

# Santam Group **Privacy Policy**

Santam is an authorised financial services provider (FSP 3416),  
a licensed non-life insurer and controlling company for its group companies.



# Santam Group

# **Privacy Policy**

## **Table of contents**

1.	Policy statement	<b>3</b>
2.	Purpose of the policy	<b>3</b>
3.	Scope	<b>3</b>
4.	Santam's privacy principles	<b>3</b>
5.	Information officers	<b>4</b>
6.	Privacy information disclosures	<b>5</b>
7.	Legitimate bases	<b>5</b>
8.	Special personal information	<b>6</b>
9.	Staff obligations	<b>6</b>
10.	Intra-group sharing	<b>7</b>
11.	Authorised third parties	<b>7</b>
12.	Cross border transfers of personal information	<b>8</b>
13.	Procedure to request access to personal information	<b>8</b>
14.	Disclosure of information required by competent authorities	<b>9</b>
15.	Security safeguards	<b>9</b>
16.	Data storage and retention	<b>10</b>
17.	Direct marketing	<b>10</b>
18.	Automated decision making	<b>11</b>
19.	Processing of personal information of staff	<b>11</b>
20.	Complaints procedures	<b>11</b>
21.	Implementation, enforcement and reporting of breaches of this policy	<b>11</b>
22.	Definitions	<b>12</b>

# Santam Group

# Privacy Policy

## 1. POLICY STATEMENT

The Santam Group is committed to ensure that Personal Information is at all times processed fairly, lawfully and correctly, and within the ambit of applicable legislation which is underpinned by the constitutional right to privacy and to provide an appropriate level of security and privacy of Personal Information about its data subjects (which would include customers, intermediaries, business partners and employees) that comes into its possession or custody.

## 2. PURPOSE OF THE POLICY

2.1 The primary objective of this Policy is to ensure that the Santam Group and consequently the Sanlam Group 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:

2.1.1 the right of access to information; and

2.1.2 the interests of other stakeholders, including the free flow of information across international borders.

### 2.2 This Policy:

2.2.1 specifies minimum requirements that are to be adhered to with regard to the Processing of Personal Information by Group Companies;

2.2.2 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 Group Companies with Santam Limited (for purposes of enabling it to comply with its obligations as the Controlling Company of the Santam Limited Insurance Group) and with one another, where there is a legitimate reason to do so; and

2.2.3 sets high level standards for Santam Limited and Group Companies, 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.

## 3. SCOPE

### 3.1 This Policy:

3.1.1 is a Santam Group Policy and shall apply to all Group Companies in the manner foreseen in the Group Governance Policy;

3.1.2 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

3.1.3 **does not apply** to:

3.1.3.1 the Processing of Personal Information in the course of a purely personal or household activity; or

3.1.3.2 Personal Information which has been De-Identified.

## 4. SANTAM'S PRIVACY PRINCIPLES

Santam has developed the following set of Privacy Principles governing the lawful processing of Personal Information applicable within the Santam Group.

### 4.1 Accountability

Each Group Company 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, Group Companies must be in a position to demonstrate such compliance.

### 4.2 Processing Limitation/Minimisation

Each Group Company 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.

# Santam Group

# Privacy Policy

## 4.3 Purpose Specification

A Group Company must Process Personal Information only for specific, explicitly defined and legitimate reasons.

## 4.4 Transparency

All of a Group Company'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.

## 4.5 Further Processing

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

Each Group Company 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

Each Group Company 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 Santam Group Information Security policies.

