Kanaan Asset Managers
(the "**Provider**")

PROTECTION OF PERSONAL INFORMATION POLICY

Last Update: 2021-08-27

Revision History

Revision	Date of Adoption
Version 1	**[●]**

1. INTRODUCTION TO POPIA

1.1. The Protection of Personal Information Act, 4 of 2013 ("POPIA") places an obligation on everyone particularly businesses and organisations to process Personal Information belonging to both natural persons and juristic persons lawfully and in accordance with the principles set out in POPI.

1.2. Personal Information can be created and kept in many forms, such as emails, paper, photographs, data bases, registers, videos and many other forms.

1.3. Every employee who processes Personal Information for the purpose and in a manner determined by the Company is jointly responsible for compliance with POPIA.

1.4. The objective of this Policy is to ensure that the Company's Human Resources Department and all other employees comply with the provisions of POPIA when handling Personal Information.

2. WHEN IS THE POPIA NOT APPLICABLE?

2.1. POPIA does not apply:

2.1.1. to information that does not meet the criteria of the definition of Personal Information;

2.1.2. where informed consent is given voluntarily for to the use of the information, as in s 11(1) and other sections;

2.1.3. to the extent that an exemption applies;

2.1.4. to the use of information solely for journalistic, literary or artistic expression to the extent that such an exclusion is necessary to reconcile the right to privacy with the right to freedom of expression, in terms of s 7; or

2.1.5. to the processing of Personal Information, namely –

2.1.5.1. in the course of a purely personal or household activity;

2.1.5.2. data that is anonymised, namely, data de-identified to the extent that it cannot be re-identified again;

2.1.6. information by or on behalf of a public body which involves national security or the prevention of unlawful activities to the extent that adequate safeguards have been established in legislation;

2.1.7. information by the Cabinet or its committees or the executive council of a province; or

2.1.8. information relating to the judicial functions of a court.

3. PURPOSE OF THE POPIA

3.1. The POPIA aims to:

3.1.1. give effect to s14 of the Constitution of the Republic of South Africa which guarantees everyone the right to privacy by safeguarding Personal Information when processed by a Responsible Party and balancing this right against other rights such as the right to access to information;

3.1.2. regulate the manner in which Personal Information may be processed by establishing conditions in harmony with international standards prescribing minimum threshold requirements for lawful processing of Personal Information;

3.1.3. provide persons with rights and remedies to protect their Personal Information from processing that in not in accordance with the POPIA; and

3.1.4. establish voluntary and compulsory measures, including establishing an Information Regulator to, ensure respect for and promote and fulfil the rights protected by POPIA.

4. KEY DEFINITIONS

4.1. "The Company" means **Kanaan Asset Managers**

4.2. "Information Officer" means the person appointed to ensure compliance with POPI and to deal with requests for access to personal data or information.

4.3. "Data Subject "means the person to whom Personal Information relates.

4.4. "Personal Information" Includes:

4.4.1. information about an identifiable natural person, and in so far as it is applicable, an identifiable juristic person, including but not limited to:

4.4.2. 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 a person;

4.4.3. Information relating to the education or the medical, criminal or employment history of the person or information relating to financial transactions in which the person has been involved

4.4.4. Any identifying number, symbol or other particular assigned to the person;

4.4.5. The address, fingerprints or blood type of the person;

4.4.6. The personal opinions, view or preferences of the person, except where they are about another individual or about a proposal for a grant, an award or prize to be made to another individual;

4.4.7. Correspondence sent by the person that is implicitly or explicitly of a private and confidential nature or further correspondence that would reveal the contents of the original correspondence;

4.4.8. The views or opinion of another individual about the person;

4.4.9. The views or opinions of another individual about a proposal for a grant, an award or prize to be made to the person, but excluding the name of the other individual where it appears with the views or opinions of the other individual;

4.4.10. The name of the person where it appears with other Personal Information relating to the person or where the disclosure of the name itself would be reveal information about the person;

4.4.11. Excludes information about a natural person who has been dead or juristic person that has ceased to exist, for more than 20 years.

4.5. "Processing "means any operation or any set of operations concerning Personal Information, including in any case the collection, recording, organisation, storage, updating or modification, retrieval, consultation, use, dissemination by means of transmission or making available in any other form, merging, linking, as well as blocking, erasure or destruction of information.

