RetirementSA

Redefining Retirement

Protection of Personal Information
Compliance & Risk Management Plan

Information Officer | MC van Rooyen

Definitions	
Company	**Ukholo Property Consultants** and **Developments & Retirement Villages SA** Pty Ltd (referred to as either "Nationlink", "RetirementSA", "the Company", "We", "Us" or "Our" in this Agreement).
Cookies	Files containing the information of the user (such as yourself) which are stored on devices, websites and apps containing information which includes information from your browser history.
Data Subject	The natural person or juristic person whose information is submitted and retained by the company.
Device	Any device (computer, cell phone, tablet) which the consumer, uses to access our platform or to communicate with us.
Information Officer	Compliance Officer, MC van Rooyen, as per the Protection of Personal Information Act.
Personal Information / Data	May include, but not limited to any information which can identify an individual (natural) or juristic person (Close Corporation, Company), partnership or trusts. This also includes telephone numbers, addresses, locations, email addresses, biometric data and demographic data. Basically, any information that can identify an individual or juristic person.
Responsible Party	Nationlink & RetirementSA.
Third party service providers	Any third party contracted by Nationlink & RetirementSA to assist with the acquiring, processing, management, or destruction of, but not limited to personal information, held by Nationlink & RetirementSA.
Usage Data	This is data which is collected automatically when a person uses our website, any applications, such as: • device's internet protocol address (IP address) • browser type • browser version • which of our pages you visit, as well as the dates, times and time spent per page • unique device identifiers • diagnostic data In terms of app usage, data includes, but is not limited to: • type of device • device unique ID • the IP address of the mobile device • mobile operating system • browser type • unique device identifiers • diagnostic data
Website	**www.nationlink.co.za** & **www.retirementsa.com** It includes any other sites which may be registered from time to time by the companies.
You	The person/ individual who submits their information via any one of our platforms, via email, application or telephonically.

For the purpose of this document "Data" refers to any and all "Personal Information" and vice versa

Purpose & Scope

The purpose of this compliance and risk management plan is to ensure the Nationlink & RetirementSA lawfully obtains, process, retains and destroys personal information of Data Subjects, in line with the Protection of Personal Information Act, 4 of 2013.

The Protection of Personal Information Act 4 of 2013 aims:

- to promote the protection of personal information processed by public and private bodies;
- to introduce certain conditions so as to establish minimum requirements for the processing of personal information;
- to provide for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of this Act and the Promotion of Access to Information Act, 2000;
- to provide for the issuing of codes of conduct;
- to provide for the rights of persons regarding unsolicited electronic communications and automated decision making;
- to regulate the flow of personal information across the borders of the Republic; and
- to provide for matters connected therewith.
  https://www.gov.za/documents/protection-personal-information-act?gclid=Cj0KCQiApsiBBhCKARIsAN8o_4j9UTV28JZY74LbUMQTukrsldWkyX1C-4IM_2y4WhoWvxaCnCMtcm4aAg4tEALw_wcB#

During the day-to-day operations of the agency, it gathers personal information from data subjects to conduct a real estate service.

This document outlines how Nationlink & RetirementSA will source, process, retain, transfer and destroy personal information of both natural and juristic persons/ Data Subjects.

A Data Subject is defined as any person, business, legal entity or organisation who/which provides personal information to Nationlink & RetirementSA, the Responsible Party.

Personal Information is defined as any information, as listed below, but not limited to, which can identify a Data Subject:

- information relating to race, gender, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, wellbeing, disability, religion, conscience, belief, culture, language and birth of the person, medical information and financial information
- education, medical, financial, criminal or employment history of a person
- any identity number, symbol, email address, physical address, telephone number, location information, online identifier, or other assignment to the person
- the biometric information of a person
- the personal opinions, views, or preferences of a person
- correspondence sent by a person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence.
- the views or opinions of another individual about the person; and
- the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

Direct marketing means to approach 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
- request the data subject to make a donation of any kind, for any reason.

Electronic communication means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

Any Data subject has the right to request that the Responsible Party correct, destroy, or delete his/ her personal info, provided that the personal info is:

- inaccurate
- irrelevant
- excessive
- out of date
- incomplete
- misleading
- has been unlawfully obtained.

OR in the case of the responsible party is no longer authorised to keep the personal info (Section 14)

When deleting or destroying data/ info the onus is on the responsible party to ensure that the info cannot be reconstructed into an intelligible form so that it can be used after it has been destroyed.