## 4.8 Data Subject Participation

Each Group Company 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 Group Company, facilitate access to (and where justified, deletion or correction) of that Data Subject's Personal Information. Each Group Company 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 Santam shall appoint a Group Information Officer.
- 5.2 Each Group Company shall, to the extent required by Data Protection Laws, appoint an Information Officer or equivalent under the relevant Data Protection Laws. Any such appointments must comply with the requirements of applicable laws.
- 5.3 Each Business Cluster must appoint or designate an Information Officer, where necessary and appropriate and based on the scale, nature and complexity of the business, or an equivalent designation at management level and whose role will be a first-line management responsibility and not a second-line assurance provider responsibility.
- 5.4 The Cluster Information Officer is responsible for ensuring that this Policy is implemented throughout all Group Companies and Business Entities within the relevant Business Cluster.
- 5.5 The Cluster Information Officer must engage with the Group Company to ensure that a Statutory Information Officer is appointed. The Cluster Information Officer may also consider registering as the Statutory Information Officer for a Group Company to the extent possible.
- 5.6 The Chief Executive Officer of:
  - 5.6.1 Santam Limited shall be responsible for appointing and authorising the Group Information Officer;
  - 5.6.2 each Business Cluster, subject to Clause 5.3, above shall be responsible for appointing and authorising the respective Cluster Information Officers; and
  - 5.6.3 a Group Company shall be responsible for formally appointing and authorising a Group Company Information Officer.

# Santam Group

# Privacy Policy

- 5.7 The Cluster Information Officer or its designated equivalent as contemplated in clause 5.4 above is responsible for, inter alia –
  - 5.7.1 where relevant, ensuring that the business documents 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 the Business Cluster'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 Group Companies operating within the Business Cluster). This will include reviewing all information protection procedures and related policies which are relevant to the Business Entities;
  - 5.7.4 taking steps to ensure the Business Cluster's compliance with the provisions of Data Protection Laws including by developing, implementing, monitoring and maintaining a compliance framework;
  - 5.7.5 keeping the Business Cluster updated about the Personal Information protection
  - 5.7.6 responsibilities under Data Protection Laws including informing and advising Business Entities of their obligations under Data Protection Laws;
  - 5.7.7 ensuring compliance with the conditions required for the lawful Processing of Personal Information and the principles contained in this Policy;
  - 5.7.8 organising and overseeing the awareness training of Staff and other individuals involved in the Processing of Personal Information on behalf of a Business Cluster;
  - 5.7.9 ensuring that all requests and complaints related to Data Protection Laws made by the Business Cluster's Data Subjects and/or the Supervisory Authority are addressed; and
- 5.8 working with all relevant regulators, GTI, the Group Compliance Office and the Group.

## 6. PRIVACY INFORMATION DISCLOSURES

- 6.1 To ensure effective compliance with the principle of transparency referred to in paragraph 4.3 above, Group Companies 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 Group Company.
- 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 Group Company;
  - 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 Group Company 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; and
  - 6.2.8 any other relevant information as may be required by Data Protection Laws.

## 7. LEGITIMATE BASES

- 7.1 A Group Company may only Process Personal Information where a Legitimate Basis exists. Each Group Company 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;

# Santam Group

# Privacy Policy

7.2.2 clear and unambiguous;

7.2.3 obtained in a recorded manner; and

7.2.4 capable of being withdrawn by the Data Subject freely.

7.3 When relying on the Group Company's legitimate interests as a Legitimate Basis, an LIA must be conducted and the outcome recorded to ensure that the Group Company 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 Sanlam or a Group Company. 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 a Group Company, 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 Cluster Information Officer, the Group Company Information Officer or Deputy Information Officer (where applicable).

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

9.3.4 transfer Personal Information to a third party (not being part of the Santam Group) 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 Cluster Information Officer, the Group Company Information Officer or the Deputy Information Officer (as applicable).

# Santam Group

## Privacy Policy

- 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 Cluster Information Officer, Group Company Information Officer and/or Deputy Information Officer (as applicable). The Santam Group may prescribe a form for notifying Security Events to Santam Group Information Security.

