Protection of Personal Information (POPI) Policy and Processes for Umhlanga Insurance Brokers (Pty) Ltd, FSP Number 1150

1. INTRODUCTION

The Protection of Personal Information Act (POPIA), Act No 4 of 2013 commenced on 1 July 2020 with a 12-month grace period ending on 1 July 2021 to comply with this legislation.

The purpose of POPIA is to: -

- protect people from harm by protecting their Personal Information and their constitutional right to privacy – this means that a lawful justification must exist before a person's Personal Information may be processed; &.
- to ensure that all South African institutions conduct themselves in **a** responsible manner when collecting, processing, storing, and sharing another entity's Personal Information by holding them accountable should they abuse or compromise your Personal Information in any way

POPIA is a principled-base act as opposed to a simple rule, templates-based "tick-box" compliance approach to manage the requirements of the POPI Act which requires the FSP to think about its business and apply the relevant requirements specific to its business. This includes reviewing and implementing business policies and processes that would protect clients, employees and other business stakeholders from potential harm caused by a breach.

These POPIA policies and processes are hereby documented and implemented to ensure consistent standards and then reviewed regularly to ensure that they remain relevant. The review process will help to identify any gaps and where possible breaches of Personal Information may occur.

POPIA introduces measures whereby Personal Information processing by organisations is fair, responsible, and conducted in a secure manner.

POPIA applies to: -

- both public and private bodies
- any automated and non-automated processing of Personal Information (including hard copy and soft copy records).
- processing of Personal Information by responsible parties either domiciled in South Africa, or not domiciled in South Africa but making use of means within South Africa to process Personal Information.

2. IMPORTANT POPIA DEFINITIONS

2.1 Responsible Party

means a private or public body that determines the purpose of and means for processing Personal Information

2.2 Operator

means a person who processes Personal Information for a responsible person in terms of a contract or mandate without coming under the direct authority of that person

- acts on the instruction & mandate of the responsible person
- does not determine the purpose of the processing
- should not use the Personal Information for any other purpose

2.3 Personal Information (PI)

means information relating to an identifiable natural living person or existing juristic person including

race, gender, home or email address, ID number, biometric information, sexual orientation, religion, personal opinions, views or beliefs, consumer purchase history, education, employment history, medical history, criminal record.

Special Personal Information. Special Personal Information includes religious or philosophical beliefs, race or ethnic origin, Trade Union membership, political persuasion, health and sex life, biometric information, and criminal behaviour (alleged prior to conviction). The POPI Act imposes greater restrictions on the Processing of Special Personal Information, as well as Personal information of children (under the age of 18).

2.4 Processing

is defined as

- collecting, receiving, recording, organising, collating, storing, updating, or modifying, retrieving, altering, consulting, or using
- disseminating by transmitting or distributing
- merging, linking, erasing, or destroying

of Personal Information, in digital/automatic form or otherwise.

2.5 Data Subjects

Include your clients / customers, your organisation (the brokerage), the staff and representatives of your organisation and the parties with whom you are in contract (e.g., external service providers)

3. CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

Umhlanga Insurance Brokers (Pty) Ltd is a Category 1 Financial Services Provider providing advice and intermediary services in terms of the FAIS Act to clients in terms of the following sub-categories: -

- Short-Term Insurance Personal Lines & Personal Lines A1 (1.2 & 1.23); &
- Commercial Lines (1.6)

Umhlanga Insurance Brokers (Pty) Ltd determines the purpose of the Personal Information and the means for processing it, therefore is the Responsible Party. The FSP and its staff collect and process Personal Information on behalf of the FSP and therefore act as an extension of the Responsible Party. This means that where a representative is performing advice and intermediary services, he is acting on behalf of the FSP as the Responsible Party.

There are with the eight conditions Umhlanga Insurance Brokers (Pty) Ltd needs to comply with for the processing of Personal Information in terms of POPIA.

3.1 Condition 1 - Accountability

Umhlanga Insurance Brokers (Pty) Ltd as the Responsible Party must ensure that the conditions in POPIA and the measures that give effect thereto are complied with

- at the time of determination of the purpose and means of the processing, and
- also, during the processing, itself (i.e., comply at all times)

The FSP will ensure that all processing of Personal Information is done in a responsible manner, having due regard for the purpose of such processing.

