NEW NATIONAL
ASSURANCE COMPANY
People you can talk to.

PROTECTION OF PERSONAL INFORMATION POLICY & MANUAL V1

Version history	
V1	Board Approved May 2021

For Confirmation by Board| Last updated: April 2021

Board Approval required on:

Protection of Personal Information Policy	Management Recommendation 2021
Protection of Personal Information Policy Document	As Detailed

TABLE OF CONTENTS

1. INTRODUCTION

The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 (POPIA)

POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner.

A person's right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions.

Given the importance of privacy, we are committed to effectively managing personal information in accordance with POPIA's provisions.

2. DEFINITIONS

The following terms may be defined as:

2.1 Biometrics- Means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, finger printing, DNA analysis, retinal scanning and voice recognition.

2.2 Consent- Means any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information.

2.3 Data Subject- This refers to the natural or juristic person to whom personal information relates, such as an individual client, customer or a company that supplies us with products or other goods and services.

2.4 De- Identify- This means to delete any information that identifies a data subject, or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.

2.5 Filing System- Means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

2.6 Information Officer- The information officer is responsible for ensuring our compliance with POPIA.

2.7 Operator- An operator means 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 party.

2.8 PAIA – Promotion of Access to Information act No 2 of 2000.

2.9 Personal Information- Personal information is any information that can be used to reveal a person's identity. Personal Information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person. (Such as a company), including but not limited to information concerning:

- Race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language, and birth of a person.
- Information relating to the education or the medical, financial, criminal or employment history of the person.
- Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier, or other assignment to the person.
- The biometric information of the person.
- The personal opinions, views, or preferences of the person.
- The views or opinions of another individual about the person.

2.10 **Persons –** Maybe defined as a human being or a corporation having rights and obligations of a person.

2.11 POPI Act- The POPI (Protection of Personal Information) Act of 2013, also called POPIA, is a piece of legislation introduced to try and protect the constitutional right to privacy by implementing rules designed to protect private information.

2.12 Policy Application- This Policy applies to NNAC's Board of Directors, all branches, business units and divisions of the Company, All employees and Management, All business partners or other persons acting on behalf of the Company.

2.13 Policyholder- A policyholder is a person or entity whose name appears on the records of the insurance company and is also a person or entity who owns or controls an insurance policy and has the privilege to exercise the rights outlined in the contract.

2.14 Primary Purpose- The collection of data for its intended use.

2.15 Processing- The act of processing information includes any activity or any set of operations, concerning personal information and includes:

- 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
- Margining, linking, as well as any restriction, degradation, erasure, or destruction of information.

2.16 Record- is any recorded information, regardless of form or medium, including:

- Writing on any material
- Information produced, recorded, or stored by means of any tape- recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored.

2.17 Re- Identify- In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

2.18 Responsible Party- The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case, NNAC is the responsible party.

2.19 Secondary Purpose- is the use or disclosure of information for a purpose other than that for which it was originally collected.

2.20 Third Party - relating to a person or group besides the two primarily involved in a situation.

2.21 Unique Identifier- any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

3 PURPOSE

The purpose of this policy is to protect NNAC from the compliance risk associated with the protection of personal information which includes:

- Breaches of confidentiality. For instance, we could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.
- Failing to offer choice. For instance, all data subjects should be free to choose how and for what purpose the company uses information relating to them.
- Reputational damage. For instance, we could suffer a decline in Policy Holder value following an adverse event such as a computer hacker deleting the personal information held by the company.

This policy demonstrates our commitment to protecting the privacy rights of data subjects in the following manner:

- Through directing compliance with the provisions of POPIA and best practice.
- By cultivating a company culture that recognises privacy as a valuable human right.
- By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.

- By assigning specific duties and responsibilities to the Board of Directors, including the appointment of an Information Officer and Deputy Information Officers to protect the interests of our Company and data subjects.
- By raising awareness through training and providing guidance to staff who process personal information so that they can act confidently and consistently.

4 APPLICATION

This policy and its guiding principles apply to:

- NNAC's Board of Directors
- All branches, business units and divisions of the Company.
- All employees and Management
- All business partners or other persons acting on behalf of the Company.

The policy's guiding principles find application in all situations and must be read in conjunction with the POPIA as well as our PAIA policy as required by the Promotion of Access to Information Act No 2 of 2000.

POPIA does not apply in situations where the processing of personal information:

- Is concluded during purely personal or household activities or
- Where the personal information has been de-identified

5. RIGHTS OF DATA SUBJECTS

Where appropriate, we will ensure that our clients and customers are made aware of the rights conferred upon them as data subjects.

