



POPI MANUAL

In terms of The Protection of Personal Information Act (Act No. 4, 2013)

INTRODUCTION

LIFA INSURANCE BROKERS (PTY) LTD is an authorised financial service provider (“the FSP”) which is obliged to comply with The Protection of Personal Information Act (‘POPI’). POPI requires the FSP to inform their clients as to how their Personal Information is used, disclosed and destroyed.

The FSP guarantees its commitment to protecting their client’s privacy and ensuring their Personal Information is used appropriately, transparently, securely and in accordance with applicable laws.

This Policy sets out how the FSP deals with their client’s Personal Information and in addition for what purpose said information is used for.

This Policy will be made available on request from our office during business hours.

Section 9 of POPI states that *“Personal Information may only be processed if given the purpose for which it is processed, it is adequate, relevant and not excessive.”*

THE PERSONAL INFORMATION COLLECTED

The FSP collects and processes clients Personal Information pertaining to clients Financial Needs. The type of information will depend on the need for which it is collected and will be processed for that purpose only.

Whenever possible, we will inform the client what information they are required to provide us with and what information is optional.

Examples of the Personal Information we collect may include but not limited to:

1. Clients’ Identity numbers, name, surname, address, postal code, marital status and how many dependents they have
2. Description of clients residence, business and assets; and
3. Any other information required by us and Insurers in order to provide clients with an accurate Analysis of their Insurance needs.

The FSP also collects and processes clients Personal Information for marketing purposes to ensure our products and services remain applicable to our clients and potential clients.

We have agreements in place with all our Product Suppliers, Insurers and third-party Service



Providers to ensure there is a mutual understanding with regard to the protection of Client Personal Information. Our suppliers are subject to the same regulations as we are subjected to.

With clients' consent, we may also supplement the information provided with information we receive from other providers in order to offer a more consistent and personalized experience in clients' interaction with us. For purposes of this manual, clients include Potential and existing clients.

HOW PERSONAL INFORMATION IS USED

Client's Personal Information will only be used for the purpose for which it was collected and agreed.

This may include:

1. Providing products or services to clients and to carry out the transactions requested
2. For underwriting purposes
3. Assessing and Processing claims
4. Conducting credit reference searches or verification
5. Confirming, verifying and updating clients details
6. For purposes of claims history
7. For the detection and prevention of fraud, crime, money laundering or other malpractice
8. Conducting market or customer satisfaction research
9. For audit and record keeping purposes
10. In connection with legal proceedings
11. Providing our services to clients to carry out the services requested and to maintain and constantly improve the relationship
12. Providing communications in respect of the FSP and regulatory matters that may affect clients
13. In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

According to Section 10 of POPI, Personal Information may only be processed if certain conditions are met which are listed below along with supporting information for the FSP processing of Personal Information:

1. Client consents to the processing – consent is obtained from clients during the introductory, appointment and Needs Analysis stage of our relationship;
2. The processing is necessary – in order to conduct an accurate Analysis of clients Insurance needs certain Persona information is required;
3. Processing complies with an obligation imposed by law on the FSP – The Financial Advisory and Intermediary Services Act ('FAIS') requires Financial Service Provider's ('FSPs') to conduct a Needs Analysis and obtain information from clients about their Insurance Needs in order to provide them with applicable and beneficial products;



4. Processing protects a legitimate interest of the client – it is in the client’s best interest to have a full and proper Needs Analysis performed in order to provide them with an applicable and beneficial product, this requires obtaining Personal Information;
5. Processing is necessary for pursuing the legitimate interests of the FSP or of a third party to whom information is supplied – in order to provide our clients with products both ourselves and our Product suppliers and insurers need certain Personal Information from the clients to make an expert decision on the unique and specific product they require.

DISCLOSURE OF PERSONAL INFORMATION

1. We may disclose clients’ Personal Information to our providers whose services or products clients elect to use. We have agreements in place to ensure that they comply with confidentiality and privacy conditions.
2. We may also share client Personal Information with, and obtain information about clients from third parties for the reasons already discussed above.
3. We may also disclose clients’ information to where we have a duty or a right to disclose in terms of applicable legislation, the law or where it may be necessary protect our rights.

THE RIGHTS OF CLIENTS (DATA SUBJECTS)

POPIA creates the following rights for South African citizens (data subjects):

- a) Right to be notified about collection and processing of personal information
- b) Right to access personal information
- c) Right to request correction of personal information
- d) Right to request deletion of personal information
- e) Right to object to the processing of personal information
- f) Right not to have personal information processed for the purpose of direct marketing by means of unsolicited electronic communications
- g) Right to not be subject to a decision which results in legal circumstances based solely on the basis of the automated processing
- h) Right to complain to the Information Regulator
- i) Right to effect judicial remedy

In other words, South African citizens have the right to know when their personal information is likely to be collected and have the right to consent to it before it happens. They also have the ability to request that your company gives them access to see what personal information it has collected about them, as well as have that information either corrected or deleted altogether.



SAFEGUARDING CLIENTS’ INFORMATION

It is a requirement of POPI to adequately protect the Personal Information we hold and to avoid unauthorised access and use of your Personal Information. We will continuously review our security controls and processes to ensure that your Personal Information is secure.

The following procedures are in place in order to protect your Personal Information:

Our external Compliance Officer is hereby mandated to monitor the status of the safeguarding of clients Personal Information and the recommendations made by him will be actioned. This will take place as part of the quarterly compliance monitoring.

