POLICY IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT (POPIA)

FSP NAME: LIB 8 CONSULT (PTY)LTD

FSP NUMBER: 50323

INFORMATION OFFICER: JEMIMA JAGESUR

PROTECTION OF PERSONAL INFORMATION POLICY

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.

Through the provision of advice and intermediary services, the FSP is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, employees and other stakeholders.

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, the FSP is committed to effectively managing personal information in accordance with POPIA'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:

- 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 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;
- 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 (referred to as client)

This refers to the natural or juristic person to whom personal information relates, such as an individual client or a company that supplies the FSP with products or other goods.

2.3. Responsible Party (FSP)

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 FSP is the responsible party.

2.4. Information Officer

The Information Officer is responsible for ensuring the FSP's compliance with POPIA and will be the head of the FSP.

Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.

2.5. Processing

The act of processing information includes any activity or any set of operations, whether or not by automatic means, 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
- merging, linking, as well as any restriction, degradation, erasure or destruction of information.

2.6. Consent

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

2.7. Direct Marketing

Means to approach a client, 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 client.

3. POLICY PURPOSE

This purpose of this policy is to protect the FSP from the compliance risks associated with the protection of personal information which includes:

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

This policy demonstrates the FSP's commitment to protecting the privacy rights of clients in the following manner:

- Through stating desired behaviour and directing compliance with the provisions of POPIA and best practice.
- By cultivating a 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 creating business practices that will provide reasonable assurance that the rights of clients are protected and balanced with the legitimate business needs of the FSP.
- By assigning specific duties and responsibilities, including the appointment of an Information Officer and where necessary, Deputy Information Officers in order to protect the interests of the FSP and clients.
- By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

4. POLICY APPLICATION

This policy and its guiding principles apply to:

- All branches, business units and divisions of the FSP;
- All employees

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

The legal duty to comply with POPIA's provisions is activated in any situation where there is a **processing** of **personal information** entered into a **record** by or for a **responsible person** who is **domiciled** in South Africa.

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

- is concluded in the course of purely personal or household activities, or
- where the personal information has been de-identified

4.1. Collection of Personal Information

The FSP collects and processes client's personal information in the ordinary course and scope of its business. The type of Personal Information collected is dependent on the need for which it is collected, and the information will be processed for that purpose only. Whenever possible, the client will be informed as to what Personal Information is required and what information is optional.

THE FSP also collects and processes client's Personal Information for marketing purposes to ensure that its products and services remain relevant to our clients and potential clients.

THE FSP aims to have agreements in place with all product suppliers, insurers, and third-party service providers to ensure a mutual understanding regarding the protection of its client's Personal Information.

With the client's consent, THE FSP may also supplement the information provided by the client with information received from other providers, in order to offer the client a more comprehensive experience in their interaction with us. For purposes of this Policy, clients include potential and existing clients.

4.2. The use of Personal Information

The client's Personal Information will only be used for the purpose for which it was collected and as agreed. This may include:

- Providing products or services to clients and to carry out the transactions requested;
- For underwriting purposes;
- Assessing and processing claims;
- Confirming, verifying, and updating client details;
- For purposes of claims history;
- For the detection and prevention of fraud, crime, money laundering or other malpractices;
- For audit and record keeping purposes;
- Providing services to clients, to render the services requested and to maintain and constantly improve the relationship with the client;
- Providing communication in respect of THE FSP and/or regulatory matters that may affect clients; and
- In connection with and to comply with legal and regulatory requirements, or when otherwise allowed by law.

According to the Act, the following conditions must be met for THE FSP to process the client's Personal Information:

- The client's consent must be obtained;
- The processing of information is necessary for the conclusion or performance of a contract;
- The processing of information is necessary for THE FSP to comply with an obligation imposed by law;
- The processing of information protects a legitimate interest of the client;
- The processing of information is necessary for pursuing the legitimate interests of THE FSP or of a third party to whom information is supplied.

4.3. Disclosure of Personal Information

THE FSP may disclose a client's personal information to an approved product supplier or third-party service provider whose services or products clients elect to use.
THE FSP may also disclose a client's information where it has a duty or a right to disclose in terms of applicable legislation or where it may be deemed necessary in order to protect THE FSP's rights.

4.4. Storage of Documents

It is the responsibility of the FSP to ensure that records of personal information are not retained any longer than is necessary for achieving the purpose for which the information was collected.

The FSP will no longer be authorised to retain information if**:**

- The information is no longer necessary for the purpose for which it was obtained.
- The client has withdrawn their consent for the processing of their information.
- The client has validly objected to the processing of the information; or
- The client has made a valid request for the deletion of their personal information.

