THE PROTECTION OF PERSONAL INFORMATION ACT (POPIA) POLICY)

V1.2

Unit 1, Village Corner, 57 via Latina Crescent, Irene Corporate Corner, Irene, South Africa PO Box 61803, Pierre Van Ryneveld, Centurion, Gauteng, 0045
Company Reg: 1999/008361/07 **Director:** Mark Weetman **External Compliance:** Mrs Shashika Adsetts, Moonstone Compliance, CO 6220

+27 (0)11 384 2900 info@unum.co.za @unumcapital www.unum.co.za

1. DEFINITIONS

"Act" means the Protection of Personal Information Act 4 of 2013;

"***consent***" means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;

"data subject" means the person to whom personal information relates;

"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.

"Information Officer" means the person appointed that is responsible for ensuring the organisation's compliance with POPIA. This person must be registered with the South African Information Regulator.

"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 organisation 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.

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

(a) Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

(b) information relating to the education or the medical, financial, criminal or employment history of the person;

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

(d) the biometric information of the person;

(e) the personal opinions, views or preferences of the person;

(f) 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;

(g) the views or opinions of another individual about the person; and

(h) 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;

"Policy" means this policy on the lawful processing and protection of client information;

"Procedure" means a statement or number of statements, contained in a separate yet linked document, the effect of which is to prescribe those things that must be done or omitted in order to ensure adherence with this policy and the Act;

"Processing" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including-

(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

(b) dissemination by means of transmission, distribution or making available in any other form; or

(c) merging, linking, as well as restriction, degradation, erasure or destruction of information.

"Re-identify" In relation to personal information of a data subject, means to revive any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

"Responsible party" means any person who determines the purpose of and means for processing personal information.

2. 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 in a context-sensitive manner. Through the provision of quality goods and services, Unum Capital (Pty) Ltd **'Unum'** 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. The absence of this policy and procedure will expose the company to unnecessary risk and create a burden in respect of financial and other regulatory requirements. Unum subscribes to the principles espoused in the Protection of Personal Information Act and the Constitution of South Africa in respect of:

- The lawful processing of client data by the company acting as a responsible corporate citizen; and
- The identification and allocation of accountability, where personal data is processed contrary to the prescripts of the Act.

3. POLICY PURPOSE

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

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

4. SCOPE AND APPLICATION

This policy shall apply in respect of:

4.1. The lawful processing of Personal Information

The following conditions for processing of personal information must be met prior to any processing of personal data:

- The purpose of use of the data and the manner in which data was obtained are lawful;
- The use of the data does not infringe on the privacy of the client;
- The extent of the data obtained is commensurate with the purpose for which it is being processed; and
- The data subject's consent was obtained, or processing is otherwise necessitated to comply with laws;
- We shall obtain data directly from the data subject unless required by law to obtain data from another source; and
- Where we obtain data from another source such as third-party processors, we shall have a written agreement in place with such providers, bearing in mind that the data subject may at any time object to our processing of such data, in which case we must stop unless precluded to do so by law.

4.2. We shall not process information regarding a data subject in respect of;

- the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information;
- the criminal behaviour of a data subject to the extent that such information relates to- the alleged commission by a data subject of any offence; or
- any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings unless the data subject has consented to such processing or unless otherwise required by another law.
- We shall not process data regarding children unless authorised by such children's guardian or otherwise as required by law.

5. GENERAL GUIDING PRINCIPLES

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

5.1. 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.

Unum 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 Unum 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.

5.2. Processing Limitation

Unum will ensure that personal information under its control is processed:

- in a fair, lawful and non-excessive manner, and
- only for a specifically defined purpose.

Unum will inform the data subject of the reasons for collecting his, her or its personal information. Alternatively, where services or transactions are concluded over the telephone or electronic means, Unum will maintain a voice recording of the stated purpose for collecting the personal information and make sure that this conversation is kept and backed.

Unum 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 FSP's business and be provided with the reasons for doing so and the data subject shall also provide the consent for this.

5.3. Purpose Specification

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

5.4. 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 data subject.

5.5. Information Quality

Unum will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading.

Where personal information is collected or received from third parties, Unum 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.