The Compliance Officer’s details are as follows:

Name: Mpho Mahlakwane trading as MM LEGAL & COMPLIANCE

Tel: 0114193067|0741848467| Fax: 0862980491

E-mail: mpho@compliancemm.co.za

INFORMATION OFFICER

The details of our Information Officer are as follows:

Name :
Designation :

The Information Officer is responsible for the encouragement of compliance with the conditions of the lawful processing of Personal Information and other provisions of POPI. The Information officer is also responsible for the following:

- a) To encourage compliance with POPI
- b) Dealing with requests made to the FSP in relation to POPI, including requests from clients (data subjects) to update or view their personal information.
- c) Working with the Regulator in relation to investigations
- d) Ensure that training takes place internally in relation to POPI and maintaining training records.

The details of Information Officer should be updated on an annual basis or as and when it becomes necessary.

POPI COMPLAINTS PROCEDURE

Clients have the right to complain in instances where any of their rights in terms of the POPI Act have been infringed upon. We take all complaints very seriously and will deal with all POPI related complaints in accordance with the following procedure:



1. All complaints must be forwarded to the FSP in writing and must be addressed to the Information Officer.
2. Where a complaint has been received by any person other than the Information Officer, such person must ensure that the complaint is referred to the Information Officer within one (1) day.
3. The Information Officer will provide the complainant with a written acknowledgement within 2 working days from date of receipt.
4. The Information Officer will carefully consider the complaint in an amicable manner. The Information Officer will consider resolving the complaint in a fair manner and in accordance with the provisions of the POPI Act.
5. The Information Officer must determine whether the complaint is a result of a breach of confidentiality or an error that has occurred and that may have a wider impact on the FSP's other clients.
6. 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 must facilitate a process in which the affected clients and the Information Regulator are informed of the breach.
7. The Information Officer must return to the complainant with a proposed solution within seven (7) working days.
8. The Information Officer's response to the complainant may comprise any of the following:
 - a) A suggested remedy for the complaint.
 - b) A dismissal of the complaint and the reasons why it was dismissed.
 - c) An apology (if applicable) and details of any disciplinary action taken if any employee involved in the breach.
9. When the complainant is not satisfied with the Information Officer's remedial action, the complainant has the right to escalate the complaint to the Information Regulator.
10. The Information Officer will review this procedure at least once annually and to improve on it where necessary. The reason for complaints must also be reviewed to ensure the avoidance of occurrences giving rise to POPI related complaints.

TRAINING AND AWARENESS

1. THIS MANUAL has been put in place and training on this policy and the POPI Act will take place from the date of implementation and will be facilitated by the Information Officer
2. The Information Officer must facilitate the training and also maintain the necessary training records for future reference
3. Each employee will be required to sign a CONFIDENTIALITY AGREEMENT which will be considered an annexure to their Employment Contract



INSURANCE BROKERS cc

Cell: 082 640 7493

Tel: 011 786 8855

Fax: 086 548 3262

Fax: 086 610 2728

email: admin@lifabrokers.co.za

www.lifainsurancebrokers.co.za

4. An INCIDENT MANAGEMENT REGISTER will be kept to log any security incidents and to report on and manage said incidents this register will be maintained by the Information Officer of the FSP in conjunction with the Key Individual
5. CONSENT to process client information is obtained from clients (or a person who has been given authorisation from the client to provide THE CLIENT'S Personal Information) during the Introductory, Appointment and Needs Analysis stage of the relationship.

AMENDMENTS TO THIS MANUAL

Amendments to this manual will take place on an ad hoc basis or at least once a year. Clients are advised make the necessary inquiries to that effect or to check our website periodically to inform themselves of any changes. Where material changes take place clients will be notified directly.

Directors : P. Z. B. JIJJ

CK No.: 2009/176373/23

AN AUTHORISED FSP43132

162 8th Avenue, Highlands North 2192. P.O Box 10530, Fourways East 2055



INFORMATION OFFICER APPOINTMENT LETTER

As required by the Protection of Personal Information Act. This appointment may at any time be amended or withdrawn in writing.

THE FOLLOWING PERSON IS HEREBY APPOINTED AS INFORMATION OFFICER FOR:

Company name: _____ **FSP no:** _____

DETAILS OF INFORMATION OFFICER:

Full names: _____

Designation: _____

Contact numbers: _____

e-mail address: _____

The Information Officer is entrusted with the following responsibilities:

1. Taking steps to ensure the organization’s reasonable compliance with the provisions of POPIA.
2. Keeping the organization’s management updated about its information protection responsibilities under POPIA. For instance, in the case of a security breach, the IO must inform and advise management of their obligations pursuant to POPIA.
3. Continually analysing privacy regulations and aligning them with the organization’s personal information processing procedures. This will include reviewing the organization’s information protection procedures and policies.
4. Ensuring the POPIA audits are scheduled and conducted on a regular basis.
5. Ensuring that the organization makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the organization, do so.



6. Approving any contracts entered into with operators, employees, and other parties which may have an impact on the personal information held by the organization. This will include overseeing the amendment of the organization’s employment contracts and other service level agreements.
7. Encouraging compliance with the conditions required for the lawful processing of personal information.
8. Ensuring that employees and other persons acting on behalf of the organization are fully aware of the risks associated with the processing of personal information and that they remain informed about the organization’s security controls.
9. Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the organization.
10. Addressing employees’ POPIA related questions.
11. Addressing all POPIA related requests and complaints made by the organization’s data subjects.
12. Working with the Information Regulator in relation to ongoing investigations. The IO will therefore act as the contact point for the Information Regulator on issues relating to the process of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

I HEREBY ACCEPT APPOINTMENT AS INFORMATION OFFICER:

Name: _____

Signature: _____

Date: _____