POPI Website Policy

GL Insurance Brokers

AFSP (License 169147)

CK no 1995/010714/23

Cnr Main road & Kremetart Ave, Eldorado Park, Soweto, 1811

Website(s) Privacy Terms & Protection of Personal Information ("POPI") Policy

Our Website(s):

glinsurance.co.za

Our Email Address: info@glinsurance.co.za

Tel: +27 11 945 5151

Last updated: 29 March 2022

Whereas the Company respects the privacy of all personal data and private information collected, processed and stored. As such, we undertake to handle all personal information received and processed with due care and provide the necessary security to safeguard all information held by us. Our internal system similarly allows us to proactively react should there be a breach of any kind, alternatively our privacy practices and POPI policy dictates that we report any material breach to the Regulator.

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 ("POPI Act").

The POPI Act 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. Through the provision of quality goods and services, the organization is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees, and other stakeholders.

A person's right to privacy entails having control over his or her personal information, being able to conduct her or her affairs relatively free from unwanted intrusions. Given the importance of privacy, the organisation is committed to effectively managing personal information in accordance with the POPI Act's provisions.

2. DEFINITIONS

2.1 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:

2.1.1 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 person;
2.1.2 Information relating to the education or medical, financial, criminal or employment history of the person;
2.1.3 Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or another particular assignment to the person;
2.1.4 Biometric information of the person;
2.1.5 The personal opinions, views or preferences of the person;
2.1.6 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;
2.1.7 The views or opinions of another individual about the person;
2.1.8 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.

2.2 Data Subject: this refers to the natural or juristic person to whom the personal information relates, such as an individual client, customer or company that suppliers the organization with products or other goods.

2.3 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, the organization is the responsible party.

2.4 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. For example, a third-party service provider that has contracted with the organization to shred documents containing personal information. When dealing with an operator. It is considered good practice for a responsible party to include an indemnity clause.

2.5 Information Officer: the information officer is responsible for ensuring the organization's compliance with the POPI Act. Where no information officer is

appointed, the head of the organization will be responsible for fulfilling the information officer's duties. Once appointed, the information officer must be registered with the South African Information Regulator established under the POPI Act prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.

2.6 Processing: the act of processing information includes any activity or any set of operations, whether by automatic means, concerning personal information and includes:

2.6.1 The collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use;
2.6.2 Dissemination by means of transmission, distribution or making available in any other form; or
2.6.3 Merging, linking, as well as any restriction, degradation, erasure or destruction of information.

2.7 Record: means any recorded information, regardless of form or medium, including:

2.7.1 Writing on any material;
2.7.2 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;
2.7.3 Label, marking or other writing which identifies or describes anything of which it forms part, or to which it is attached by any means;
2.7.4 Book, map, plan, graph or drawing;
2.7.5 Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced.

2.8 Filing System: means any structed set of personal information, whether centralized, decentralized or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

2.9 Unique Identifier: means any Identifier that is assigned to a data subject and is used by a responsible party for the purposed of the operations of the responsible party and that uniquely identifies that data subject in relation to that responsible party.

2.10 De-Identify: 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.

2.11 Re-Identity: means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

2.12 Direct Marketing: means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

2.12.1 Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
2.12.2 Requesting the data subject to make a donation of any kind for any reason.

2.13 Biometrics: means a technique of personal identification that is based on physical, physiological or behavioural characterization including blood tying, fingerprinting, DNA analysis, retinal scanning and voice recognition.

3. POLICY PURPOSE

3.1 The purpose of this policy is to protect the organization from the compliance risks associated with the POPI Act which includes:

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

3.2 This policy demonstrates the organization's commitment to protecting the privacy rights of data subjects in the following manner:

3.2.1 Through stating desired behaviour and directing compliance with the provisions of the POPI Act and best practice.
3.2.2 By cultivating an organizational culture that recognizes privacy as a valuable human right.
3.2.3 By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.
3.2.4 By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of the organization.
3.2.5 By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information officers, to protect the interests of the organization and data subjects.