4.6. "Responsible Party "means the natural or juristic person, administrative body or any other entity which, alone or in conjunction with others, determines the purpose of and the means for processing of Personal Information. In this case the Responsible Party is The Company.

4.7. "Special Personal Information "includes religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, sexual life or biometric information of a Data Subject or criminal behaviour.

5. EIGHT CONDITIONS FOR LAWFUL PROCESSING?

5.1. POPI establishes a framework which imposes obligations, in accordance with eight conditions, on private and public bodies that process Personal Information, and gives rights to individuals and juristic persons whose information is processed. It will regulate every aspect of processing of Personal Information, from the moment that it is collected to the moment that it is destroyed.

5.2. These conditions cannot be read in isolation. They constitute a constellation of conditions which interact with one another and need to be applied holistically. These are effectively principles that must apply when The Company processes Personal Information.

5.2.1. **Condition 1: Accountability: Section 8**

5.2.1.1. The first condition requires The Company, to be accountable for and comply with the conditions for lawful processing from the time when the purpose and the means of processing are determined.

5.2.1.2. The Company is obliged to ensure that the conditions for processing are complied with, even when the processing functions are outsourced.

5.2.2. **Condition 2 : Processing Limitation: Section 9**

5.2.2.1. Personal Information must be processed lawfully, and in a reasonable and adequate manner, which does not infringe the privacy of the Data Subject.

5.2.2.2. Personal Information may only be processed:

5.2.2.2.1. with the voluntary, specific and informed consent of the Data Subject; or

5.2.2.2.2. when processing is necessary to comply with the terms of a contract or law;

5.2.2.2.3. when it protects the legitimate interests of a Data Subject; or

5.2.2.2.4. when processing is necessary for the pursuit of legitimate interests of The Company or of a third party to whom the information is supplied.

5.2.2.3. Information must be collected directly from the Data Subject, but subject to exceptions in particular circumstances.

5.2.2.4. A Data Subject may object, at any time, on reasonable grounds to the processing of his or her Personal Information, at which point, the processing must be discontinued.

5.2.3. **Condition 3 : Purpose Specification :Section 13 and Section 14**

5.2.3.1. Personal Information must be collected for a specific, explicitly defined purpose related to the function and activity of The Company.

5.2.3.2. Steps must be taken to ensure that the Data Subject is aware of the purpose of collection.

5.2.3.3. Information must be kept only for as long as necessary for the specific limited purposes. The Company must destroy/delete or de-identify a record of Personal Information as soon as it is reasonably practicable to do so.

5.2.4. **Condition 4 : Further Processing Limitation :Section 15**

5.2.4.1. This condition restricts the additional processing of information only to those instances where the purpose for the further processing is "compatible" with the original purpose for which the Personal Information was originally collected.

5.2.5. **Condition 5: Information Quality :Section 16**

5.2.5.1. Reasonable steps must be taken to ensure that all the Personal Information The Company holds is complete, accurate, not misleading and updated where necessary.

5.2.6. **Condition 6: Openness :Section 17 and Section 18**

5.2.6.1. The Company must ensure that the Data Subject knows:

5.2.6.1.1. that their information is being collected and the source from which it was collected;

5.2.6.1.2. the purpose for which the information is collected;

5.2.6.1.3. whether supplying the information is compulsory or voluntary;

5.2.6.1.4. any consequence of failing to provide the information;

5.2.6.1.5. whether The Company intends on transferring the information to another country or international organisation; and

5.2.6.1.6. whether the Data Subject's right of access to, right to rectify and right to object to the processing of information are being upheld.

5.2.7. **Condition 7: Security Safeguards : Section 19,20,21 and 22**

5.2.7.1. The Company must secure the integrity and confidentiality of Personal Information, and prevent loss, damage, unauthorised destruction, and unlawful access.

5.2.7.2. It is necessary to identify any risks to the security of the Personal Information and establish appropriate safeguards to minimise the risk.

5.2.7.3. If a third party is processing Personal Information on The Company's behalf, a written contract must be concluded that guarantees that appropriate security measures will be implemented.

5.2.7.4. Where there are grounds to believe that Personal Information has been accessed by an unauthorised person, The Company must notify, as soon as reasonably possible, both the Data Subject and the Information Regulator.