## 10. INTRA-GROUP SHARING

- 10.1 As the Controlling Company of the Santam Limited Insurance Group, Santam requires Group Companies that form part of the Santam Limited Insurance Group to provide to Santam any such information as may be prescribed from time to time (including Personal Information) which is needed to enable Santam to comply with its obligations in terms of the South African Insurance Act, No. 18 of 2017 or any other law governing the Santam Group as a financial conglomerate or insurance group. Each Group Company shall be bound by any BCRs imposed by Santam or BCAs entered into between Santam and a Group Company 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 Santam for purposes of Santam 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 Group Companies (and Santam) where there are Legitimate Bases for sharing, subject always to applicable Data Protection Laws.
- 10.3 Where a Group Company acts as an Operator on behalf of another Group Company, which acts as a Responsible Party, the relevant 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 Group Companies.

## 11. AUTHORISED THIRD PARTIES

- 11.1 Where a 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 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 Group Company must perform 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 a Group Company's Personal Information. The Group Information Officer, in consultation with GTI, other Group Functionaries and Cluster Information Officers, 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 the Santam Group's Security policy(ies) (including the Santam Group 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 Group Company 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 a Group Company, including a right to terminate, indemnification for breach and/or appropriate insurance cover for cyber security breaches, to the Group Company where the Authorised Third Party is not complying with the requirements set forth in the Processor Agreement.



# Santam Group

# Privacy Policy

- 11.6 Authorised Third Parties must, as part of the Operator Agreement, be required to immediately inform the Group Company (via the office of the Group Company 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 Group Company's instructions, via the office of the relevant Group Company 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. Each Group Company must ensure that these Authorised Third Parties only Process the Personal Information in accordance with the instructions of the Group Company and relevant provisions of this Policy, all other relevant internal policies of the Santam Group or Business Cluster and Data Protection Laws.

## 12. CROSS BORDER TRANSFERS OF PERSONAL INFORMATION

- 12.1 Each Group Company must determine and adhere to all relevant and applicable legal requirements for cross-border transfers of Personal Information in their respective jurisdictions. Furthermore, each Group 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 Group Company is relying on for such transfers.
- 12.2 Subject to paragraph 12.1 above, a Group Company may only transfer Personal Information to a third party in a foreign country in any of the following circumstances:
  - 12.2.1 to another 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 Santam or the Group Company and the Data Subject;
    - 12.2.4.2 the performance of a contract concluded between a Group Company 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 Santam or the Group Company.
- 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 Group Companies, 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 Santam or a Group Company holds about them as well as request the reasons for Santam or a Group Company, as the case may be, holding it;



# Santam Group

# Privacy Policy

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 Each Business Cluster 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 the Business Cluster 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, Group Companies 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 a Group Company 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 Group Company 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 each Group Company 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 Santam Group Cyber and Information Security Policy with its underlying policies, as well as the Santam Group 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 Each Group Company 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 Group Company 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 Cluster Information Officer and Group Information Officer, and comply with the requirements of applicable laws (including Data Protection Laws).

15.5 The Group Information Officer may prescribe a form for notifying Security Events to Santam Group Information Security.

# Santam Group

# Privacy Policy

## 16. DATA STORAGE AND RETENTION

- 16.1 Group Companies 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 the Business Cluster's data retention and destruction policy and/or relevant provisions of Data Protection Laws.
- 16.2 In order to comply with Data Protection Laws, each Group Company –
  - 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 Group Company 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 Group Company 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 Group Company 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 The Santam Group 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, Group Companies 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 the 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.

# Santam Group

# Privacy Policy

## 18. AUTOMATED DECISION MAKING

- 18.1 Each Group Company 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 Group Company 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 Each Business Cluster'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 Group Company, to comply with applicable laws or where the Group 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 Group Information Officer, and each Group 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 Group Company instead of approaching the Supervisory Authority, in order to give the Group Company 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 Group Company Information Officer. Each Group Company 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 Group Company 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 Group Company 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 a Group Company. Any breach of this Policy may result in disciplinary action and individuals may be subject to a fine under the applicable Data Protection Laws.

