



ENIGMA SOLUTIONS (Pty) Ltd
Creative Employee Benefits Consulting

Company Registration No: 2000/003098/07

Financial Services Provider no: 1731

**POLICY
ON
PROTECTION OF PERSONAL INFORMATION
(POPIA)**

Contents	Page number
Definitions	3-6
1. Introduction	7
2. Object of the policy	7
3. Scope	7
4. Use of personal information	7-8
5. Key Principles	8
6. Accountability	9
7. Limitations on processing personal information	9-10
8. Purpose specific, retention and restriction of information	10
9. Limitations of further processing of personal information	10-11
10. Quantity of information	11
11. Transparency / Openness	11
12. Security safeguards	11-12
13. Data subject participation	12
14. Monitoring and enforcement	13
15. Standard operating procedures	13
16. Complaints and concerns	13
17. Ownership	13
18. Review of policy	14
19. Interpretation	14
20. Policy approval	14

DEFINITIONS

“biometrics”	means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;
“child”	means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself;
“code of conduct”	means a code of conduct of the Fund
“competent person”	means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child;
“consent”	means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;
“Constitution”	means the Constitution of the Republic of South Africa, 1996;
“data subject”	means the person to whom personal information relates;
“de-identify”,	in relation to personal information of a data subject, means to delete any information that— <ul style="list-style-type: none">(a) identifies the data subject;(b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or(c) can be linked by a reasonably foreseeable method to other information that identifies the data subject, and
“de-identified”	has a corresponding meaning;
“information officer”	of, or in relation to, a— <ul style="list-style-type: none">(a) public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17 of POPI; or(b) private body means the head of a private body as contemplated in section 1 of the Promotion of Access to Information Act;

“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;
“person”	means a natural person or a juristic person;
“personal information”	<p>means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—</p> <ul style="list-style-type: none"> (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;
“processing”	<p>means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—</p> <ul style="list-style-type: none"> (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

“record”	<ul style="list-style-type: none"> (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; <p>means any recorded information—</p> <ul style="list-style-type: none"> (a) regardless of form or medium, including any of the following: <ul style="list-style-type: none"> (i) Writing on any material; (ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored; (iii) label, marking or other writing that identifies or describes any thing of which it forms part, or to which it is attached by any means; (iv) book, map, plan, graph or drawing; (v) photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced; (b) in the possession or under the control of a responsible party; (c) whether or not it was created by a responsible party; and (d) regardless of when it came into existence;
“Regulator”	<p>means the Information Regulator established in terms of section 39 of POPI;</p>
“Responsible party”	<p>means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;</p>
“special personal information”	<p>means-</p> <ul style="list-style-type: none"> (a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or

- (b) the criminal behaviour of a data subject to the extent that such information relates to—
 - (i) the alleged commission by a data subject of any offence;
or
 - (ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

1. Introduction

Enigma Solutions (Pty) Ltd (“Enigma”) recognises that section 14 of the Constitution of the Republic of South Africa, 1996 provides that everyone has the right to privacy. The right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information. The Enigma undertakes to respect, protect, promote and fulfil the rights in the Bill of Rights.

2. Object of the Policy

The policy provides general principles regarding the safeguard of member’s personal information and their right to privacy.

3. Scope

This policy explains how Enigma obtains, uses and discloses personal information of its members, in line with best practice and as required by the Protection of Personal Information Act (“POPI”).

Enigma is committed to protecting its member’s privacy and to ensure that their personal information is collected and used properly, lawfully and transparently.

4. Use of personal information

Member’s Personal Information will only be used for the purpose for which it was collected and agreed. This may include:

- 4.1 Providing products or services to members and to carry out the transactions requested;
- 4.2 For underwriting purposes;
- 4.3 Assessing and processing claims;
- 4.4 Conducting credit reference searches or verification;
- 4.5 Confirming, verifying and updating clients details;
- 4.6 For purposes of claims history;
- 4.7 For the detection and prevention of fraud, crime, money laundering or other malpractice;
- 4.8 Conducting market or customer satisfaction research;
- 4.9 For audit and record keeping purposes;

- 4.10 In connection with legal proceedings;
- 4.11 Providing services to clients to carry out the services requested and to maintain and constantly improve the relationship; and
- 4.12 In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

5. Key Principles

Enigma is committed to the following principles:

- 5.1 To be transparent in its standard operating procedures which govern the collection and processing of personal information.
- 5.2 To comply with all applicable legal and regulatory requirements regarding the processing of personal information.
- 5.3 To collect personal information by lawful and fair means and to process personal information in a manner compatible with the purpose for which they were collected.
- 5.4 Where required by law and according to local requirements, to inform members when personal information is collected about them.
- 5.5 Where required by law, regulations or guidelines, to obtain member's consent to process their personal information.
- 5.6 To strive to keep personal information accurate, complete and up-to-date and reliable for their intended use.
- 5.7 To strive to develop reasonable security safeguards against such risks as loss or, unauthorized access, destruction, use, modification or disclosure of personal information.
- 5.8 To strive to provide members with the opportunity to access the personal information relating to them and, where applicable, to comply with requests to correct, amend or rectify the personal information, where incomplete, inaccurate or not compliant with the standard operating procedures.
- 5.9 To share personal information, such as permitting access, transmission or publication, with third parties only with a reasonable assurance that the recipient will apply suitable privacy and security protection to the personal information.
- 5.10 To comply with any restrictions and requirements that applies to the international transfer of personal information.

6. Accountability

- 6.1 Enigma is responsible for member's personal information in its possession or control, including information that may be transferred by it to third parties for processing. Enigma require such third parties to keep personal information under strict standards of privacy and protection.
- 6.2 Enigma adheres to legislated and self-imposed rules, aimed to safeguard member's privacy. The rules are established by this Policy, the Code of Conduct, industry guidelines and applicable law.

7. Limitations on Processing Personal Information

- 7.1 Enigma ensures that the member's personal information is collected or processed under strict and lawful means with the expressed authority of the Information Officer in a manner that is reasonable and that does not compromise the privacy of the member.
- 7.2 The information that is collected or processed must be relevant to the purpose it is required, adequate and not excessive.
- 7.3 Enigma limits the collection of member's personal information to what it needs in relation to the purposes identified to the members.
- 7.4 Enigma collect the information directly from the members unless the member allows it to collect information from a third party or in accordance with the law.
- 7.5 Enigma limits the use of member's personal information to the purposes it has identified to such member. This means that Enigma cannot use member's personal information for other purposes without the member's consent, except as required by law.
- 7.6 Enigma will not disclose the member's personal information to anyone except with the member's consent or as required by law.
- 7.7 The member's personal information is only accessible to certain authorized persons, and only to the extent necessary to perform their duties.
- 7.8 When Enigma collects personal information from the employer or the members as the case may be, it obtains the member's consent to use the information for the purposes collected or processed. Enigma will obtain consent from members for any additional use or collection, or if the purpose of using the information is changed.
- 7.9 Enigma generally seeks the member's express written consent in order to collect, use or disclose personal information. Where appropriate, for less sensitive information, Enigma may accept verbal consent.

- 7.10 Consent must be given by the member or his/her authorized representative such as a legal guardian or a person having power of attorney.
- 7.11 The members may withdraw their consent at any time, subject to legal or contractual restrictions. Enigma will inform the members of the consequences of such withdrawal, including the possibility that it may not be able to provide a product or process a request. If the member chooses not to consent, Enigma will record the decision in the member's file.
- 7.12 In limited circumstances, Enigma have the right (or obligation) to collect, use or disclose personal information without the member's knowledge and consent. This occurs when legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the investigation of a potential breach of contract, the prevention or detection of fraud, or for law enforcement purposes, seeking consent might defeat the purpose of the information collection.

8. Purpose Specific, Retention and Restriction of Information

- 8.1 Enigma will ensure that member information will at all times be collected for an explicitly defined and specific purpose and for the lawful use by the responsible party.
- 8.2 Extra measures must be in place to ensure that the member whose information is collected, knows and understand the reason for which the information is collected unless it is to comply with an obligation imposed by law
- 8.3 Enigma only retains personal information of members for as long as needed for the purpose it was collected or to enforce a lawful right. Enigma destroys this information in accordance with its file retention guidelines. When Enigma destroys the member's personal information, it ensures that confidentiality is secured and that no unauthorized person can access the information during the destruction process.

9. Limitations on Further Processing of Personal Information

Enigma will ensure that there is an exact correlation between the personal information collected or processed and the reasons for which the personal information is needed. Therefore:

- 9.1 Enigma will assess whether there is a relationship between the purpose for which the intended further processing and the reason for which the information is need is aligned.

