27four Investment Managers

PROTECTION OF PERSONAL INFORMATION ("POPI") POLICY

Version	1.0
Policy Owner	27four IM Compliance
External review	ICS
Review and recommendation	27four Group Risk Committee
Approval	27four IM Board of Directors
Review Intervals	Annual
Date of approval	July 2024

CONTENTS

1. INTRODUCTION

1.1. 27four Investment Managers (Pty) Ltd ("27four IM") is committed to protecting the privacy and personal information of individuals in compliance with the Protection of Personal Information Act, No. 4 of 2013 ("POPI").

1.2. 27four IM processes and stores personal information, relating to natural and juristic persons to operate its business efficiently.

1.3. 27four IM shall ensure that such personal information is processed, stored and disposed of in accordance with POPI.

1.4. 27four IM regards the lawful and appropriate processing of all Personal Information as crucial to successful service delivery and essential to maintaining confidence between the Company and those individuals and entities who deal with it.

1.5. 27four IM therefore fully endorses and adheres to the principles of POPI.

1.6. This policy outlines its commitment to responsible collection, storage, processing, and protection of personal information, ensuring that it is handled in a lawful and ethical manner.

2. PURPOSE AND SCOPE

2.1. The purpose of this policy is to govern and manage the actions that 27four IM takes to protect the right to privacy of data subjects.

2.2. It is used to direct, monitor and continuously improve compliance with the conditions for lawfully processing personal information.

2.3. This policy applies to all employees, contractors, third-party service providers, and any other individuals or entities acting for and on behalf of 27four IM who collect, process, or have access to personal information during the course of their duties.

3. DEFINITIONS

3.1. **"Administrator"** means a party or parties appointed by 27four IM to provide it with financial administration services;

3.2. **"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;

3.3. **"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 themselves;

3.4. **"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;

3.5. **"consent"** means any voluntary, specific and informed expression of will in terms of

which permission is given for the processing of personal information;

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

3.7. **"direct marketing"** means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of -

3.7.1. promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or

3.7.2. requesting the data subject to make a donation for any reason;

3.8. **"electronic communication"** means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient;

3.9. **"Information Officer"** means the person who is appointed and registered as the Information Officer of 27four IM with the Information Regulator of South Africa;

3.10. **"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;

3.11. **"person"** means any natural person or a juristic person;

3.12. **"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 -

3.12.1. 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;

3.12.2. information relating to the education or the medical, financial, criminal or employment history of the person;

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

3.12.4. the biometric information of the person;

3.12.5. the personal opinions, views or preferences of the person;

3.12.6. 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;

3.12.7. the views or opinions of another individual about the person; and

3.12.8. 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;

3.13. **"processing"** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—

3.13.1. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

3.13.2. dissemination by means of transmission, distribution or making available in any other form; or

3.13.3. merging, linking, as well as restriction, degradation, erasure or destruction of information;

3.14. **"Promotion of Access to Information Act"** means the Promotion of Access to Information Act, No. 2 of 2000;

3.15. **"public record"** means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body;

3.16. **"Regulator"** means the Information Regulator established in terms of Section 39 of POPI;

3.17. **"responsible party"** 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;

4. PRINCIPLES OF PROCESSING PERSONAL INFORMATION

4.1. 27four IM is committed to upholding the following principles when processing and protecting personal information.

4.2. ACCOUNTABILITY

4.2.1. 27four IM acknowledges that, as a Responsible Party, it must ensure compliance with the relevant regulations, including the appointment of a designated Information Officer who oversees the implementation and monitoring of the organisation's data protection efforts.

4.3. PROCESSING LIMITATION

4.3.1. 27four IM will ensure that personal information is only processed based on one or more of the following:

4.3.1.1. Consent: the data subject or competent person where the data subject is a child has given clear consent for 27four IM to process the personal information for a specific purpose.

4.3.1.2. Contract: processing is necessary to carry out actions for

the conclusion or performance of a contract to which the data subject is party.

4.3.1.3. Legal obligation: processing complies with an obligation imposed by law on 27four IM.

4.3.1.4. Legitimate interest of data subject: processing protects a legitimate interest of the data subject.

4.3.1.5. Responsible party and third-party legitimate interests: processing is necessary for the legitimate interests of a third party or of 27four IM.

4.3.2. 27four IM will use the Personal Information Risk and Impact Assessment Questionnaire to identify and record the appropriate lawful basis for all personal information being processed.

