



**Data Privacy Policy:
Knowledge Objects Healthcare (Pty) Ltd & Knowledge
Objects Solutions (Pty) Ltd**

July 2021

Table of Contents

1. Definition of terms.....	3
2. Acronyms / Abbreviations	3
3. Introduction to the Data Protection Policy.....	3
3.1. Background.....	3
3.2. Purpose of the Data Protection Policy	3
3.3. Scope	3
3.4. Policy Review	3
4. Protection of Personal Information in Terms of POPIA	3
4.1. Personal Information Collected	3
4.2. The Usage of Personal Information	4
4.3. Disclosure of Personal Information	4
4.4. Safeguarding Stakeholders' Personal Information	5
4.5. Access and Correction of Personal Information	6
5. Retention & Confidentiality of Documents, Information and Electronic Transactions	6
5.1. Access to documents	6
6. Destruction of documents	7
7. Non-compliance with the Policy	7
8. Availability of the PAIA Manual.....	7
9. Information Officer Details.....	7
10. Deputy Information Officer Details.....	9

1. DEFINITION OF TERMS

Term	Description
Personal Information	Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person.

2. ACRONYMS / ABBREVIATIONS

Abbreviation	Description
PAIA	Promotion of Access to Information Act 2 of 2000
POPIA	Protection of Personal Information Act 4 of 2013

3. INTRODUCTION TO THE DATA PROTECTION POLICY

3.1. BACKGROUND

This policy applies to the entities **Knowledge Objects Healthcare (Pty) Ltd** and **Knowledge Objects Solutions (Pty) Ltd**. Both entities are South African based companies that specialise in the latest-generation risk management and higher automation solutions across the insurance and healthcare industry. Both entities will be referred to as “**The Companies**” in this document.

The Companies guarantees their commitment to protecting its stakeholders' privacy and ensuring that their personal information is used appropriately, transparently, securely and under applicable laws.

3.2. PURPOSE OF THE DATA PROTECTION POLICY

The Policy sets out how the organisations deal with their stakeholders' personal information and stipulates the purpose for which such personal information is used. The Policy is made available on **The Companies'** website (www.knowledgeobjects.com) and by request from the head office.

3.3. SCOPE

The Policy applies to all employees, third parties, and all other users of **The Companies'** ICT facilities and all forms of information resources.

3.4. POLICY REVIEW

The Policy will be reviewed annually. Interim changes might be approved by the Executive Committee if they are not material. Material changes must be approved by the Board. Stakeholders are advised to access **The Companies'** website periodically to keep abreast of any changes to the Policy. Where material changes take place, stakeholders will be notified directly or changes will be updated on the website.

4. PROTECTION OF PERSONAL INFORMATION IN TERMS OF POPIA

4.1. PERSONAL INFORMATION COLLECTED

Section 9 of POPIA 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 Companies collect and process personal information as received from the stakeholders or specifically relating to the stakeholders' 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, **The Companies** will inform the stakeholder as to the information required and the information deemed optional.

Website usage information may be collected using "cookies" which allows **The Companies** to collect standard internet visitor usage information.

4.2. THE USAGE OF PERSONAL INFORMATION

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

This may include the following:

- ❖ Providing services to stakeholders and carrying out the transactions requested;
- ❖ For sharing with other third parties, if necessary;
- ❖ Processing applications for medical aids, insurance and non-insurance products;
- ❖ Processing medical claims and other related non-medical claims for payment;
- ❖ Confirming, verifying and updating stakeholders' details;
- ❖ For the detection and prevention of fraud, crime, money laundering;
- ❖ For audit and record-keeping purposes;
- ❖ In connection with legal proceedings;
- ❖ Providing communication in respect of **The Companies** and regulatory matters that may affect stakeholders; and
- ❖ In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

According to section 10 of POPIA, personal information may only be processed if certain conditions, listed below, are met along with supporting information for the processing of personal information:

- ❖ The stakeholder consents to the processing: - consent is obtained from stakeholders during the introductory, appointment and application stage of the relationship;
- ❖ Processing complies with an obligation imposed by the Medical Schemes Act, as well as other related legislation; and
- ❖ Processing protects the legitimate interest of the stakeholder.

4.3. DISCLOSURE OF PERSONAL INFORMATION

The Companies may disclose a stakeholder's personal information to any of its third-party service providers. **The Companies** has agreements in place to ensure compliance with confidentiality and privacy conditions.

The Companies may also share personal information with, and obtain information about stakeholders from third parties for the reasons already discussed above.

The Companies may also disclose a stakeholder's information where it has a duty or a right to disclose in terms of applicable legislation, the law, or where it may be deemed necessary to protect its rights.

4.4. SAFEGUARDING STAKEHOLDERS' PERSONAL INFORMATION

POPIA requires **The Companies** to adequately protect personal information. **The Companies** continuously reviews their security controls and processes to ensure that personal information is secure.