4. POLICY APPLICATION

4.1 This policy and its guiding principles applies to:

4.1.1 The organization's governing body;
4.1.2 All branches, business units and divisions of the organization;

4.1.3 All employees and volunteers;
4.1.4 All contractors, suppliers and other persons acting on behalf of the organization.

4.2 The policy's guiding principles find application in all situations and must be read in conjunction with the POPI Act, as well as any other applicable documentation (PAIA Manual).

4.3 The legal duty to comply with the POPI Act is activated in any situation where there is: a processing of personal information entered into a record by or for a responsible party who is domiciled in South Africa.

4.4 The POPI Act does not apply in situations where the processing of personal information:

4.4.1 Is concluded in the course of purely personal or household activities; or
4.4.2 Where the personal information has been de-identified.

5. RIGHTS OF DATA SUBJECTS

5.1 The right to access of personal information

5.1.1 The organization recognizes that a data subject has the right to establish whether the organization holds personal information related to him/her or it including the right to request access to that personal information.

5.2 The Right to have Personal Information Corrected or Deleted (where appropriate), the organization will ensure that its clients and customers are made aware of the rights conferred upon them as data subjects. The organization will ensure that it gives effect to the following rights:

5.2.1 The Right to Object to the Processing of Personal Information
5.2.2 The Right to Object to Direct Marketing
5.2.3 The Right to Complain to the Information Regulator
5.2.4 The Right to be Informed

5.3 The data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where the organisation is no longer authorised to retain the personal information.

5.4 The data subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information. In such circumstances, the organization will give due consideration to the request and the requirements of POPIA. The organization 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.

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

5.6 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.

5.7 The data subject has the right to be notified that his, her or its personal information is being collected by the organisation. The data subject also has the right to be notified in any situation where the organization 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

6.1 Accountability

6.1.1 All employees and persons acting on behalf of the organisation will at all times be subject to, and act in accordance with, the following guiding principles:

- Processing Limitation
- Purpose Specification
- Further Processing Limitation
- Information Quality

6.2 Failing to comply with the POPI Act could potentially damage the organisation's reputation or expose the organisation to a civil claim for damages. The protection of personal information is therefore everybody's responsibility. The organisation will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour.

6.3 However, the organisation will take appropriate sanctions, which may include: disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

6.4 The organisation will ensure that personal information under its control is processed:
in a fair, lawful and non-excessive manner;
only with the informed consent of the data subject; and
only for a specifically defined purpose.

6.5 The organisation 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 transactions are concluded over the telephone or electronic video feed, the organisation will maintain a voice recording of

the stated purpose for collecting the personal information followed by the data subject's subsequent consent.

6.6 The organisation will under no circumstances distribute or share personal information between separate legal entities, associated organisations (such as subsidiary companies) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected. Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other aspects of the organisation's business and be provided with the reasons for doing so.

6.7 All the organisation's business units and operations must be informed by the principle of transparency. The organisation will process personal information only for specific, explicitly defined and legitimate reasons. The organisation will inform data subjects of these reasons prior to collecting or recording the data subject's personal information.

6.8 Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose. Therefore, where the organisation seeks to process personal information it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, the organisation will first obtain additional consent from the data subject.

6.9 The organisation will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading. The more important it is that the personal information be accurate (for example, the beneficiary details of a life insurance policy are of the utmost importance), the greater the effort the organisation will put into ensuring its accuracy. Where personal information is collected or received from third parties, the organisation will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources.

6.10 The organisation will take reasonable steps to ensure that data subjects are notified (are at all times aware) that their personal information is being collected including the purpose for which it is being collected and processed.

6.11 The organisation will ensure that it establishes and maintains a "contact us" facility, for instance via its website or through an electronic helpdesk, for data subjects who want to:
Enquire whether the organisation holds related personal information;
Request access to related personal information;
Request the organisation to update or correct related personal information; or
Make a complaint concerning the processing of personal information.