NNAC ensures that it gives effect to the following six rights:

5.1 The Right to Access Personal Information

We recognise that a data subject has the right to establish whether the company holds personal information related to him or her or it includes the right to request access to that personal information.

5.2 The Right to have Personal Information Corrected or Deleted

The Data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where we are no longer authorised to retain the personal information.

5.3 The Right to Object to the Processing of Personal Information

The data subject has the right to object to the processing of his, hers or its personal information.

In such circumstances, we will give due consideration to the request and the requirements of POPIA. The company may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal Information.

5.4 The Right to Object to Direct Marketing

The data subject has the right to object to the processing of his, hers or its personal information for purposes of direct marketing by means of unsolicited electronic communications.

5.5 The Right to Lodge a Complaint with the Information Regulator

The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non- compliance with the protection of his, her or its personal information.

5.6 The Right to be Informed

The data subject has the right to be notified that his, her or its personal information is being collected by us.

The data subject also has the right to be notified in any situation where the company has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

6 GENERAL GUIDING PRINCIPLES IN TERMS OF THE ACT

All employees and persons acting on behalf of the company are to adhere to the following guiding principles:

6.1 Accountability

Failing to comply with POPIA could potentially damage NNAC's reputation or expose us to a damage's claim. The protection of personal information is therefore the responsibility of any person associated with NNAC i.e.: Employees and Business partners.

We will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with. However, failure to comply, we will be obliged to administer appropriate sanctions, which may include disciplinary action, against those employees who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

6.2 Processing Limitations (Primary Purpose)

NNAC ensures that personal information under its control is processed:

- In a fair, lawful, and non-excessive manner and,
- Only with the informed consent of the data subject, and

- Only for a specifically defined purpose.

We will inform the data subject of the reasons for collecting his, her or its personal information and obtain written consent prior to processing personal information.

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

Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other aspects of the company's business and be provided with the reasons for doing so.

6.3 Purpose Specification

We will process personal information only for specific, explicitly defined, and legitimate reasons.

In the event of data being retained or stored, we will inform data subjects of our reasons for retention and storage.

6.4 Further Processing Limitation (Secondary Purpose)

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose. Secondary Purpose may be referred to the use or disclosure of information for a purpose other than that for which it was originally collected.

Therefore, consent will be obtained from the data subject.

6.5 Information Quality

We will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading.

Where personal information is collected or received from third parties, we will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject.

6.6 Open Communication

We will take reasonable steps to ensure that data subjects are notified that their personal information is being collected including the purpose for which it is being collected and processed.

6.7 Security Safeguards

We will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls have been implemented to minimise the risk of loss, unauthorised access, disclosure, interference, modification, or destruction.

NNAC continuously reviews its security controls which includes regular testing of protocols and measures put in place to combat cyber- attacks on our IT network.

We ensure that all paper and electronic records comprising of personal information are securely stored and made accessible only to authorised individuals.

All new employees will be required to sign employment contracts containing contractual terms for use and storage of employee information. Confidentiality clauses will be included to reduce the risk of unauthorised disclosures of personal information for which we are responsible.

6.8 Data Subject Participation

A data subject may request the correction or deletion of his, hers or its personal information held by us.

We will ensure that it provides a facility for data subjects who want to request the correction or deletion of their personal information.

7 INFORMATION OFFICER

We have appointed an Information officer and a Deputy Information Officer to assist the Information officer.

The Information Officer is Mr Kalim Rajab, and the Deputy Information Officer is Ms Vicky Lakhraj. The contact details for the Information Officer is krajab@nnac.co.za and Deputy Information Officer is vicky@nnac.co.za

The Information Officer and Deputy Information Officer is responsible for ensuring compliance with POPIA.

The Information Officer and Deputy Information Officer will be registered with the South African Information Regulator established under POPIA prior to performing his or her duties.

8 SPECIFIC DUTIES AND RESPONSIBILITIES

8.1 NNAC's Board of Directors

The Board of Directors cannot delegate its accountability and is ultimately responsible for ensuring that we comply with the requirements of POPIA.

The Board may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

The Board of Directors are responsible for ensuring:

- NNAC appoints an Information Officer and a Deputy Information officer.
- All persons responsible for the processing of personal information on behalf of the Company:
  - Are appropriately trained and supervised to do so.

- Understand that they are contractually obligated to protect the personal information they encounter, and
- Are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.

- Data subjects who want to make enquiries about their personal information are made aware of the procedure that needs to be followed should they wish to do so.