However, we may retain your information for as long we are required to comply with legal or regulatory requirements or to protect our legal interests. This may mean that your information is retained for longer than the minimum time set out by the law.

5. RIGHTS OF CLIENTS

Where appropriate, the FSP will ensure that its clients are made aware of the rights conferred upon them as clients.

The FSP will ensure that it gives effect to the following six rights.

5.1. The Right to Access Personal Information

The FSP recognises that a client has the right to establish whether the FSP holds personal information related to them, including the right to request access to that personal information.

An example of a "Personal Information Request Form" can be found under Annexure A.

5.2. The Right to have Personal Information Corrected or Deleted

The client has the right to request, where necessary, that their personal information must be corrected or deleted where the FSP is no longer authorised to retain the personal information.

5.3. The Right to Object to the Processing of Personal Information

The client has the right, on reasonable grounds, to object to the processing of their personal information.

In such circumstances, the FSP will give due consideration to the request and the requirements of POPIA. The FSP may cease to use or disclose the client'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 client has the right to object to the processing of their personal information for purposes of direct marketing by means of unsolicited electronic communications.

5.5. The Right to Complain to the Information Regulator

The client 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 their personal information.

5.6. The Right to be Informed.

The client has the right to be notified that their personal information is being collected by the FSP.

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

6. GENERAL GUIDING PRINCIPLES

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

6.1. Accountability

Failing to comply with POPIA could potentially damage the FSP's reputation or expose the FSP to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

The FSP will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, the FSP 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.

6.2. Processing Limitation

The FSP will ensure that personal information under its control is processed:

- in a fair, lawful and non-excessive manner, and
- only with the informed consent of the client, and
- only for a specifically defined purpose.

The FSP will inform the client of the reasons for collecting 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 FSP will maintain a voice recording of the stated purpose for collecting the personal information followed by the client's subsequent consent.

The FSP will under no circumstances distribute or share personal information between separate legal entities, associated FSPs (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 client must be informed of the possibility that their personal information will be shared with other aspects of the FSP's business and be provided with the reasons for doing so.

An example of a “POPI Consent Form” can be found under Annexure C.

6.3. Purpose Specification

The FSP will process personal information only for specific, explicitly defined and legitimate reasons. The FSP will inform clients of these reasons prior to collecting or recording the client's personal information.

6.4. Further Processing Limitation

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose.

Therefore, where the FSP 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 FSP will first obtain additional consent from the client.

6.5. Information Quality

The FSP 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 FSP will put into ensuring its accuracy.

Where personal information is collected or received from third parties, the FSP will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the client or by way of independent sources.

6.6. Open Communication

The FSP will take reasonable steps to ensure that clients are at all times aware that their personal information is being collected including the purpose for which it is being collected and processed.

6.7. Security Safeguards

The FSP will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise 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.

The FSP will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the FSP's IT network.
The FSP will ensure that all paper and electronic records comprising 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 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 FSP 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.

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

6.8. Client Participation

A client may request the correction or deletion of his, her or its personal information held by the FSP.

The FSP will ensure that it provides a facility for clients who want to request the correction of deletion of their personal information. Where applicable, the FSP will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

7. INFORMATION OFFICERS

The FSP will appoint an Information Officer and where necessary, a Deputy Information Officer to assist the Information Officer.
The FSP's Information Officer is responsible for ensuring compliance with POPIA.
Once appointed, the FSP will register the Information Officer with the South African Information Regulator established under POPIA prior to performing his or her duties.

8. SPECIFIC DUTIES AND RESPONSIBILITIES

8.1. Information Officer

The FSP's Information Officer is responsible for:

- Taking steps to ensure the FSP's reasonable compliance with the provision of POPIA.
- Keeping the management team updated about the FSP's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the management team of their obligations pursuant to POPIA.
- Continually analysing privacy regulations and aligning them with the FSP's personal information processing procedures. This will include reviewing the FSP's information protection procedures and related policies.
- Ensuring that POPI Audits are scheduled and conducted on a regular basis.
- Ensuring that the FSP makes it convenient for clients who want to update their personal information or submit POPI related complaints to the FSP.
- Approving any contracts entered with employees and other third parties which may have an impact on the personal information held by the FSP. This will include overseeing the amendment of the FSP's employment contracts and other service level agreements.
- Encouraging compliance with the conditions required for the lawful processing of personal information.
- Ensuring that employees and other persons acting on behalf of the FSP are fully aware of the risks associated with the processing of personal information and that they remain informed about the FSP's security controls.
- Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the FSP.
- Addressing employees' POPIA related questions.
- Addressing all POPIA related requests and complaints made by the FSP's clients.
- 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.