4.3.3. Where special personal information is processed, 27four IM will obtain authorisation for processing this type of information.

4.4. **PURPOSE SPECIFICATION**

4.4.1. Personal information will be collected for specified, explicit, and legitimate purposes, and may not be further processed in a manner that is incompatible with those purposes.

4.4.2. Data subjects will be provided with the purpose of the collection of their information before collection thereof.

4.4.3. Personal information will be retained and destroyed according to the 27four IM Records Management Retention and Disposal Policy.

4.5. **FURTHER PROCESSING LIMITATION**

4.5.1. Only the necessary and relevant personal information required for the intended purpose will be collected and processed.

4.6. **INFORMATION QUALITY**

4.6.1. Reasonable steps will be taken to ensure that personal information is accurate, complete, and up to date.

4.6.2. Individuals will be provided with opportunities to update their personal information as needed.

4.7. **OPENNESS**

4.7.1. Personal Information will be processed in a transparent manner.

4.8. **SECURITY SAFEGUARDS**

4.8.1. Appropriate technical, physical, and organisational measures will be implemented to protect personal information against loss, unauthorized

access, disclosure, alteration, or destruction.

4.8.2. Regular risk assessments and security audits will be conducted to identify and address any vulnerabilities.

4.9. DATA SUBJECT PARTICIPATION

4.9.1. 27 four IM respects the rights of individuals in relation to their personal information, including the right to access, rectify, restrict processing, and request deletion of their data in accordance with POPI.

4.9.2. Processes will be put in place to address such requests promptly and effectively.

5. CLEAN DESK POLICY

5.1. WORKING IN THE OFFICE

5.1.1. Employees are required to protect all personal or confidential information in their workspace at at all times. This includes electronic and physical hardcopy information.

5.1.2. Whiteboards containing personal or confidential information are erased after use.

5.1.3. Employees are encouraged to consider scanning paper items and filing them electronically.

5.1.4. Desktops/laptops are to be locked when left unattended.

5.1.5. Portable devices such as laptops and tablets that stay overnight in the office are to be turned off and stored out of sight.

5.2. WORKING AWAY FROM THE OFFICE

5.2.1. Confidential information and personal information on data subjects should only be taken home if absolutely necessary.

5.2.2. Where an employee accesses and prints company files on a home computer or is using personal Wi-Fi connection, all computer security software must be up-to-date and effective.

6. ROLES AND RESPONSIBILITIES

6.1. INFORMATION OFFICER

6.1.1. The designated Information Officer is responsible for overseeing the implementation and compliance with this policy, as well as providing guidance and support to employees regarding data protection matters.

6.2. EMPLOYEES

6.2.1. All employees have a responsibility to handle personal information in

accordance with this policy.

6.2.2. All employees should be familiar with the principles of data protection and follow the established procedures.

6.2.3. All employees must report any breaches or concerns to the Information Officer.

6.3. **THIRD-PARTY SERVICE PROVIDERS**

6.3.1. When engaging third-party service providers, 27four IM will ensure that appropriate data protection agreements are in place, clearly defining the responsibilities and obligations of each party regarding the processing of personal information.

7. TRAINING AND AWARENESS

7.1. 27four IM will provide regular training and awareness programs to its employees to ensure their understanding of this policy and their responsibilities in protecting personal information.

7.2. Training will cover relevant data protection laws, principles, procedures, and best practices.

8. BREACH NOTIFICATION

8.1. In the event of a personal data breach, 27four IM will follow the Incident Management Response Plan as outlined in POPI.

8.2. This includes promptly assessing the risk to individuals' rights and freedoms, notifying the relevant supervisory authority and affected individuals, and taking appropriate remedial actions to mitigate the impact of the data breach.

9. POLICY REVIEW

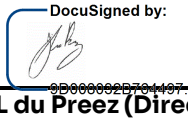
9.1. This policy will be reviewed as and when required to ensure its ongoing relevance and effectiveness.

9.2. Changes to the policy will be communicated to employees and stakeholders, and training programs will be updated accordingly.

10. COMPLIANCE AND CONSEQUENCES

10.1. Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract, in accordance with 27four IM's disciplinary procedures.

11. DOCUMENT SIGN-OFF



JL du Preez (Director)

Duly authorized to sign.

16-Jul-2024 | 08:58 SAST

Date