As part of the mitigation of risk process, the Information Officer, will do ongoing assessments of the processed and security measures in place to ensure compliance. As part of this process, staff will also receive ongoing training.

The processes implemented will apply to both the business information, such as human resources, management, financial, legal, compliance, operations, sales and marketing, as well as technological information (IT), AND information procured during the course of providing real estate services, which includes the personal information of Data Subjects, such as existing clients, historical clients, information passed on to Nationlink & RetirementSA from third parties and information obtained via subscription services.

Roles & Responsibilities

Nationlink & RetirementSA is owned and managed by Marelize van Rooyen, who manages all aspects of compliance for the business. As Information Officer, the assessment, implementation, and maintenance of the POPIA policies, compliance and risk management falls within her ambit and responsibility.

All staff and agents are to adhere to the prescribed policies and procedures outlined in the POPIA compliance and risk management plan, as well as:

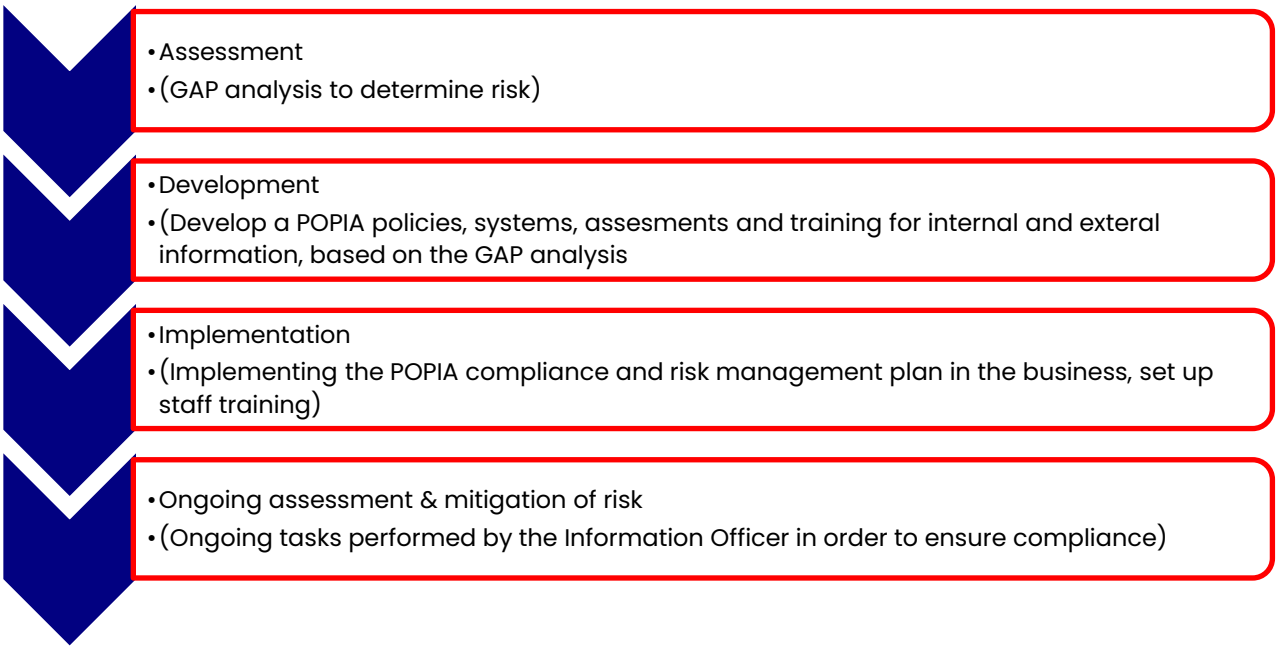
- Protection of Personal Information Act,4 of 2013,
- Electronic Communications and Transactions Act, 25 of 2002
- Consumer Protection Act, 68 of 2008
- Financial Intelligence Centre Act, 38 of 2001
- Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 33 of 2004
- Prevention of Organised Crime Act, 121 of 1998
- Estate Agency Affairs Act, 112 of 1976
- Estate Agents Code of Conduct

Should any employee or estate agent be found guilty, after investigation of any contravention of the company policy or procedures contained herein or in any of the above-mentioned pieces of legislation, the guilty party will be subject to dismissal, or any form of action found reasonable, including reporting to the local authorities and/or regulatory bodies, by the business owner.