5.6. Open Communication

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

Unum maintains a **"contact us"** facility, via its website or data subjects may contact the client support desk (clientsupport@unum.co.za), if the data subjects want to:

- Enquire whether the FSP holds related personal information, or
- Request access to related personal information, or
- Request the FSP to update or correct related personal information, or
- Make a complaint concerning the processing of personal information.

5.7. Security Safeguards

Unum 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.

Unum 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.

Unum 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 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.

Unum'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.

5.8. Data Subject Participation

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

Unum will ensure that it provides a facility for data subjects who want to request the correction of deletion of their personal information. These forms shall be found on the website or by request from the company website.

Where applicable, Unum will include a link to unsubscribe from any of its electronic newsletters or related marketing.

6. PROTECTION OF DATA

We shall ensure that data in our possession is secure and confidential so as to protect us against loss, unlawful access or accidental destruction of data.

6.1. In so doing, we shall take measures to incorporate data protection in our risk management framework and adapt our risk management practices so as to align them, insofar as data protection is concerned, with generally accepted data security practices and procedures.

6.2. We shall ensure that any service provider to whom we outsource any aspect relating to data collection abides by the terms of this policy.

6.3. We shall ensure, in the event of a breach of security regarding data that we notify the Regulator and the affected data subjects as soon as reasonably possible, by such means and media as are appropriate in the circumstances to enable them to take steps to protect their interests.

6.4. We shall ensure, when requested to transfer data across the borders of South Africa, that we do so only with the consent of the data subject and thereafter only to a jurisdiction which has rules on the protection of data substantially similar to those contained in this policy and the Protection of Personal Information Act.

6.5. All electronic data are backed up by Unum's Information Technology Provider who is also responsible for system security which protects third party access and physical threats to data.

7. DATA SUBJECTS RIGHTS

7.1. 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 POPI and to institute civil proceedings regarding the alleged non-compliance with the protection of his/her or its personal information. The complaint form may be found in Unum Complaints policy, which can be accessed on the www.unum.co.za under the Regulation tab or alternatively may be requested by the data subject from clientsupport@unum.co.za.

7.2. 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.

7.3. The data subject has the right to request, where necessary, that his/her or its personal information must be corrected or deleted where the FSP is no longer authorised to retain the personal information. The request form is on **Annexure A**.

7.4. The data subject has the right, on reasonable grounds, to object to the processing of his/her or its personal information. In such situations, Unum will give due consideration to the request and the requirements of POPI. Unum 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.

7.5. The data subjects has a right to access and/or request access to such personal information that Unum holds on them. The personal information request form is marked as **(Annexure A)**

8. DUTIES OF THE INFORMATION OFFICER

We have appointed an Information Officer, the purpose of which is to ensure compliance with this policy. The duties of the Information Officer include:

8.1. Taking steps to ensure the FSP's reasonable compliance with the provision of POPI.

8.2. Keeping senior management updated about the FSP's information protection responsibilities under POPI.

8.3. Reviewing the FSP's information protection procedures and related policies.

8.4. Ensuring that POPI audits are scheduled and conducted on a regular basis.

8.5. Ensuring that the FSP makes it convenient for data subjects who want to update their personal information or submit changes to their personal information.

8.6. Managing all POPI related complaints to the FSP.

8.7. Ensuring the maintenance of a "contact us" facility on the FSP's website.

8.8. Approving any contracts entered into with operators, 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.

8.9. Encouraging compliance with the conditions required for the lawful processing of personal information.

8.10. 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.

8.11. Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the FSP.

8.12. Addressing employees' POPI related questions.

8.13. Addressing all POPI related requests and complaints made by the FSP's data subjects.

The Deputy Information Officer will assist the Information Officer in performing his/ her duties.

9. EMPLOYEES REQUIREMENTS CONCERNING POPIA

9.1. Ensuring that personal information is held in as few places as necessary. No unnecessary additional records, filing systems and data sets should therefore be created.

9.2. Ensuring that personal information is encrypted, or password protected prior to sending or sharing the information electronically. The IT Service Provider will assist employees and where required, other persons acting on behalf of the FSP, with the sending or sharing of personal information to or with authorised external persons.

9.3. 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. Personal Information that is stored in phones is deleted once filed internally.

9.4. Ensuring that computer screens and other devices are switched off or locked when not in use or when away from their desks.