5.2.8. **Condition 8: Data Subject Participation : Section 23,24 and 25**

5.2.8.1. Data Subjects have the right to access, correct, update or rectify Personal Information held by The Company.

5.2.8.2. Data Subjects may also request that The Company destroy or delete their Personal Information.

6. SPECIAL PERSONAL INFORMATION

6.1. Special Personal Information is information in relation to the Data Subject's religious and philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health, sex life, biometric information and criminal behaviour relating to the alleged commission of any offence, any proceedings in respect of any offence allegedly committed or the disposal of such proceedings.

6.2. The processing of Special Personal Information is subject to more stringent requirements than that of Personal Information.

6.3. It is The Company's policy to avoid handling any Special Personal Information on individuals as far as possible. However, there will be instances where The Company will hold this type of information. Such information should be kept to a minimum and will be kept for a short a period as required by law.

7. GUIDELINES ON HOW TO HANDLE PERSONAL INFORMATION

7.1. Information Officer

7.1.1. All entities processing Personal Information must appoint an Information Officer. This is a legal function bestowed on the 'head' of an organisation or business or someone of a similar ranking or high ranking in the business. **Gert Delport** serves as the Information Officer. If the employee is ever in doubt about whether any processing activities that the employee intends to undertake comply with POPI, please contact the Information Officer at **gert@kanaantrust.com or call at 031 561 2208**.

7.1.2. Deputy Information Officers can be appointed by the business as per section 56 of the Personal Information Act. The Deputy information officer is **Andries van Tonder.**

7.1.3. The details of both Information Officers and Deputy Information Officers are registered with the Regulator as prescribed by the regulators Guidelines issued in this regard.

7.2. Standard Privacy Policy Statement

7.2.1. A privacy policy statement is a document that discloses some or all of the ways The Company gathers, uses, discloses, and manages the Personal Information of Data Subject.

7.2.2. The Company will share the policy on their website, newsletters, and in other communications with business clients and stakeholders and employees.

7.2.3. Data Subjects (employees and clients) must familiarise themselves with the Company's privacy policy statement in order to give informed consent to processing of their information.

7.3. Recruitment and Employee Participation

7.3.1.1. To ensure employee commitment, accountability, and compliance, The Company has updated job descriptions to ensure that they are in line with the POPIA Requirements.

7.3.1.2. If an employee fails to comply with the POPIA Regulations there could be possible penalties (including disciplinary hearings and accountability for financial losses) for non-adherence of or breaches, due to the high risk and implications of POPI Act penalties and fines.

7.3.1.3. The Human Resources Department will also ensure that they are handling information of prospective, current and future employees in accordance with POPIA principles.

7.4. Training for Management and Employees

7.4.1.1. The Company must ensure that all personnel are trained on the POPI Act and they are aware of their responsibilities in terms of the Act as well as the penalties for non compliance.

7.5. Record Keeping

7.5.1. A Responsible Party can create a database of all the Personal Information they collect, and keep record of how they process the information throughout its lifecycle. Personal Information can also be classified (e.g. based on type, sensitivity)

7.5.2. Classifying the Personal Information will also assist in the risk management process. The business can assess and mitigate possible compliance and breach risks.

7.6. Security measures

7.6.1. **Assessing software systems**

7.6.1.1. The Company must consider the potential risks when using software systems. These systems must be adapted to ensure likelihood of a breach is reduced.

7.6.2. **Reviewing of agreements**

7.6.2.1. The Company must consider all clauses in their agreements and measure them against the POPI conditions and lawful processing requirements and amend them as required.

7.6.3. **Retention or restriction of records**

7.6.3.1. S14 of the POPI Act requires Responsible Parties to delete, destroy or de-identify Personal Information as soon as practicable after the Responsible Party is no longer authorised to retain the record. This must be done in a manner that prevents reconstruction in intelligible form.

7.6.3.2. The Company must ensure that the personal information that the Company holds is adequate, relevant and not excessive in relation to the Company's business purposes. Do not ask data

subjects for or record excessive information that the Company does not need, even if it is information that is "nice to know".

7.6.3.3. Only use personal information for the purpose for which it was originally collected. Should the Company wish to use the information for a different purpose, consult the Information Officer.

7.6.3.4. Make sure that the personal information is accurate and kept up to date, and is not kept for longer than necessary.

7.6.3.5. Make sure that data subjects are given notice of the processing of their personal information, including, details of the information being collected, the purpose for which it is to be collected and used and any other relevant information.