The details of our Information Officer appointed within the business is

NAME:	Adrian Joubert
DESIGNATION:	Director & KI.
E-MAIL ADDRESS:	adrian@uib.co.za
TELEPHONE NUMBERS:	
LANDLINE	031 5831980
MOBILE	079 611 7116
POSTAL ADDRESS:	Suite 103, Granada Square, 16 Chartwell Drive, Umhlanga, 4310

PHYSICAL ADDRESS:	Suite 103, Granada Square, 16 Chartwell Drive, Umhlanga, 4310
COMPANY E-MAIL ADDRESS:	adrian@uib.co.za

Section 55(2) of POPIA requires that Information Officers must be registered with the Information Regulator before they can take up their duties in terms of POPIA and the Promotion of Access to Information Act (PAIA).

Umhlanga Insurance Brokers (Pty) Ltd has agreements in place with all our product suppliers and third-party service providers to ensure that there is a mutual understanding with regard to the protection of a client's Personal Information.

Checklist for Condition 1

- Has an Information Officer (IO) as required by POPIA who must ensure compliance with POPIA been determined and has he / she been registered with the Information Regulator?
- Do your contracts with your IT providers and other service providers cater for the POPIA conditions?
- Do you have processes in place to verify that your service providers meet their contractual responsibilities with regard to POPIA?

3.2 Condition 2 – Processing limitation

Personal Information may only be processed lawfully

- with consent from the data subject, or
- with justification, and
- in a manner that does not infringe on the privacy of the data subject.

Processing must be adequate, relevant, and not excessive.

Umhlanga Insurance Brokers (Pty) Ltd will not engage in any unnecessary processing of Personal Information that is not justifiable by reference to the purpose of the processing.

Consent must be: -

- voluntary, explicit, and informed.
- in writing, or recorded where it is given verbally, and
- the data subject has the right to withdraw consent

Justification–no consent for processing is required when: -

- it is necessary to perform in terms of a contract where the data subject is a party;
- it has to be done under obligation by the law;
- it is necessary to protect the legitimate interest of the data subject; or
- it is necessary to protect the legitimate interest of the Responsible Party

Personal Information may only be processed if one or more of the following applies-

- Data subject has consented
- Processing is necessary to carry out actions for conclusion/ performance of a contract to which data subject is party
- Processing complies with an obligation imposed by law
- Processing protects a legitimate interest of the data subject
- Processing is necessary for performance of a public law duty by public body
- Processing is necessary for pursuing legitimate interests of Responsible Party

Umhlanga Insurance Brokers (Pty) Ltd collects and processes a client's Personal Information in order to determine a client's needs. The type of information collected will depend on the need for which it is collected, and it will only be used for that purpose. Wherever possible the client will be informed of the information required. This information will include but not be limited to: -

- Personal details such as name, address, identity number, marital status

- Description of residence, assets, and business
- Description of assets and liabilities
- Details of existing insurance cover and investments
- Ownership certificates
- Any other information requested by an insurer to provide the client with an accurate analysis of their financial needs.

Umhlanga Insurance Brokers (Pty) Ltd will also collect and process information for marketing purposes to ensure that products and services remain applicable to clients.

Checklist for Condition 2

- Does your on boarding and fact-finding documentation include consent from prospects/clients to process their Personal Information?
- Do you collect Personal Information using third parties?
- If so, are your prospects/clients aware that you are collecting their information, and have they given consent?
- Is there a service level agreement in place with the third party?
- Does your client documentation explain to clients that you will process their Personal Information, subject to the requirements of POPIA and other legislation?
- Do you only collect data that is relevant to the purpose you are collecting data for?
- Do you give clients the option to opt out from any newsletters or campaigns that you run in your practice?

3.3 Condition 3 – Purpose specification

Personal Information must be collected for a specific, explicitly defined, and lawful purpose that is related to the service being provided, or the contractual obligation that was agreed upon.

Data subject must be aware of and understand the purpose of collecting Personal Information

Personal Information may not be kept for longer than is necessary to achieve the purpose, unless required by law, e.g., to meet the requirements of the FAIS Act, or the data subject had consented to the retention of its Personal Information.

Depending on the specific circumstances, Umhlanga Insurance Brokers (Pty) Ltd may use the Personal Information collected for one or more of the following purposes: -

- Providing products or services to clients and to carry out transactions requested
- For underwriting purposes
- Assessing and processing claims
- Conducting credit reference searches or verification
- Confirming, verifying, and updating clients' details
- Obtaining claims history
- Detection and prevention of fraud, crime, money laundering or other malpractice.
- Conducting market or customer satisfaction research
- For audit and record keeping purposes
- In connection with legal proceedings
- Providing our services to clients to carry out the services requested
- In connection with and to comply with legislative and regulatory requirements.

