirect shareholding of more than 50% of the entity's issued share capital. For governance purposes it includes subsidiaries of subsidiaries.
Supervisory Authority	The supervisory authority or other regulatory authority responsible for monitoring and enforcing Data Protection Laws in the relevant jurisdiction. In South Africa, the Supervisory Authority is the Information Regulator appointed in terms of POPIA.