7.6.3.6. Such notices have been/will be incorporated into the Company's standard terms of engagement, the Company's employment contracts and written agreements with third parties.

7.6.3.7. Comply with the rights of people on who the Company holds information (such as the right to access information about themselves).

7.6.3.8. Only process special personal information with the explicit consent of the person on whom the Company holds the information. If in doubt about whether the Company is permitted to process the special personal information, consult the Information Officer.

7.7. Information Security

7.7.1. Measures must be put in place to help secure Personal Information such as email security, security on laptops, firewalls, servers and encryption to control access to Personal Information and prevent data loss.

7.7.2. The Company must take positive steps to prevent the accidental, improper or deliberate disclosure or misuse of personal information and prevent unauthorised access.

7.7.3. The Company must limit the disclosure of and access to personal information to those who have a business need to access the information.

7.7.4. In the event of personal information being compromised, the Company should notify the Information Officer immediately.

7.7.5. The use or disclosure of personal information that has been collected for the Company's business purposes for any ulterior purpose is strictly prohibited and will lead to disciplinary action against the staff member concerned.

7.8. Updating of Policies

7.8.1. Policies such as the Business Continuity Plans, the Risk Management Plan and Social Media Policy and the Complaints Management Framework must be updated regularly to ensure that they reflect the principles of the POPI Act. The Company must identify potential breaches and risks and impact thereof and update the policies accordingly.

7.9. Third Parties or Operators

7.9.1. It is advisable that the business as a Responsible Party should not only address the section 21 requirement in the POPIA in an agreement with an operator or third party, but conduct due diligence to ascertain that contracted operators or third parties are compliant with the Act and have adequate data security and protection measures in place.

7.9.2. The Company must ensure that where any person or organisation is processesing Personal Information on behalf of the Company (e.g.: security or IT service provider), a written agreement is concluded with the service provider requiring them to:

7.9.2.1. process the Personal Information in accordance with the Company's instructions and in compliance with POPI;

7.9.2.2. maintain adequate information security; and

7.9.2.3. take reasonable steps to ensure that staff who have access to the information are familiar with the terms of the agreement.

7.9.2.4. inform The Company as soon as practicable possible should there be a breach.

7.10. Data Subject Access Requests

7.10.1. A Data Subject, whose information The Company holds, may submit a request for a description, deletion or correction of Personal Information held by the Responsible Party, as well as a list of all third parties who have or have had access to the Personal Information.

7.10.2. Any such requests from Data Subjects should be transferred to the Information Officer if the request relates to a person who is not an employee or to the Head of Human Resources in relation to requests from employees or former employees.

7.10.3. All Personal Information is potentially disclosable to the person to whom it relates. The Company should bear this in mind when recording expressions of opinion about people and ensure that the Responsible Party can justify what it writes (e.g.: interview notes, performance appraisals or in emails).

7.11. Disclosure of Personal Information outside of South Africa

7.11.1. If information is required to be transferred outside of South Africa, The Company’ s is obliged to make sure that the Data Subject whose information is being transferred has specifically consented to the transfer of the information or ensure that the Responsible Party's engagement terms are in place, which provides the necessary consent to do so.

7.11.2. In the event that specific consent for the transfer is sought from the Data Subject, the Data Subject must be informed about the destination to which the information is going to be sent and the level of protection that the information will receive once it is transferred.

7.11.3. If obtaining consent for a transfer will pose a difficulty, consult the Information Officer, who will determine how best to handle the matter.

7.12. Breach Management and Complaints

7.12.1. Breaches and Complaints must be reported to the Information Regulator in writing as well as to any parties whose Personal Information has been accessed or acquired by an unauthorised party.

7.12.2. The Company will keep a register of all breaches that occur, when they are logged and how they handled and how they are finally resolved.

7.12.3. The Company will also have Professional Indemnity cover and this typically includes cyber liability. This cover is to also address financial and legal costs and losses that arise as a result of normal business procedural breaches and these should also be investigated.

7.12.4. If an employee suspects that a breach has occurred the employee must report the breach to their immediate superior who can escalate the matter to The Company Information Officer.

7.12.5. The Company will notify the Information Regulator and the affected parties in writing as well as investigate the source of the breach and mitigate any future occurrences.

7.12.6. The Full Breach Protocol can be found in the Company’s Complaints Management Framework.