The following procedures are in place to protect personal information:

- (i) The Information Officer for **Knowledge Objects Healthcare (Pty) Ltd** is Chantal Viljoen. Her details are available below and she is responsible for the compliance with the conditions of the lawful processing of personal information and other provisions of POPIA for **Knowledge Objects Healthcare (Pty) Ltd**;
- (ii) The Information Officer for **Knowledge Objects Solutions (Pty) Ltd** is Dr Dena van den Berg. Her details are available below and she is responsible for the compliance with the conditions of the lawful processing of personal information and other provisions of POPIA for **Knowledge Objects Solutions (Pty) Ltd**;
- (iii) This Policy has been put in place throughout **The Companies** and training on this Policy and the POPIA Act has already taken place;
- (iv) Each new employee is required to sign an employment contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPIA;
- (v) Every employee currently employed within **The Companies** is required to sign an addendum to their employment contracts containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPIA;
- (vi) **The Companies'** archived stakeholder information is stored in the cloud in a secure location that is password-protected as governed by POPIA, and access is limited to these areas to authorised personnel;
- (vii) **The Companies'** suppliers, insurers and other third-party service providers are required to sign a service level agreement guaranteeing their commitment to the Protection of Personal Information. This is however an ongoing process that is evaluated as needed;
- (viii) All electronic files or data are backed up by **The Companies** which is also responsible for system security that protects third party access and physical threats. **The Companies** are responsible for Electronic Information Security; and
- (ix) **The Companies'** policies and procedures cover the following:
 - ❖ Physical security;
 - ❖ Computer and network security;
 - ❖ Access to personal information;
 - ❖ Secure communications;
 - ❖ Security in contracting out activities or functions;
 - ❖ Retention and disposal of information;

- ❖ Acceptable usage of personal information;
- ❖ Governance and regulatory issues;
- ❖ Monitoring access and usage of private information; and
- ❖ Investigating and reacting to security incidents.

Consent to process stakeholder information is obtained from stakeholders (or a person who has been given authorisation from the stakeholder to provide the stakeholder's personal information) during the introductory, appointment and application stage of the relationship.

4.5. ACCESS AND CORRECTION OF PERSONAL INFORMATION

- (i) Stakeholders have the right to access the personal information **The Companies** holds about them;
- (ii) Stakeholders also have the right to ask **The Companies** to update, correct or delete their personal information on reasonable grounds;
- (iii) Once a stakeholder objects to the processing of their personal information, **The Companies** may no longer process said personal information; and
- (iv) **The Companies** will take all reasonable steps to confirm their stakeholders' identity before providing details of their personal information or making changes to their personal information.

The details of **The Companies'** Information Officers are shown below.

5. RETENTION & CONFIDENTIALITY OF DOCUMENTS, INFORMATION AND ELECTRONIC TRANSACTIONS

5.1. ACCESS TO DOCUMENTS

- (i) All personal information is dealt with in the strictest confidence and may only be disclosed, without fear of redress, in the following circumstances:
 - ❖ where disclosure is under compulsion of law;
 - ❖ where there is a duty to the public to disclose; and
 - ❖ where the interests of **The Companies** require disclosure.
- (ii) Disclosure to 3rd parties
 All employees have a duty of confidentiality concerning **The Companies** and their stakeholders. In addition to the provisions of clauses above, the following are also applicable:
 - ❖ Information on stakeholders: Our stakeholders' right to confidentiality is protected in the Constitution and terms of legislation. Information may be given to a 3rd party if the stakeholder has consented in writing to that person receiving the information;
 - ❖ Requests for **The Companies** information: These are dealt with in terms of PAIA, which gives effect to the constitutional right of access to information held by the State or any person (natural and juristic) that is required for the exercise or protection of rights. **The Companies** may however refuse access to records if disclosure would constitute an action for breach of the duty of secrecy owed to a third party.

In terms hereof, requests must be made in writing on the prescribed form to the Information Officer in terms of PAIA. The requesting party has to state the reason for wanting the information and has to pay a prescribed fee.

The Companies' manual in terms of PAIA, which contains the prescribed forms and details of prescribed fees, is available on the website www.knowledgeobjects.com.

- ❖ Confidential information of **The Companies** and/or business information may not be disclosed to third parties as this could constitute industrial espionage. The affairs of **The Companies** are kept strictly confidential at all times; and
- ❖ **The Companies** views any contravention of this policy very seriously and employees who are guilty of contravening the policy will be subject to disciplinary procedures, which may lead to the dismissal of any guilty party.

6. DESTRUCTION OF DOCUMENTS

- (i) Documents may be destroyed after the termination of the specified retention periods;
- (ii) Each department is responsible for attending to the destruction of its documents, which must be done regularly. Files must be checked to make sure that they may be destroyed and also to ascertain if there are important original documents in the file. Original documents are returned to the holder thereof, failing which, they are retained by **The Companies** pending such return; and
- (iii) Documents may also be stored off-site, in storage facilities approved by **The Companies**.

7. NON-COMPLIANCE WITH THE POLICY

Appropriate disciplinary action is taken against employees who contravenes this Policy.

8. AVAILABILITY OF THE PAIA MANUAL

The PAIA manual is made available in terms of Regulation Number R. 187 of 15 February 2002. The manual is available at **The Companies'** offices.

9. INFORMATION OFFICER DETAILS

Entity Name	Knowledge Objects Healthcare (Pty) Ltd
Name	ME CHANTAL VILJOEN
Telephone Number	012-673 8600
E-mail Address	popi@knowledgeobjects.com

Entity Name	Knowledge Objects Solutions (Pty) Ltd
Name	DR DENA VAN DEN BERG
Telephone Number	012-673 8600
E-mail Address	popi@knowledgeobjects.com