- 9.2 Whether the nature, the manner, the rights and the consequences of the further processing of the personal information are protected in law.

10. Quality of Information

Enigma makes every possible effort to ensure that member's personal information is as accurate and complete as necessary for the purposes it is collected, used, or disclosed.

11. Openness and Transparency

- 11.1 The members have the right to know, on request, to whom the information was disclosed. Only in rare instances will Enigma be prevented by law from making such disclosure.
- 11.2 Enigma will maintain accurate records, recording to whom it disclosed personal information and in what circumstances it was disclosed.
- 11.3 Enigma will occasionally share the member's personal information with service providers such as actuaries, investment consultants and insurers to ensure the proper administration of products, or to provide the members with the services they require. These service providers or agents must agree to comply with privacy legislation before receiving any personal information.

12. Security Safeguards

- 12.1 Enigma have implemented and continue to implement rigorous safeguards so that member's personal information remains strictly confidential and is protected against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification.
- 12.2 Protection methods include organizational measures such as limiting access to a "need-to-know" basis and physical measures (e.g. biometric for employees, visitor registration, off-site backups and archiving), and technological measures such as the use of password and encryption (e.g. the use of routinely changing passwords, firewalls and segmented operator access).
- 12.3 Enigma will continuously review its security controls and processes to ensure that member's personal information is secure.

- 12.4 Enigma will further review the operational ability of operators it is connected to ensure that the spirit and letter of the Act is maintained.

13. Data Subject Participation

- 13.1 The members and beneficiaries have the right to be informed whether Enigma holds personal information about them and to see that information. Members also have the right to enquire as to how the Enigma collected their information, how it used it and to whom it may have been disclosed.
- 13.2 This information will be provided to members within a reasonable time from the date Enigma receives their written request. Enigma may charge a reasonable fee for processing member's request.
- 13.3 In certain limited and specific circumstances, Enigma may refuse to provide to members with the requested information. Exceptions to the member's access right can include information that contains references to other individuals, information that cannot be disclosed for legal, security or commercial proprietary reasons, information that has been obtained in the course of an investigation of a potential breach of contract or fraud, and information that is subject to attorney-client or litigation privilege.
- 13.4 Members and beneficiaries may challenge the accuracy and completeness of their personal information, in which case, they may respond to an amended request within a reasonable time.
- 13.5 Any request for access to information or request for amendment must be sent to the following address:

The General Manager
Enigma Solutions (Pty) Ltd
Enigma House, Unit 2
15 Maria Street
Fontainebleau
Randburg
2194

14. Monitoring and enforcement

Enigma will administer and oversee implementation of this policy and, as applicable, supporting guidelines, standard operating procedures, notices, consents and appropriate related documents and processes. It will conduct periodic reviews and audits, where appropriate, to demonstrate compliance with POPI, policy and guidelines.

15. Standard Operating Procedures

15.1 Enigma will establish appropriate privacy standard operating procedures that are consistent with this policy and industry practices as well as legal and regulatory requirements.

15.2 Enigma will similarly ensure that all operators connected to them have demonstrable and documented standard privacy operating procedures, to ensure the integrity of record keeping and the safe guard of member's personal information in their possession.

16. Complaints and Concerns

Should anyone be unsatisfied with our officer's or representative's response, he/she may contact the Information Officer at the address:

The General Manager
Enigma Solutions (Pty) Ltd
Enigma House, Unit 2
15 Maria Street
Fontainebleau
Randburg
2194

A complaint concerning the protection of personal information should be addressed to the Information Officer at the address provided above.

17. Ownership

The ultimate responsibility for ensuring that appropriate standards and processes are in place to ensure fairness outcomes for the members rests with the Directors of Enigma.

18. Review of Policy

This Policy will be reviewed as and when required, but at least annually. Any changes to the Policy shall be communicated immediately to all members of Enigma.

19. Interpretation


In the event of any inconsistency between this Policy and the POPI Act, the POPI Act shall prevail.

20. Policy approval

This Policy was approved electronically by Enigma Solutions (Pty) Ltd on 30 June 2021 and is considered the official POPIA policy of Enigma Solutions (Pty) Ltd with effect from 1 July 2021.



Chief Executive Officer



General Manager/Information Officer