Contravention, even if done so in negligence, is a serious offence.

Any data breach will have to be reported to the Information Regulator and affected Data Subjects by the Information Officer.

The process of setting up, managing and general compliance with POPIA, will be done in a systematic manner from February 2021, to meet the compliance deadline on 30 June 2021. As of 01 July 2021, the focus will shift from implementation to maintenance and general ongoing compliance in terms of POPIA.



It is the responsibility of all agents and staff to ensure that the prescribed email signature with the relevant disclosure and privacy policy is displayed an all-outgoing email, whether the email be of a business or private nature.

The required disclosures and privacy policies will also be visible on the company website.

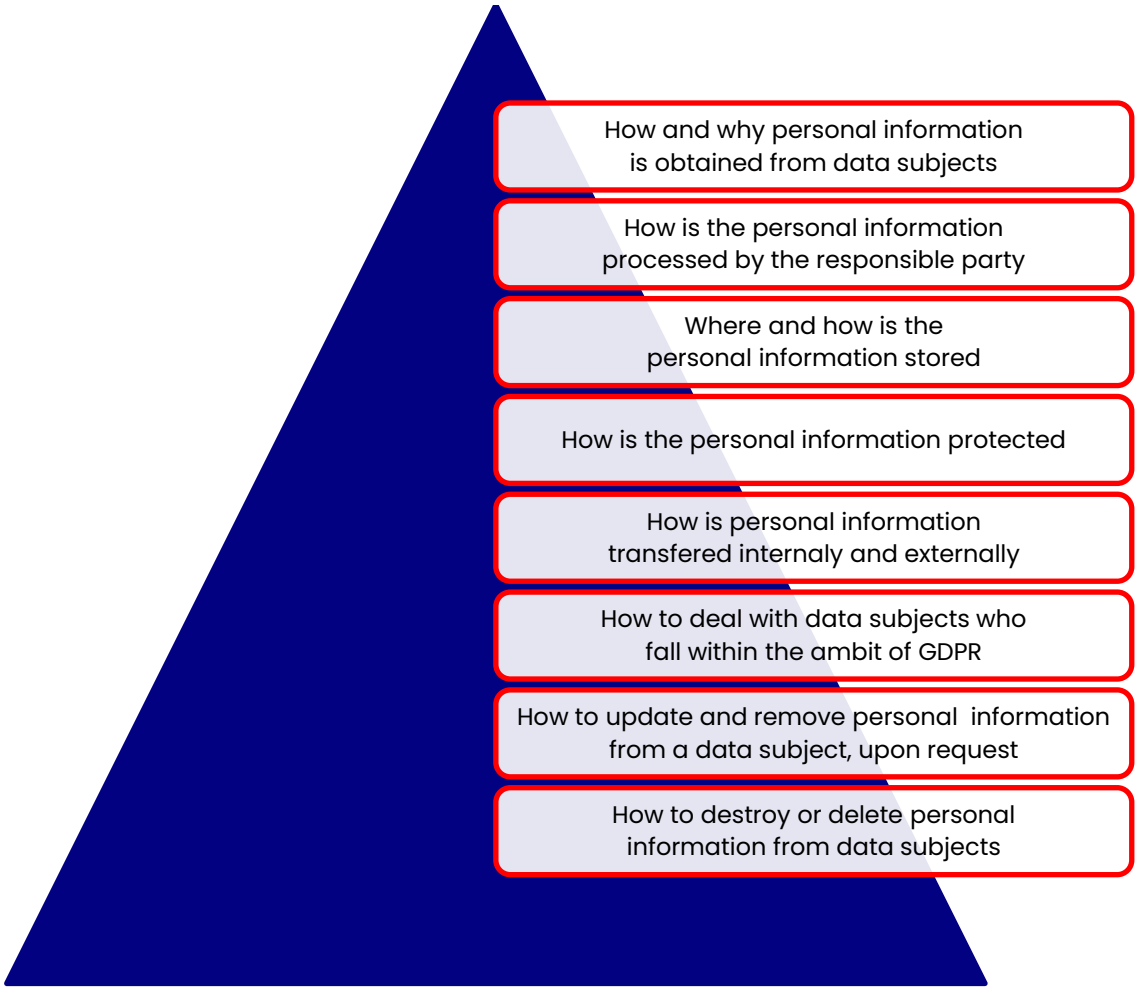
When obtaining personal information from any Data Subject, the employee or agent ensure that the Data Subject has completed the correct form, granting permission for his/ her personal information to be processed and retained by the company.