6.12 Open Communication

6.12.1 Security Safeguards
6.12.1.1 The organisation will manage the security of its filing system to ensure that personal information is adequately protected.
6.12.1.2 To this end, security controls will be implemented to minimize the risk of loss, unauthorised access, disclosure, interference, modification or destruction. Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as medical information or credit card details, the greater the security required.

6.13 The organisation will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the organisation's IT network. The organisation will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.

6.14 All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which the organisation is responsible. All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses.

6.15 The organisation's operators and third-party service providers will be required to enter into service level agreements with the organisation where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

6.16 Data Subject Participation

6.16.1 A data subject may request the correction or deletion of his, her or its personal information held by the organisation. The organisation will ensure that it provides a facility for data subjects who want to request the correction of deletion of their personal information. Where applicable, the organisation will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

7. COOKIES

7.1 Whereas the Company respects the privacy of all personal data and private information collected, processed and stored. As such, we undertake to handle all personal information received and processed with due care and provide the necessary security to safeguard all information held by us. Our internal system similarly allows us to proactively react should there be a breach of any kind, alternatively our privacy practices and POPI policy dictates that we report any material breach to the Regulator. The further terms of the Company's cookies policy and general terms of compliance are recorded hereunder:

Cookies

The Company uses cookies, pixels and other technologies (collectively referred to as "cookies") to recognize your browser or device, learn more about your company or industry, and provide you with essential features and services, as well as for additional purposes, including:

1. Recognizing you when you sign-up to use our services. This allows us to provide each user or data subject with customized features and services, if applicable.
2. Conducting research and diagnostics to improve the Company's website content, products, and services.
3. Preventing fraudulent activity.
4. Improving security.
5. Delivering content, including ads, relevant to your interests.
6. Reporting. This allows us to measure and analyse the performance of our services.

You can manage browser cookies through your browser setting. The "Help" feature on most browsers will tell you how to prevent your browser from accepting new cookies; how to have the browser notify you when you receive a new cookie; how to disable cookies; and when cookies will expire. If you disable all cookies on your browser, the Company, nor any of its third parties, will transfer cookies to your browser. If you do this, however, you may have to manually adjust some preferences every time you visit a site, and some features and services may not work.

7.2 The Data We Collect And The Cookies We Use

We collect and sends the following data to data processor partners:

Analytics cookies

For tracking audience numbers, what advertising is viewed and what the audience does on the site. Does not track what users do on other sites.

Google Ad Manager: Online identifiers, including cookie identifiers, internet protocol addresses and device identifiers.
Google Analytics: Online identifiers, including cookie identifiers and device identifiers; client identifiers. Internet protocol addresses are anonymized.
Google Tag Manager: Online identifiers, including cookie identifiers and internet protocol addresses.
Find more information on Google as a data processor by clicking here.

7.3 Advertising cookies

Adsense tracks users across multiple websites, and while it does not appear on all of our pages, there are some Google Ads delivered on some of our pages. Users can see what data Google has on their advertising interests, and can control all aspects of how Google collect information on them by clicking here.

Google Adsense: Online identifiers, including cookie identifiers and internet protocol addresses.

Find more information on Google Adsense as a data processor – how they use information collected from partner websites – by clicking here

Dianomi: Online identifiers, including cookie identifiers and internet protocol addresses.
The Dianomi cookie is used for conversion tracking in online advertising. View their privacy policy here.

Vidoomy: Online identifiers, including cookie identifiers and internet protocol addresses.
The Vidoomy cookie is used for Ad Serving, Ad Targeting, Analytics/Measurement. View their privacy policy here.

7.4 Embedded content cookies

Twitter: Online identifiers, including cookie identifiers and internet protocol addresses.
Twitter is a social messaging and sharing platform. On pages with Twitter widgets, Twitter will set a cookie on your computer. To view all the data Twitter has on your profile, you will have to log into your Twitter account. Your data can be found by clicking here. Twitter's privacy policy is available here.

