PROTECTION OF PERSONAL INFORMATION POLICY

REVISED: 30 JUNE 2025

PURPOSE AND SCOPE

The purpose of this document is to detail the business strategy of Independent Alternatives Investment Managers (Pty) Ltd ("FSP") to ensure data privacy and protection, and compliance to the Protection of Personal Information Act (POPIA), also known as the POPI Act. The business aims to promote the protection of personal information by requiring that public and private entities comply with certain standards when collecting, processing, storing and sharing personal information that may be made available to them during their interactions with the business.

For: INDEPENDENT ALTERNATIVE INVESTMENT MANAGERS (PROPRIETARY) LIMITED

.....	.....
Grant Hogan	Tatenda Chapinduka

1. INTRODUCTION

The purpose of this policy is to enable IAIM to:

- Comply with the Protection of Personal Information Act, 4 of 2013 ("POPIA");
- Follow best practice in the handling of personal data;
- Protect the privacy of IAIM employees, directors, key individuals; representatives, clients, service providers, and other stakeholders; and
- Safeguard the organisation from the consequences of a breach of its data protection responsibilities.

This policy applies to all processing of personal information conducted by IAIM in its business operations and in line with its PAIA Manual.

2. DEFINITIONS

Definitions in Section 1 of POPIA apply. For ease of reference:

- Biometrics: Personal identification using physical, physiological, or behavioural characteristics (e.g., fingerprinting, DNA, retinal scans).
- Competent Person: A legally competent individual who can consent to decisions concerning a child.
- Consent: Voluntary, specific, and informed expression of will.
- Data Subject: The person or juristic entity to whom personal information relates.
- De-identify: To delete or alter information so that the Data Subject cannot be identified.
- Operator: A person or entity processing personal information for a Responsible Party under contract or mandate.
- Personal Information: Information relating to an identifiable, natural living person or juristic entity (e.g., demographics, employment history, identifiers, opinions, correspondence, biometric data).
- Processing: Any activity involving personal information, including collection, storage, updating, dissemination, or destruction.
- Record: Any form of recorded information, whether written, electronic, photographic, or otherwise.

- Responsible Party (RP): IAIM, as the entity that determines the purpose and means of processing.
- Special Personal Information: Information relating to religious/philosophical beliefs, race/ethnic origin, trade union membership, political affiliation, health, sex life, or biometrics.

3. KEY PRINCIPLES

3.1 Information Officer Responsibilities

In line with IAIM's PAIA Manual:

- Information Officer: Mr. Grant Hogan (CEO)
- Deputy Information Officer: Mr. Tatenda Chapinduka

The Information Officer is responsible for:

- Reviewing POPIA and related regulatory updates;
- Ensuring POPIA induction training for all employees;
- Developing and maintaining internal and external Privacy Notices;
- Handling Data Subject access and correction requests;
- Approving unusual disclosures of personal information;
- Approving contracts with Operators;
- Ensuring information quality and security safeguards are maintained;
- Liaising with the Information Regulator.

3.2 Conditions for Lawful Processing

3.2.1 Accountability

IAIM must ensure compliance with all lawful processing conditions.

3.2.2 Processing Limitation

- Processing must be lawful, fair, and not excessive.
- Consent must be obtained where appropriate (written or recorded verbal).

- Collection should be directly from the Data Subject unless exceptions apply (e.g., public record, consented by the Data Subject, or necessary for compliance).

3.2.3 Purpose Specification

- Personal information must be collected for a specific, lawful purpose related to IAIM's business activities.
- Data Subjects must be informed of the purpose, the responsible party, and consequences of not providing information.
- Records must not be retained longer than necessary unless retention is required by law, contract, or for research/statistical purposes under safeguards.
- IAIM must destroy or de-identify personal information when no longer authorised to retain it, preventing reconstruction.

3.2.4 Further Processing Limitation

Further processing must be compatible with the original purpose unless:

- The Data Subject consents;
- Information comes from a public record;
- Required by law, court order, or public health/safety obligations;
- For statistical or research purposes under safeguards.

3.2.5 Information Quality

IAIM must ensure information is complete, accurate, up to date, and not misleading. Systems and procedures will be regularly reviewed to ensure accuracy.

3.2.6 Openness

IAIM maintains documentation of all processing activities, supported by its PAIA Manual. Employees are informed through this policy; clients and third parties via IAIM's Privacy Notice.

3.2.7 Security Safeguards

- IAIM will protect personal information against loss, destruction, or unauthorised access.
- Risks will be identified, safeguards implemented and regularly updated.
- Operators processing information on IAIM's behalf must maintain contractual safeguards.
- Any security compromise will be reported promptly to the Information Regulator and affected Data Subjects.

3.2.8 Data Subject Participation

Data Subjects may request access to their personal information, request correction or deletion, or object to processing. Requests follow IAIM's PAIA procedure.

3.3 Processing of Special Personal Information

IAIM will not process Special Personal Information unless:

- The Data Subject consents;
- Processing is required by law;
- Necessary for legal rights or obligations;
- For research/statistical purposes in the public interest under safeguards;
- Approved by the Information Regulator.

Special provisions apply for:

- Race/Ethnic Origin: Only for identification or compliance with anti-discrimination laws.
- Health/Sex Life: Where necessary for medical treatment, insurance, schools, pensions, or employment law obligations.
- Children: Only with consent of a Competent Person or where permitted by law.

3.5 Direct Marketing, Directories & Automated Decision-Making

Data Subjects will be informed if their information may be used for marketing and given the opportunity to opt-out.

3.6 Transborder Information Flows

IAIM may not transfer personal information outside South Africa unless:

- The recipient is subject to adequate data protection laws;
- The Data Subject consents;
- The transfer is necessary for contract performance; or
- It is in the interest or benefit of the Data Subject.

4. APPLICABILITY & AUTHORITY

- This policy applies to all IAIM business operations, employees, directors, representatives, service providers, and clients.
- The IAIM Board authorises this policy, and the Information Officer and Deputy are empowered to implement and monitor compliance.