Umhlanga Insurance Brokers (Pty) Ltd will inform their clients as to how their Personal Information is used, disclosed, and destroyed.

Umhlanga Insurance Brokers (Pty) Ltd is committed to protecting the privacy of their clients and ensuring that the Personal Information of clients is used appropriately, transparently, securely and in accordance with all applicable legislation.

Checklist for condition 3

- Does your client documentation explain the purpose for which data is collected?
- Does your client documentation explain how long data will be kept (e.g., to meet the FAIS requirements)?

3.4 Condition 4 – Further processing limitation

Once the FSP has obtained Personal Information for specific, legitimate, and defined purposes, processing of such Personal Information may only occur as is necessary for fulfilment of those purposes.

Any further processing must be compatible with the original purpose for which it was collected.

Further processing is allowed if: -

- the information is available in a public record, or the data subject has deliberately made it public;
- further processing is necessary to maintain the law, or it is in the public interest.

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

In order to process a client's Personal Information, Umhlanga Insurance Brokers (Pty) Ltd confirms that the following will be met: -

- The client has consented to the processing of the information in writing.
- The processing is necessary to conduct an accurate analysis of the client's needs.
- Processing complies with the obligation set out in the FAIS Act to conduct a needs analysis and obtain information from a client in order to provide the client with the most appropriate product for their needs.
- Processing of the information will protect a legitimate interest of the client, to receive a full and proper needs analysis.
- Processing is necessary to pursue the legitimate interests of (name of FSP) or a third party to whom the information is supplied to ensure that the most appropriate product is recommended to the client.
- Disclosing clients' Personal Information to our providers whose services or products clients elect to use. Agreements are in place to ensure that the providers comply with confidentiality and privacy conditions.

Umhlanga Insurance Brokers (Pty) Ltd may also disclose clients' information where we have a duty or a right to disclose in terms of applicable legislation or where it may be necessary to protect our rights.

Checklist for condition 4

- Do you do any further processing of client Personal Information?
- Have you determined for yourself that the further processing is in line with the purpose for which the PI was collected in the first instance?
- If the further processing is not in line with the purpose for which the Personal Information was obtained initially, do you have any legal justification (e.g., The data subject's consent) to do the further processing?
- Is Personal Information transferred to other countries, e.g., if your data is hosted offshore in the cloud?
- Do you ensure that this information is protected adequately by law, corporate rule, or binding agreement?

3.5 Condition 5 – Information quality

Reasonable practical steps must be taken to ensure that the Personal Information is

- complete,
- accurate,
- not misleading and
- updated where necessary

It is the responsibility of the FSP to ensure and maintain the quality and accuracy of the Personal Information they process.

Any Personal Information collected from a data subject must be complete, accurate, not misleading and updated as and when it becomes necessary.

It is the representative's responsibility to ensure that a data subject's Personal Information is accurate and up to date when he/she provides it to the product provider and to contact last mentioned if correction of such information is required.

The FSP will make reasonable efforts to keep the Personal Information that is used on an on-going basis accurate and up to date.

The FSP will generally rely on a data subject to timeously provide them with updated information, such as changes to addresses and other contact information.

When maintaining the quality of the Personal Information, the purpose for which it was collected or processed further must always be considered.

If a data subject informs the FSP that his/her Personal Information is inaccurate, incomplete, out of date, or irrelevant, the FSP must revise or annotate the Personal Information.

It is the data subject's obligation to notify FSP of changes to information is included in the Disclosure form.

Checklist for condition 5

- Do you inform clients of the importance of providing complete and accurate information, and that they should inform you if data is incorrect or changes overtime?
- Do you inform clients of their obligation in terms of POPIA to advise you of any changes in their personal information as and then they occur?
- Do you review and update client information on a regular basis, e.g., when you review their financial plans?

3.6 Condition 6 - Openness

It is the Responsible Party's duty to process information in a fair and transparent manner, with due awareness of the data subject.

- Data subjects must be aware that the Responsible Party is collecting their Personal Information,
- the purpose of collection, and
- the consequences of not providing information
- Data subjects must also be informed of the source of any PI not being collected directly from them,
- whether or not it is mandatory to give their PI to the Responsible Party, and
- of their rights to object to the processing of the PI.

At the time that the personal information is gathered, the Data Subject must be advised of his/her rights to complain to the Information Regulator if misuse is suspected. The Information Regulator's information and contact details must be provided to the Data Subject – to be included in the Compliance paperwork.