Without this consent, the personal information of the Data Subject may not be processed. In the case of a Data Subject requesting corrections, updates or removal of his/her personal information, the employee or agent must forward that request (by means of a completed form) on to the Information Officer for processing. Only the Information Officer may make changes to the database.

Any changes or deletion of the personal information of a Data Subject will be confirmed by the Information Officer to the Data Subject.

It is the responsibility of the Information Officer to ensure that all changes and deletions are done in accordance with the prescribed outlined in POPIA.

Outline of the PoPIA Compliance and Risk Management Plan



This compliance and risk management plan also extends to the prevention of:

- Unauthorised access to personal information
- Unlawful processing of personal information
- Unlawful deletion or destruction of personal information, or any data, where it be accidental or on purpose by any employee, agent or management of the business.

It further extends to the usage and protection personal devices deemed a work device.

Lawful Purpose for Obtaining Personal Information

- There must always be a lawful purpose for obtaining and processing personal information of Data Subjects by the Responsible Party.

Permission to Process Personal Information of Data Subjects

- Data Subject must, post implementation of this compliance and risk management plan obtains written consent from the Data Subject, BEFORE processing his/her personal information. Without written consent, the information may not be processed.
- The Data Subject must consent to providing their personal information for a specific use, i.e., direct marketing consent or for the purposes of identification and verification for any of the anti-money laundering purposes, OR for the purposes of conducting a real estate transaction.
- The Data Subject must consent to receiving direct marketing via specific channels/ platforms, to which the Responsible Party must adhere to.

Quality of Personal Information Obtained

- The onus is on the Responsible Party to ensure the quality of information procured, processed, and retained. The updating of records and information is the responsibility of the Information Officer. This also includes information received from third parties.

Purpose for Obtaining Personal Information of Data Subjects

- Personal Information of Data Subjects must be obtained for a specific purpose by lawful means.
- Personal Information may not be obtained in excess for unspecified future use. Only the required information may be obtained, processed, and retained.
- As of the 1st of July 2021, all new Data Subjects must formally opt in for marketing material to be sent on to them.

The conditions for the lawful processing of personal information & collection of data

Definition of Personal Information as stated in the POPI Act:

"personal information means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

- information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the 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 particular assignment to the person;
- the biometric information of the person;
- the personal opinions, views or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the person; and
- the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;"
- Personal information further extends to financial and medical information of Data Subjects as well as to surety on lease agreements.

Conditions for the Processing of Personal Information

1. •Accountability
2. •Data Subject Particpation
3. •Purpose Specific
4. •Processing Limitations
5. •Further Processing Limitations
6. •Information Quality
7. •Openness
8. •Safeguards

✓ Accountability

The onus rests with the Responsible Party to comply in full with the Protection of Personal Information Act (POPIA), to ensure that the conditions for the processing of personal information, as set out in the Act, is complied with in full.

It is the responsibility of the appointed Information Officer to ensure that the required mechanisms are in place to ensure that the processing of personal information is done in compliance with the Act and as per the company POPIA policies and protocols.

✓ Data Subject Participation

The Information Officer must ensure that there are processes in place whereby Data Subjects may request:

- whether their personal information is retained by the Responsible Party, and/ or
- which of their personal information is held, and/or
- for the correction and/or deletion of any personal information held about them.

The Information Officer must also ensure that there are proper communication channels in place to allow for direct communication with Data Subjects.

✓ Purpose Specification

The processing of personal information is only permitted when the data was collected by legitimate means and for a specific lawful purpose, related to the functions of the Responsible Party.

The following must be adhered to:

- The Data Subject must be aware of the purpose for the data collection.
- The purpose for the data collection must be unambiguous.
- The retention of the data may not be longer than required by law, in the case of data collected for the purposes of anti-money laundering legislation (AML) compliance, such as FICA, POCA and POCDATARA, the period is outlined as 5 years.
- Records of the use of personal information must be retained by the Responsible Party in order for the Data Subjects to request access thereto. The period of retention of such records are 5 years.
- The deletion/removal/destruction of personal information of a Data Subject must be done within 1 working day after receiving the instruction from the Data Subject.
- Personal information earmarked for destruction, must be destroyed in a manner preventing it from being reconstructed in any way in order to identify a Data Subject.