- Ensuring that the FSP's IT infrastructure, filing systems and any other devices used for processing personal information meet 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 servers containing personal information are sited in a secure location, away from the general office space. 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 shacking 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 audits to ensure that the security of the FSP's hardware and software systems are functioning properly.
- Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.
- Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on the FSP's behalf. For instance, cloud computing services.
- Approving and maintaining the protection of personal information statements and disclaimers that are displayed on the FSP's website, including those attached to communications such as emails and electronic newsletters.
- Addressing any personal information protection queries from journalists or media outlets such as newspapers.
- Where necessary, working with persons acting on behalf of the FSP to ensure that any outsourced marketing initiatives comply with POPIA.

8.2. Employees and other Persons acting on behalf of the FSP

Employees and other persons acting on behalf of the FSP will, during the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other employees.

Employees and other persons acting on behalf of the FSP are required to treat personal information as a confidential business asset and to respect the privacy of clients.

Employees and other persons acting on behalf of the FSP may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the FSP 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 the FSP must request assistance from the Information Officer if they are unsure about any aspect related to the protection of a client's personal information.

Employees and other persons acting on behalf of the FSP will only process personal information where:

- The client, or a competent person where the client is a child, consents to the processing; or
- The processing is necessary to carry out actions for the conclusion or performance of a contract to which the client is a party; or
- The processing complies with an obligation imposed by law on the responsible party; or
- The processing protects a legitimate interest of the client; or
- The processing is necessary for pursuing the legitimate interests of the FSP or of a third party to whom the information is supplied.

Furthermore, personal information will only be processed where the client:

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

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

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

Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form.
Consent to process a client's personal information will be obtained directly from the client, except where:

- the personal information has been made public, or where valid consent has been given to a third party, or
- the information is necessary for effective law enforcement.

Employees and other persons acting on behalf of the FSP 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. All personal information must be accessed and updated from the FSP's central database or a dedicated server.

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

- Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.
- Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records or filing systems therefore be created.
- 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.
- Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.
- 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.
- 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.
- 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.
- Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a client's contact details when the client phones or communicates via email.
- 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.
- Undergoing POPI Awareness training from time to time.

Where an employee, or a person acting on behalf of the FSP, 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.

9. POPI AUDIT

The FSP's Information Officer will schedule periodic POPI Audits.

The purpose of a POPI audit is to:

- Identify the processes used to collect, record, store, disseminate and destroy personal information.
- Determine the flow of personal information throughout the FSP. For instance, the FSP's various business units, divisions, branches and other associated FSPs.
- Redefine the purpose for gathering and processing personal information. Ensure that the processing parameters are still adequately limited.
- Ensure that new clients are made aware of the processing of their personal information.
- Re-establish the rationale for any further processing where information is received via a third party.
- Verify the quality and security of personal information.
- Monitor the extend of compliance with POPIA and this policy.
- Monitor the effectiveness of internal controls established to manage the FSP's POPI related compliance risk.

10. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

Clients have the right to:

- Request what personal information the FSP holds about them and why.
- Request access to their personal information.
- Be informed how to keep their personal information up to date.

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

Once the completed form has been received, the Information Officer will verify the identity of the client prior to handing over any personal information. All requests will be processed and considered against the FSP's PAIA Policy.

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

11. POPI COMPLAINTS PROCEDURE

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

- POPI complaints must be submitted to the FSP in writing. Where so required, the Information Officer will provide the client with a "POPI Complaint Form".
- 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.
- The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days.
- 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.
- 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 FSP's clients.
- Where the Information Officer has reason to believe that the personal information of clients has been accessed or acquired by an unauthorised person, the Information Officer will consult with the FSP's management team where after the affected clients and the Information Regulator will be informed of this breach.
- The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to the FSP's management team within 7 working days of receipt of the complaint. In all instances, the FSP will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.

The Information Officer's response to the client may comprise any of the following:

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

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

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. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPI related complaints.

12. DESTRUCTION OF INFORMATION

We will destroy all personal information that is not required to be retained by law or any other purposes in the following way

Personal information will be destroyed in the following manner

Hard copies/Paper will be shredded

Electronic information will be deleted

13. DISCIPLINARY ACTION

Where a POPI complaint or a POPI infringement investigation has been finalised, the FSP 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.

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

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

Examples of immediate actions that may be taken after an investigation include:

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