Checklist for condition 6

- Do you inform clients when you collect their Personal Information what the purpose is, as well as the consequence of not providing information?
- Do you keep evidence of the consent provided by prospects and clients for the collection and processing of their information?
- Do you inform the client of their right to complain to the Information Regulator if misuse is suspected and provide the information and contact details of the Information Regulator?

3.7 Condition 7 – Security safeguards

All Personal Information should be kept secure against the risk of loss, unauthorised access, interference, modification, destruction, or disclosure.

Reasonable precautions must be taken to secure the integrity and confidentiality of PI and to prevent loss, damage, or unlawful access

The FSP will protect the integrity and confidentiality of Personal Information processed and retained and will implement measures to protect such information against unauthorised access or loss.

Umhlanga Insurance Brokers (Pty) Ltd will: -

- protect Personal Information with safeguards appropriate to the sensitivity of the information.
- have measures in place to monitor compliance with its privacy policies and procedures and to address privacy related risk assessments and verification of the implementation of safeguards, like audits.
- use care in the disposal or destruction of Personal Information in order to prevent unauthorized access.
- employ security safeguards to protect Personal Information against loss or theft, as well as unauthorised access, disclosure, copying, use, or modification. The FSP adequately addresses security measures to safeguard the privacy of Personal Information whether in electronic, paper, or other forms. The nature of these safeguards will vary depending on the sensitivity of the Personal Information that has been collected, the quantity, distribution, and format of the information as well as the method of storage.
- create and maintain awareness amongst its employees about its information security policies and procedures through on-boarding processes and security awareness drives.

The FSP must have a procedure in place to identify any foreseeable internal and external risks to personal information which can include a safety and security risk assessment looking at password usage and secure networks. The following can be considered: -

- establishing strong passwords which are regularly changed
- secure networks

- setting up a firewall
- antivirus protection
- securing desk- and laptops
- securing mobile devices including phones
- schedules backups
- regular monitoring
- be smart with e-mails and surfing the web
- educate your employees about Data Security

Where a data subject's Personal Information has been accessed or acquired by any unauthorised parties, the Responsible Party must notify:

- the information regulator; and
- data subject (unless his/her identity cannot be established)

If the data subject cannot be identified, a statement re the breach must be published The notification must be made as soon as possible after the breach is discovered.

Should a breach of personal information be identified by a staff member, then he / she must notify the office manager immediately who will then investigate the nature, circumstances and extent of the breach and then notify the Information Officer who will then notify the Information Regulator as well as the clients involved of what data was accessed. Should it not be established which clients and what data was accessed, then the Information Officer shall publish such breach in a public forum.

Checklist for condition 7

- Is all Personal Information of clients and staff in your practice stored securely, both paper and electronic versions?

- If you keep paper, is it locked away?
- Do you have a clean desk policy?
- Do you shred all paper before disposing of it?
- Have you considered scanning the information and only keeping electronic versions?
- Do you manage the access to electronic information, by your staff and any operator acting on your behalf?
- Are all devices, including computers, storage devices and servers, in your practice properly protected, e.g., with passwords, anti-virus software, encryption?
- Do your employee contracts include the responsibilities of your staff with regards to meeting POPIA conditions?
- Are your staff all made aware of the legal requirements with regards to protecting Personal Information?
- Does their training include detail on their specific responsibilities?
- Do you revoke the access of staff members when they leave your service, both to applications used in your practice and product provider applications?
- Do you keep record of prospects that you have contacted who did not give you consent for further interaction, so that you do not contact them again?
- Do you have processes in place to ensure their data is not used for any other purpose?
- Do you verify the identity of clients when you receive a request for information, to ensure that information is provided to the correct person?
- What processes do you have in place to prevent Personal Information falling into the wrong hands?
- Do you have a process to detect and report security breaches to the Information Regulator and clients or staff whose Personal Information is impacted?

3.8 Condition 8 – Data subject participation

A data subject has a right to request a copy of the information that a Responsible Party, the FSP holds. The information should be provided within a reasonable timeframe, in an understandable format and at a prescribed fee, if any.

A data subject may request a Responsible Party to correct his/her information that is inaccurate, irrelevant, out-of-date, misleading, or obtained in a manner not permitted by law.

They may also request that their information be deleted or destroyed should the Responsible Party no longer be authorised to hold their Personal Information.

All client information is stored in hard copy format on-site in filing cabinets as well as electronically on an external hard drive.