8.2 Information officer

NNAC's Information Officer is responsible for:

- Taking steps to ensure compliance with the provision of POPIA.
- Keeping the Board of Directors updated on our information protection responsibilities under POPIA.
- Ensuring POPI audits are scheduled and conducted on a regular basis.
- Ensuring that we make it convenient for data subjects who want to update their personal information.
- Encouraging compliance with the conditions required for the lawful processing of personal information.
- Ensuring that employees and person's acting on behalf of the Company are fully aware of the risks associated with the processing of personal information and that they remain informed about our security controls.
- Working with the Information Regulator in relation to any on-going investigations, the Information Officer will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate on any other related matter.

The Deputy Information Officer will assist the Information Officer in performing his duties.

8.3 Head of IT

NNAC's IT manager is responsible for:

- Ensuring our IT infrastructure, filing systems and any other devices used for processing personal information meets acceptable security standards.
- Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services.
- Ensuring that all electronically stored personal information is backed up and tested on a regular basis.
- Ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious hacking attempts.
- Ensuring that personal information being transferred electronically is encrypted.

- Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.
- Performing regular IT checks to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.
- Performing regular IT checks to ensure that the security of our hardware and software systems are functioning properly.
- Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on our behalf. For instance, cloud computing services.

8.4 Responsibility of Employees and other Persons acting on behalf of NNAC.

Employees and other persons acting on behalf of the Company may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the company or externally, any personal information, unless such information is already publicly known, or the disclosure is necessary in order for the employee or person to perform his or her duties.

Employees and other persons acting on behalf of NNAC will only process personal information 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.
- The processing protects a legitimate interest of NNAC or of a third party to whom the information is supplied.

Furthermore, personal information will only be processed where the data subject:

- Clearly understands why and for what purpose his, her or its personal information is being collected, and
- Has granted us explicit written or verbally recorded consent to process his, her or its personal information.

Consent can be obtained in written form alternately; we will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

Employees and other persons acting on behalf of NNAC will under no circumstances:

- Process or have access to personal information where such processing or access is not a requirement to perform their respective work- related tasks or duties.
- Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones.
- Share personal information informally. Personal information should never be sent by email, other than to the data subject.

Employees and other persons acting on behalf of NNAC are responsible for:

- Keeping all personal information that they encounter secure, by taking sensible precautions and following guidelines outlined in this policy.
- Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.
- Taking reasonable steps to ensure that personal information is kept accurate and up to date.

Where an employee and other persons acting on behalf of NNAC, become aware or suspicious of any security breach such as unauthorised access, interference, modification, destruction, or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer or the Deputy Information Officer.

9 REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

Data subjects have the right to:

- Request what personal information we holds about them and why.
- Request access to their personal information.

Access to information can be made by email, addressed to the Information Officer. The Information Officer will provide the data subject with a “Personal Information Request Form”.

Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information.

The information Officer will process all requests within a reasonable time.

10 DISCIPLINARY ACTION

Where a POPI complaint or a POPI infringement investigation has been finalised, we may recommend any appropriate legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non- compliant activity outlined within this policy.

Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which we may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee’s gross negligence.

11 POPI COMPLAINTS PROCEDURE

Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon.

All complaints submitted in writing will be considered by the Information Officer.

Where the data subject is not satisfied with the Information Officers determination, the data subject has the right to complain to the Information Regulator.

12. ANNEXURE A: PERSONAL INFORMATION REQUEST FORM

Please submit the completed form to the Information Officer	
Name	
Contact number	
Email address	

Please be aware that we may require you to provide proof of identification prior to processing your request.

A. Particulars of Data Subject	
Name & Surname	
Identity Number	
Postal address	
Contact number	
Email address	

B. Request		
I request the organisation to:		
(a) Inform me whether it holds any of my personal information		
(b) Provide me with a record or description of my personal information		
(c) Correct or update my personal information		
(d) Destroy or delete a record of my personal information		

C. Instructions

D. Signature
Signature:
Date:

13. CONSENT FORM: CONSENT TO PERSONAL INFORMATION

I, _____as the data subject, by signing this document, hereby consents to the use of my personal information contained herein and confirms that:

1. The information is supplied voluntarily, without undue influence from any party and not under any duress,
2. The information which is supplied herewith is mandatory for the purposes of this agreement and that without such information, New National Assurance Company will not be able to fulfil their obligations.

The data subject acknowledges that he/she is aware that he/she has the following rights with regards to such personal information which is hereby collected.

The right to:

1. Access the personal information at any reasonable time for the purposes of rectifications.
2. Object to the processing of the personal information
3. Lodge a complaint with the Information Regulator

Thus, signed on this _____ day of _____ 20___.

_____

SIGNATURE