# Santam Group

## Privacy Policy

- 21.2 Each Group Company 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 a Group Company 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 Group Companies, provided that the Cluster Information Officer shall be responsible for ensuring alignment across the Business Cluster. All Group Companies 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 the Santam Group and the Group Company.
- 21.4 The Group Information Officer, GTI, the Group Compliance Office and other Group Functionaries may formulate operational standards in terms of this Policy for submission to the Group Executive Committee for consideration and approval. Once approved, the operational standards will be binding on Group Companies in the manner foreseen in the Group Governance Policy.
- 21.5 Any non-compliance with the terms of this Policy could have serious legal and reputational repercussions for the Santam Group and may cause significant reputational- and financial damage to the Santam Group.
- 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 Cluster Information Officer.
- 21.7 The Group Compliance Office will provide clarification on any aspect of the Policy and how it should be incorporated in the activities of Santam.

## 22. DEFINITIONS

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

DEFINITION	DESCRIPTION
<b>Associated company and joint venture</b>	An investment over which Santam exercises significant influence or joint control, which requires the investment to be equity accounted in the group financial statements. In most cases Santam 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 group financial statements. Strategic shareholding of less than 20% into unlisted businesses can also be classified as an associated company or joint venture.
<b>Authorised Third Party</b>	A third party (not being a Group Company) who Processes Personal Information on behalf of a Group Company or as part of any functions or duties which they perform in terms of a contract for a Group Company.
<b>BCAs</b>	Binding Corporate Agreements which shall be entered into between at least two Group Companies (which may be in lieu of, or in addition to, the BCRs) to facilitate the transfer of information (including Personal Information) between: <ul style="list-style-type: none"> <li>• Santam and Group Companies; and</li> <li>• Group Companies amongst each other.</li> </ul>
<b>BCRs</b>	Binding Corporate Rules applicable to Group Companies which shall be developed to facilitate the transfer of information (including Personal Information) between: <ul style="list-style-type: none"> <li>• Santam and Group Companies; and</li> <li>• Group Companies amongst each other.</li> </ul>
<b>Business unit (Entity)</b>	The Santam businesses that perform the activities of a Business unit. Business Entities include Santam Group Entities, Business Divisions and business units subject to governance oversight requirements provided on a Business unit level.

# Santam Group

## Privacy Policy

DEFINITION	DESCRIPTION
<b>Business units</b>	<p>The grouping of businesses controlled by a separate board of directors or a notional board established for governance purposes, with their own governance structures who report directly to the Santam Limited boards. Currently this currently includes:</p> <ul style="list-style-type: none"> <li>• Santam Commercial and Personal (Santam C&amp;P)</li> <li>• Santam Specialist</li> <li>• MiWay</li> <li>• Santam Re</li> <li>• Santam International</li> <li>• Alternative Risk Transfer (ART)</li> </ul> <p>The definition of Business unit should not be confused with the reference to licenced entities.</p>
<b>Child</b>	A natural living person under the age of majority in the relevant jurisdiction in which a Group Company operates.
<b>Business Entity Information Officer</b>	The designated information officer of the Business Entity, tasked with ensuring compliance by Business Entities with Data Protection Laws.
<b>Consent</b>	Any voluntary, specific and informed expression of will, in terms of which permission is given for the Processing of Personal Information.
<b>Controlling Company</b>	Has the meaning given to it in the South African Insurance Act, No. 18 of 2017.
<b>Data Protection Laws</b>	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.
<b>Data Subject</b>	A living natural or where applicable, existing juristic, person to whom Personal Information relates.
<b>De-Identify</b>	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).
<b>Deputy Information Officers</b>	A person(s) to whom Information Officers and/or Group Company Information Officers have delegated the day-to-day administration of this Policy and related privacy policies and practices.
<b>Direct Marketing</b>	<p>To approach a Data Subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:</p> <ul style="list-style-type: none"> <li>• promoting or offering to supply, in the ordinary course of business, any goods or services to the Data Subject; or</li> <li>• requesting the Data Subject to make a donation of any kind for any reason.</li> </ul>
<b>Group Company(ies)</b>	A Santam Group Entity in respect of which Santam exercises a level of control that requires consolidation in the Santam Group accounts (either due to equity holding or material influence), but excludes consolidated portfolio investment. In most cases Santam will have a direct or indirect shareholding of more than 50% of the entity's issued capital.
<b>Group Company Information Officer</b>	The Statutory Information Officer for a Group Company.
<b>Group Function(ary)</b>	A centralised function in the Santam Group Office that includes strategic direction, financial and risk management, compliance, internal audit, tax services, group actuarial, market development, stakeholder management, brand and communications, group human resources, information technology (GTI) and corporate social investment.
<b>Group Information Officer</b>	The Statutory Information Officer for Santam Limited.
<b>GTI</b>	Santam Group Technology and Information.