Umhlanga Insurance Brokers (Pty) Ltd is obligated to keep copies of all financial services rendered to clients for a minimum period of 5-years, or 5-years after the business relationship has terminated or for 5-years after the termination of the policy whereafter all such files are to be destroyed on an annual basis.

These are files that have been stored for a minimum period of 5 (FIVE) years, as is required by the Financial Advisers & Intermediary Services (FAIS) Act and / or the General Code of Conduct to the FAIS Act and / or the Financial Intelligence Centre (FIC) Act. Eternity Financial Consulting (Pty) Ltd destroys these files according to a protocol that is POPI compliant.

Umhlanga Insurance Brokers (Pty) Ltd will, upon receiving a request in writing, inform an individual of the existence, use and disclosure of his/her Personal Information and will provide access to that information, except where the law requires or permits the FSP to deny access.

Checklist for condition 8

- Do you inform clients about their rights to access and ask for correction or deletion of information?
- Do you keep record of any third party you provided Personal Information to?
- Do you have a process to retrieve the necessary information on request?

4. PROCESSING OF PERSONAL INFORMATION OF CHILDREN

A responsible party may, subject to section 35, not process personal information concerning a child unless

- carried out with the prior consent of a competent person;
- necessary for the establishment, exercise, or defence of a right or obligation in law;
- necessary to comply with an obligation of international public law;
- for historical, statistical or research purposes to the extent that -
    1. the purpose serves a public interest, and the processing is necessary for the purpose concerned; or
    2. it appears to be impossible or would involve a disproportionate effort to ask for consent,
    3. and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; or
- of personal information which has deliberately been made public by the child with the consent of a competent person.

The Regulator may, notwithstanding the prohibition referred to in section 34, but subject to subsection (3), upon application by a responsible party and by notice in the Gazette, authorise a responsible party to process the personal information of children if the processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the child.

The Regulator may impose reasonable conditions in respect of any authorisation granted under subsection (2), including conditions with regard to how a responsible party must—

a. upon request of a competent person provide a reasonable means for that person to —
    i. review the personal information processed; and
    ii. refuse to permit its further processing;
b. provide notice —

i. regarding the nature of the personal information of children that is processed;
ii. how such information is processed; and
iii. regarding any further processing practices;

c. refrain from any action that is intended to encourage or persuade a child to disclose more personal information about him- or herself than is reasonably necessary given the purpose for which it is intended; and
d. establish and maintain reasonable procedures to protect the integrity and confidentiality of the personal information collected from children.

5. TRANSFER OF PERSONAL INFORMATION OUTSIDE THE REPUBLIC

A responsible party in the Republic may not transfer personal information about a data subject to a third party who is in a foreign country unless the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that:-

1. effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and

2. includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;

- the data subject consents to the transfer;
- the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or
- the transfer is for the benefit of the data subject, and—

1. it is not reasonably practicable to obtain the consent of the data subject to that transfer; and
2. if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

6. EXCLUSIONS

This Act does not apply to the processing of personal information—

- in the course of a purely personal or household activity;
- that has been de-identified to the extent that it cannot be re-identified again;
- by or on behalf of a public body—

1. which involves national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defence, or public safety; or

2. the purpose of which is the prevention, detection, including assistance in the identification of the proceeds of unlawful activities and the combating of money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in legislation for the protection of such personal information;

    - by the Cabinet and its committees or the Executive Council of a province; or
    - relating to the judicial functions of a court referred to in section 166 of the Constitution.

3. "Terrorist and related activities", for purposes of subsection (1)(c), means those activities referred to in section 4 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 (Act No. 33 of 2004).

7. NON-COMPLIANCE

Section 107 of POPIA deals with Penalties and any person convicted of contravening:

- sections 100 (Obstruction of the Regulator), 103 (Failure to comply with enforcement or information notices, 104 (Offences by witnesses), 105 (Unlawful acts by responsible party in connection with account number, 106 (Unlawful acts by third parties in connection with account number,

  to a fine or to imprisonment for a period not exceeding 10 years, or to both a fine and such imprisonment; or

- sections 59 (Failure to notify processing subject to prior authorisation), section 101 (Breach of Confidentiality), 102 (Obstruction of execution of warrant), section 103(2) (Failure to comply with enforcement or information notices - making a statement that is knowingly or recklessly false or 104 (1) (Offences by witnesses), to a fine or to imprisonment for a period not exceeding 12 months, or to both a fine and such imprisonment.

Section 109 deals with Administrative fines, which amount may, subject to subsection (10), where the Regulator can increase such amounts in terms of CP, may not exceed R10 million.