✓ Processing Limitations

Personal information may only be processed in a fair and lawful manner, and only with the consent of the data subject.

- The collection of personal data must be for a specific purpose in line with the nature and daily operations of the Responsible Party.
- The collection of data must be proportionate to its purpose.
- The collection of data must be directly from the Data Subject (source), unless the information is obtained from a public record, such as the Deeds Office or municipality, or third-party service providers such as CMA Info, Lightstone or Windeed, which collects their source information from public records in the Deeds Office, or in the case where a Data Subject has volunteered the data via a public forum or social media platform.

The transfer of personal information must be limited to:

- The internal transfer of data within the business, for business purposes, or
- The transfer to third parties, such as conveyancers and other parties to a contract, for the purposes of concluding a lease agreement or the sale of immovable property.

Any Data Subject may at any given time object to the processing of his/her/their personal information, via the prescribed manner. The opting out must be done by completing the prescribed form and sending it on the Information Officer.

✓ Further Processing Limitations

The Responsible Party must take steps to prevent the further processing of personal information. Data may not be processed for a secondary purpose unless that processing is compatible with the original purpose for which it was obtained.

The further processing of data must be in line with all the contractual obligations and rights of the Data Subject.

An allowance is made for the retention of historical data, for statistics and research purposes only.

The Information Officer must ensure that any data mining does not exceed its original purpose and that any unlawful processing is stopped.

✓ Information Quality

The Responsible Party must ensure that the personal information collected are:

- accurate
- not misleading
- up to date
- does not include any unnecessary records
- are secure and access controlled

The Responsible Party must be aware of the impact the quality of personal information has on the purpose for collection.

✓ Openness

The Data Subject must always be aware of the processing of their personal information and for which purposes the information will be processed.

The Responsible Party must be identifiable (name & address) to the Data Subjects unless:

- the data subject has already been made aware of this,
- the information was obtained from public records, or
- the information will be used without identifying the Data Subject.

✓ Safeguards

Data must be protected against the risk of data breach, data loss, unlawful access, interference, modification, unauthorized destruction and disclosure.

The Responsible Party must maintain:

- The appropriate access limitation/control to personal information
- Employ the appropriate information systems and information technology safeguards for all devices (including but not limited to cell phones, tablets, computers, laptops), as well as information kept in hardy copy format. These safeguards include but not limited to the installing anti-virus, antimalware and anti-spam software on all devices, and installing physical access control mechanisms such as locks on cabinets, drawers and cupboards where records and data are kept. This should be in line with the record keeping prescriptions outlined in the Financial Intelligence Centre Act, 38 of 2001, and its amendment.
- The software updates as required by the service provider to ensure effective data protection.

It is also the responsibility of the Responsible Party to actively prevent data breaches of any and all data and ensure that there are sufficient data breach detection in place.

The Responsible Party is to review the contractual obligations of third-party service providers in order to ensure continued compliance with the Act. These would include, but not limited to:

- Advertising platforms i.e. Property24, Private Property, IOL Property, Gumtree
- Lead Generation platforms/ applications
- Data storage providers
- Data protection providers
- Data processing or verification providers i.e. TPN, PayProp, Rental Connect, RentMaster, Rentbook
- Immovable property information services i.e. Lightstone, CMA Info, Windeed

The Information Officer must ensure compliance with the collection, processing, retention, and destruction of data as outlined in the Act.

Privacy Policy – Website Display

We value our clients and respect their privacy. Outlined below is the Nationlink & RetirementSA privacy policy, outlining our commitment to procuring and managing information responsibly, as per the Protection of Personal Information Act.

Our policy makes for the provision for the procedures whereby we collect personal information, how we process, use the information, and under which circumstances we share your information and with whom, as well as the destruction of information procedures.

Clients retain the right to **update, remove or destroy** the information we retain for purposes *other* than those mandated, but not limited to, in the following acts:

- Financial Intelligence Centre Act, 38 of 2001 (FICA),
- The Prevention of Organised Crime Act, 112 of 1998,
- The Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 2004 (POCDATARA)

In our course of business, we collect information for the purpose of

- Marketing
- Concluding formal real estate transactions
- Marketing Research
- Statistical Analysis

We do not share information with any third parties unless we have the written instruction from clients to do so.