YouTube: Online identifiers, including cookie identifiers and internet protocol addresses.
YouTube is a video publishing platform. On pages with videos embedded at YouTube, YouTube will set a cookie and track user actions such as play or pause. To view YouTube's privacy policy, click here.

7.5 Site cookies
Our site cookies are integral to the functioning of our website(s). While you visit our site, we'll track location, IP address and browser type: we'll use this for purposes like improving marketing, verification, customer service and system improvements.

They are used to allow users to log in, to order services and/or pay for the said services. A list of cookies used can be found here. We'll also use cookies to keep track of orders while you're browsing our site.

When you purchase from us, we'll ask you to provide information including your name, billing address, email address, phone number, credit card/payment details and optional account information like username and password. We'll use this information for purposes, such as, to:

- Send you information about your account and order;
- Respond to your requests, including refunds and complaints;
- Process payments and prevent fraud;
- Set up your account for services;
- Comply with any legal obligations we have, such as calculating taxes.

If you create an account, we will store your name, address, email, phone number, registered company details, which will be used to populate your user account.

Our website administrators have access to the following information to help fulfill orders, process refunds and support you:

- Order information like what was purchased, when it was purchased and where it should be sent, and
- Customer information like your name, email address, and billing and shipping information.

When processing payments, some of your data will be passed to these payment gateways, including information required to process or support the payment, such as the purchase total and billing information.

Disabling Cookies

You can change the preferences of your browser to choose which cookies it must allow access to. These preferences are usually in the menu “options” or “preferences” of your browser.

Microsoft Edge: https://support.microsoft.com/en-us/microsoft-edge/delete-cookies-in-microsoft-edge-63947406-40ac-c3b8-57b9-2a946a29ae09
Firefox: https://support.mozilla.org/en-US/kb/block-websites-storing-cookies-site-data-firefox
Google Chrome: https://support.google.com/chrome/answer/95647
Safari: https://support.apple.com/en-za/guide/safari/sfri11471/mac

However, if you change your preferences and block these cookies, some functions of our website will be annulled and you will not be able to make the most of the features from our Website.

8. INFORMATION OFFICER

8.1 The organisation will appoint an Information Officer and where necessary, a Deputy Information Officer to assist the Information Officer. The organisation’s Information Officer is responsible for ensuring compliance with POPIA.

8.2 Where no Information Officer is appointed, the head of the organisation will assume the role of the Information Officer. Consideration will be given on an annual basis to the re-appointment or replacement of the Information Officer and the re-appointment or replacement of any Deputy Information Officers.

8.3 Once appointed, the organisation will register the Information Officer with the South African Information Regulator established under POPIA prior to performing his or her duties.

9. SPECIFIC DUTIES AND RESPONSIBILITIES

9.1 Governing Body

9.1.1 The organisation appoints an Information Officer, and where necessary, a Deputy Information Officer.

9.1.2 All persons responsible for the processing of personal information on behalf of the organisation:

9.1.2.1 are appropriately trained and supervised to do so;
9.1.2.2 The organisation's governing body cannot delegate its accountability and is ultimately answerable for ensuring that the organisation meets its legal obligations in terms of POPIA.
9.1.2.3 The governing body may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

9.1.3 The governing body is responsible for ensuring that:

9.1.3.1 understand that they are contractually obligated to protect the personal information they come into contact with; and
9.1.3.2 are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.

9.1.4 Data subjects who want to make enquires about their personal information are made aware of the procedure that needs to be followed should they wish to do so.
9.1.5 The scheduling of a periodic POPI Audit in order to accurately assess and review the ways in which the organisation collects, holds, uses, shares, discloses, destroys and processes personal information.