# Santam Group

## Privacy Policy

DEFINITION	DESCRIPTION
<b>Legitimate Basis</b>	Any legitimate basis for the Processing of Personal Information recognised by applicable Data Protection Laws including where – <ul style="list-style-type: none"> <li>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</li> <li>the Processing complies with an obligation imposed by law on the Responsible Party; or</li> <li>the Processing protects a legitimate interest of the Data Subject; or</li> <li>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</li> <li>the Data Subject, or the parent, legal guardian (or other competent person) where the Data Subject is a Child, Consents to the Processing.</li> </ul>
<b>LIA</b>	A legitimate interest assessment which should be undertaken by a Group Company where such Group Company is relying on its (or a third party recipient's) legitimate interests as the Legitimate Basis for Processing. Such LIA should include: <ul style="list-style-type: none"> <li>determining the purpose of the Processing, which purpose must be specific, explicitly defined and lawful;</li> <li>determining whether the Processing is necessary to achieve the purpose identified; and</li> <li>undertaking a balancing exercise to determine whether the Data Subject's rights and freedoms override the legitimate interests.</li> </ul>
<b>Operator</b>	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.
<b>Operator Agreement</b>	A written agreement (or clauses within a broader written agreement) to be concluded between: <ul style="list-style-type: none"> <li>a Group Company and an Authorised Third Party, which regulates the manner in which an Authorised Third Party, acting as an Operator, Processes Personal Information for a Group Company, acting as a Responsible Party; or</li> <li>a Group Company and another Group Company, which regulates the manner in which one Group Company, acting as an Operator, Processes Personal Information for the other Group Company, acting as a Responsible Party.</li> </ul>
<b>Personal Information</b>	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 Santam Group carrying out its operations.
<b>POPIA</b>	The South African Protection of Personal Information Act, No. 4 of 2013.
<b>Process/Processing</b>	Any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information, including – <ul style="list-style-type: none"> <li>the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;</li> <li>dissemination by means of transmission, distribution or making available in any other form; or</li> <li>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.</li> </ul>
<b>Responsible Party</b>	Where a 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.
<b>Santam</b>	Santam Limited



# Santam Group

## Privacy Policy

DEFINITION	DESCRIPTION
<b>Santam Group</b>	Santam Limited and all subsidiaries of Santam Limited as well as subsidiaries of subsidiaries.
<b>Santam Limited Insurance sub-Group</b>	The insurance sub-group designated under the South African Insurance Act, No. 18 of 2017.
<b>Security Event</b>	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.
<b>Special Personal Information</b>	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.
<b>Staff</b>	In relation to a Group Company, all employees (whether permanent or temporary), directors, officers, natural persons acting as contractors under the authority of a Group Company and other staff of such Group Company.
<b>Statutory Information Officer</b>	Where Data Protection Laws require a Group Company to register an information officer with a Supervisory Authority, the individual registered as such from time to time.
<b>Supervisory Authority</b>	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.