Types of information collected:

- Personal Information
- Usage Data

Our website does make use of cookies, view the Property24 cookie policy on https://www.property24.com/cookie-policy

Personal Data - Use

The Company may use Personal Data for the following purposes:

- Real Estate Contracts (Sale Agreements/ Offer to Purchase/ Mandates/ Leases)
- Contacting clients via electronic communication (i.e. email, SMS, app-based communication), telephonically, app notifications and postal services.
- Update clients/ subscribers with the latest news, important information and services.
- Survey and poll to track industry trends, service delivery and client satisfaction.
- Market research.

Personal Data – Sharing

In a real estate transaction, we are obligated to share certain information with third parties, such as conveyancers, other parties to a transaction in a contract, service providers for the purposes for delivering services, other agents, or in the case of an emergency. For these purposes, we will require your written consent at the commencement of the business relationship.

Data storage & processing

We retain information/ data pertaining to real estate transactions for a period of 5 years after the completion of the transaction, as per the Financial Intelligence Centre Act. After the 5-year period, the documentation and digital copies are destroyed.

Transactional copies are kept indefinitely unless specifically requested to do so by either of the parties to the agreement.

Data kept on our marketing database, consisting of names, surnames, addresses, telephone numbers, date of birth and email addresses, are kept indefinitely. The information is stored securely on a digital platform and only two members have access. Clients always have the option to opt out of any marketing database. In the case of a client opting out, we remove that client immediately from all our platforms.

Personal Data, is processed at the Nationlink & RetirementSA office and any satellite offices as well as any other places where the owner (or staff) involved in the processing, are located.

This implies that information may be transferred to, maintained on, or destroyed from computers and devices located outside of the province, country, or other governmental jurisdiction with other data protection laws, which may differ from those where the client is located.

Nationlink & RetirementSA will take all reasonable steps to ensure that all client data is treated in accordance with the Protection of Personal Information Act, and always with the utmost respect for the client's privacy and safety.

Disclosure

Anti-Money Laundering

As Accountable Institutions, Nationlink & RetirementSA is required by law to submit reports to the Financial Intelligence Centre, such as Cash Threshold Reports, Suspicious Persons or Suspicious Transaction reports.

Legal obligations

When requested we will disclose personal information if we need to:

- Lodge a defence in a legal case.
- Protect us against liability.
- Prevent an illegal transaction or activity.
- Prevent any money laundering or terrorist funding.
- Assist the South African Police Service, or any crime intelligence service of South Africa, or the National Prosecuting Authority, when a court order instructs us to do so.

Security of Your Personal Data

We endeavour to always treat your personal data as our own and never purposefully place your information at risk. That said, please note that we use commercial software and electronic storage applications and are in that respect dependent on the built-in protection of those applications and services.

Privacy Policy – Email Disclosure

The content of this e-mail, and any attachments, is strictly confidential and solely for the use of the intended recipient(s). Please notify the sender immediately by email if you have received this email by mistake and delete this email from your system. If you are not the intended recipient, you are notified that disclosing, copying, distributing, or taking any action in reliance on the contents of this information is strictly prohibited.

Any views or opinions presented in this email are solely those of the author and do not necessarily represent those of RetirementSA. RetirementSA accepts no liability for the content of this email, or for the consequences of any actions taken on the basis of the information provided, unless that information is subsequently confirmed in writing.

POPI Information Officer: Marelize van Rooyen MPRE
Email: popi@nationlink.co.za or popi@retirementsa.com | Mobile: +27 82 440 0030 or WhatsApp
PoPI Policies Manual: www.nationlink.co.za or www.retirementsa.com

By law, this agency is required as an accountable institution to comply with legislative requirements such as outlined in the FIC Act 38 of 2001 and the Financial Intelligence Centre Amendment Act of 2017. This includes the mandatory process of identifying and verifying all parties to a real estate transaction and implementing the risk-based approach and client due diligence process. For more information visit the FIC section on our website.

FIC Compliance Officer: Marelize van Rooyen MPRE
Email: fic@nationlink.co.za or fic@retirementsa.com | Mobile: +27 82 440 0030 or WhatsApp
FIC Policies Manual: www.nationlink.co.za or www.retirementsa.com

Issued by
Marelize van Rooyen
Information Officer
29 June 2021