9.2 Information officer

9.2.1 Taking steps to ensure the organisation's reasonable compliance with the provision of POPIA.
9.2.2 Keeping the governing body updated about the organisation's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to POPIA.
9.2.3 Continually analysing privacy regulations and aligning them with the organisation's personal information processing procedures. This will include reviewing the organisation's information protection procedures and related policies.
9.2.4 Ensuring that POPI Audits are scheduled and conducted on a regular basis.
9.2.5 Ensuring that the organisation makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the

organisation. For instance, maintaining a “contact us” facility on the organisation’s website.
9.2.6 Approving any contracts entered with operators, employees and other third parties which may have an impact on the personal information held by the organisation. This will include overseeing the amendment of the organisation’s employment contracts and other service level agreements.
9.2.7 Encouraging compliance with the conditions required for the lawful processing of personal information.

9.3 Information Officer responsibility

9.3.1 Ensuring that employees and other persons acting on behalf of the organisation are fully aware of the risks associated with the processing of personal information and that they remain informed about the organisation’s security controls.
9.3.2 Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the organisation.
9.3.3 Addressing employees’ POPIA related questions.
9.3.4 Addressing all POPIA related requests and complaints made by the organisation’s data subjects.
9.3.5 Working with the Information Regulator in relation to any ongoing investigations. The Information Officers 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, regarding any other matter.

9.4 IT Manager / IT Support

9.4.1 Ensuring that the organisation’s IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.
9.4.2 Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services.
9.4.3 Ensuring that servers containing personal information are sited in a secure location, away from the general office space.
9.4.4 Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.
9.4.5 Ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious shacking attempts.
9.4.6 Ensuring that personal information being transferred electronically is encrypted.
9.4.7 Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.
9.4.8 Performing regular IT audits to ensure that the security of the organisation’s hardware and software systems are functioning properly.
9.4.9 Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.
9.4.10 Performing a proper due diligence review prior to contracting with operators

or any other third-party service providers to process personal information on the organisation's behalf. For instance, cloud computing services.

9.5 Marketing Manager / Team

9.5.1 Approving and maintaining the protection of personal information statements and disclaimers that are displayed on the organisation's website, including those attached to communications such as emails and electronic newsletters.
9.5.2 Addressing any personal information protection queries from journalists or media outlets such as newspapers.
9.5.3 Where necessary, working with persons acting on behalf of the organisation to ensure that any outsourced marketing initiatives comply with POPIA.

9.6 Employees and other persons acting on behalf of the Organisation

9.6.1 Employees and other persons acting on behalf of the organisation will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other employees.
9.6.2 Employees and other persons acting on behalf of the organisation are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.
9.6.3 Employees and other persons acting on behalf of the organisation may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the organisation 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.
9.6.4 Employees and other persons acting on behalf of the organisation must request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.
9.6.5 Employees and other persons acting on behalf of the organisation will only process personal information where:

9.6.5.1 The data subject, or a competent person where the data subject is a child, consents to the processing; or
9.6.5.2 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
9.6.5.3 The processing complies with an obligation imposed by law on the responsible party; or
9.6.5.4 The processing protects a legitimate interest of the data subject; or
9.6.5.5 The processing is necessary for pursuing the legitimate interests of the organisation or of a third party to whom the information is supplied.

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

9.6.6.1 Clearly understands why and for what purpose his, her or its personal information is being collected; and

9.6.6.2 Has granted the organisation with explicit written or verbally recorded consent to process his, her or its personal information.

9.6.7 Employees and other persons acting on behalf of the organisation will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.

9.6.8 Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with.

9.6.9 Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, the organisation will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.
9.6.10 Consent to process a data subject's personal information will be obtained directly from the data subject, except where:

9.6.10.1 the personal information has been made public;
9.6.10.2 where valid consent has been given to a third party; or
9.6.10.3 the information is necessary for effective law enforcement.

9.6.11 Employees and other persons acting on behalf of the organisation will under no circumstances:

9.6.11.1 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.
9.6.11.2 Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from the organisation's central database or a dedicated server.
9.6.11.3 Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer.
9.6.11.4 Transfer personal information outside of South Africa without the express permission from the Information Officer.

9.6.12 Employees and other persons acting on behalf of the organisation are responsible for:

9.6.12.1 Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.
9.6.12.2 Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.