9.5. Ensuring that where personal information is stored on removable storage media such as external drives, that these are kept locked away securely when not being used.

9.6. 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.**

9.7. 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. All unwanted print outs should be shredded.

9.8. 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.

9.9. 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.

9.10. Undergoing POPI Awareness training from time to time.

9.11. 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.

10. DISCLOSURE AND CONSENT FOR CUSTOMER DUE DILIGENCE IN TERMS OF THE FINANCIAL INTELLIGENCE CENTRE ACT

10.1. Unum is an accountable institution as defined in the Financial Intelligence Centre Act. As such, we are required by law to obtain and process information about our Clients for the purposes of conducting Customer Due Diligence" (CDD) which includes enhanced due diligence. The purpose of CDD is to determine the risk that the Client may be engaged in money-laundering and/or terror-financing activities. We are required to obtain and process information about our Clients in respect of the following:

10.1.1. The Client identity and that of any person whom the Client purport to represent, including the Clients status as a prominent person as defined in the act;

10.1.2. The Clients place of residence and/or registration of business;

10.1.3. The Client status as defined by reference to sections 26A (i.e. whether they are a person against whom financial sanctions have been imposed) and section 28A (i.e. whether they are a person in respect of whom there is an absolute prohibition against doing business with);

10.1.4. The nature and ownership/control structure of the Clients business; and

10.1.5. The nature of our products and services, how they relate to the Clients' requirements and how they use them.

10.1.6. In certain circumstances and in the course of our CDD activities, we may avail ourselves of detail available about the Client in the public domain as well as additional detail we require to verify some of the information we collect about the Client. These sources may include commercially and publicly available information with regards to references made about and by the Client in, including but not limited, the press and media including social media, law enforcement agencies such as Interpol and information collected and processed about the Client by credit bureau and similar agencies including the verification of bank account details in the Clients' name.

10.1.7. The Client will be required to consent to and authorize us and any agency lawfully appointed by us to obtain and process the information as described above as part of our duty in law.

11. STANDARDS AND APPLICATION

In adopting the processes required to give effect to this policy, we shall at all times adhere to the highest standards set by the South African Regulatory Authority. This policy document shall be circulated to all employees, authorised representatives with a view of them assessing the extant process requirements and making recommendations to the Department of Compliance in respect of any changes required to meet the demands of this policy.

12. OBLIGATION BY EMPLOYEES

All employees have an obligation to promote the compliance culture as well as adhering to the provisions of this policy. Disregard for the compliance philosophy, compliance culture and failure to comply with any provisions of the legislation or this policy will result in remedial and/or disciplinary action being taken.

13. Penalties for non-compliance.

There are essentially two legal penalties or consequences for serious breaches of POPI for the responsible party:

13.1. A fine of between R1 million and R10 million and/or imprisonment of one to ten years; or

13.2. Paying compensation to data subjects for the damage they have suffered.

Other penalties include:

13.3. Reputational damage.

13.4. Losing clients (and employees).

13.5. Failing to attract new clients.

14. IMPLEMENTATION

This policy will be made available and distributed to all employees and representatives working in or on behalf of the organisation. Executive Management is responsible to ensure that this policy is communicated, observed and that it remains appropriate on an ongoing basis.

15. ENDORSEMENT

This policy is approved and endorsed by Executive Management.

16. REVIEW OF POLICY

This policy will be reviewed by Executive Management in consultation with the Information Officer on an annual basis or more frequently in the event of material amendments to the regulatory environment and may be altered and improved at any time and will be enforceable with immediate effect. All changes and amendments will be communicated and distributed to all stakeholders who will be required to adhere to such changes without delay.

17. AUTHORITY

The Information Officer is hereby appointed to act in terms of this policy and is specifically furnished with the power to delegate any functions to one or more deputies.

18. OWNERSHIP & ACCOUNTABILITY

This policy is owned by **Unum Capital (PTY) LTD**, an authorised financial services provider in terms of the Financial Advisory & Intermediary Services Act (37 of 2002) and subordinate legislation.
As Key Individual of the Provider, I, **Mark Weetman** hereby confirm the adoption of the policy on behalf of the governing body of the Provider.

I hereby accept responsibility for the successful training of employees and successful implementation of this Policy.

11 December 2023

Signature Date