9.6.12.3 Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, other persons acting on behalf of the organisation, with the sending or sharing of personal information to or with authorised external persons.
9.6.12.4 Ensuring that all computers, laptops, and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.
9.6.12.5 Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.
9.6.12.6 Ensuring that where personal information is stored on removable storage medias such as external drives, CDs or DVDs that these are kept locked away securely when not being used.
9.6.12.7 Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet.
9.6.12.8 Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer.
9.6.12.9 Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.
9.6.12.10 Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.
9.6.12.11 Undergoing POPI Awareness training from time to time.

9.6.13 Where an employee, or a person acting on behalf of the organisation, becomes aware or suspicious of any security breach such as the 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.

10. POPI AUDIT

10.1 The organisation's Information Officer will schedule periodic POPI Audits.
10.2 The purpose of the POPI Audit is to:

10.2.1 Identify the processes used to collect, record, store, disseminate and destroy personal information.
10.2.2 Determine the flow of personal information throughout the organisation. For instance, the organisation's various business units, divisions, branches and other associated organisations.

10.2.3 Redefine the purpose for gathering and processing personal information.
10.2.4 Ensure that the processing parameters are still adequately limited.
10.2.5 Ensure that new data subjects are made aware of the processing of their personal information.
10.2.6 Re-establish the rationale for any further processing where information is received via a third party.
10.2.7 Verify the quality and security of personal information.
10.2.8 Monitor the extend of compliance with POPIA and this policy.
10.2.9 Monitor the effectiveness of internal controls established to manage the organisation's POPI related compliance risk.
10.2.10 In performing the POPI Audit, Information Officers will liaise with line managers in order to identify areas within in the organisation's operation that are most vulnerable or susceptible to the unlawful processing of personal information. Information Officers will be permitted direct access to and have demonstrable support from line managers and the organisation's governing body in performing their duties.

11. REQUEST TO ACCES PERSONAL INFORMATION

11.1 Data subjects have the right to:

11.1.1 Request what personal information the organisation holds about them and why.
11.1.2 Request access to their personal information.
11.1.3 Be informed how to keep their personal information up to date.

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

11.3 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. All requests will be processed and considered against the organisation's PAIA Policy.

11.4 The Information Officer will process all requests within a reasonable time.

12. POPI COMPLAINTS PROCEDURE

12.1 Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. The organisation takes all complaints very seriously and will address all POPI related complaints in accordance with the following procedure:

12.1.1 POPI complaints must be submitted to the organisation in writing. Where so required, the Information Officer will provide the data subject with a "POPI Complaint Form".
12.1.2 Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint

reach the Information Officer within 1 working day.
12.1.3 The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days.
12.1.4 The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.
12.1.5 The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on the organisation's data subjects.
12.1.6 Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with the organisation's governing body where after the affected data subjects and the Information Regulator will be informed of this breach.
12.1.7 The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to the organisation's governing body within 7 working days of receipt of the complaint. In all instances, the organisation will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.
12.1.8 The Information Officer's response to the data subject may comprise any of the following:

12.1.8.1 A suggested remedy for the complaint,
12.1.8.2 A dismissal of the complaint and the reasons as to why it was dismissed, or
12.1.8.3 An apology (if applicable) and any disciplinary action that has been taken against any employees involved.

12.2 Where the data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to complain to the Information Regulator.

12.3 The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting.
12.4 The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPI related complaints.

13. DISCIPLINARY ACTION

13.1 Where a POPI complaint or a POPI infringement investigation has been finalised, the organisation may recommend any appropriate administrative, 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.

13.2 In the case of ignorance or minor negligence, the organisation will undertake to provide further awareness training to the employee.

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

13.4 Examples of immediate actions that may be taken subsequent to an investigation include:

13.4.1 A recommendation to commence with disciplinary action.
13.4.2 A referral to appropriate law enforcement agencies for criminal investigation.
13.4.3 Recovery of funds and assets in order to limit any prejudice or damages caused.

—– END—–