PROTECTION OF PERSONAL INFORMATION POLICY

("POPI POLICY")

for

MATRIX FUND MANAGERS (PTY) LTD

("MFM")

Revised: July 2021

MATRIX
FUND MANAGERS

1. INTRODUCTION

The purpose of this policy is to enable MFM to:

- comply with the relevant law in respect of data privacy, including Personal information, it holds about Data Subjects;
- follow good practice;
- protect the privacy of MFM employees, key individuals, representatives, directors, clients, and other stakeholders; and
- protect the organisation from the consequences of a breach of its responsibilities.

2. DEFINITIONS

Definitions below as defined in Section 1 of the Protection of Personal Information Act, 4 of 2013 (POPI Act):

2.1	Biometrics	A technique of personal identification that is based on the physical, physiological, or behavioural characteristics including blood type, fingerprinting, DNA analysis, retinal scanning, and voice recognition
2.2	Competent person	any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child
2.3	Consent	Voluntary, specific, and informed expression of will
2.4	Data Subject	The person to whom the information relates
2.5	De-identify	Delete any information that • identifies the Data Subject • can be used or manipulated by a reasonably foreseeable method to identify the Data Subject, or • can be linked by a reasonably foreseeable method to other information that identified the Data Subject
2.6	Operator	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
2.7	Personal information	Information relating to an identifiable, living, natural person and where applicable an identifiable, existing juristic person including: • information about the race, gender, sex, pregnancy, marital status, nationality, 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 • information about the education or the medical, financial, criminal or employment history of the person • any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier, or other particular assignment to the person • biometric information of the person • personal information opinions, views, or preferences of the person • correspondence sent by the person that is private or confidential in nature or further correspondence that would reveal the contents of the original correspondence • views or personal information opinions of another person about the person

		• name of the person if it appears with other personal information about the person or the disclosure of the name itself if it would reveal information about the person
2.8	Processing	Any operation or activity or any set of operations concerning personal information including: • collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use • dissemination by means of transmission, distribution or making available in any other format • merging, linking as well as restriction, degradation, erasure, or destruction of information
2.9	Record	Recorded information regardless of the form or medium including: • writing an any material • information produced, recorded, or stored by means of any tape-recorded, computer equipment, or other devise and any material subsequently derived from information so produced, recorded, or stored • label, marking or other writing that identifies or describes anything of which it forms part or to which it is attached by any means • book, map, plan, graph, or drawing • photograph, film negative, tape or other device in which one of more visual images are embodied so as to be capable of being processed which is in the possession or under the control of the responsible party whether or not it was created by the responsible party and regardless of when it was created
2.10	Re-identify	Resurrect information that has been de-identified that • identifies the Data Subject • can be used or manipulated by a reasonably foreseeable method to identify that Data Subject • can be linked by a reasonably foreseeable method to other information that identifies the Data Subject
2.11	Responsible party (RP)	Private or public body or any other person which alone or in conjunction with others determines the purpose of and means for processing of personal information
2.11	Restriction	Withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information
2.12	Special Personal information	Personal information relating to 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.

3. KEY PRINCIPLES

3.1 INFORMATION OFFICER RESPONSIBILITIES

3.1.1 The Information Officer has been delegated and appointed by the Chief Executive Officer and has responsibilities of developing, publishing, and maintaining this POPI Policy which addresses all relevant provisions of the POPI Act, including but not limited to the following:

- Reviewing the POPI Act and periodic updates as published;
- Ensuring that POPI Act induction training takes place for all staff;
- Ensuring that periodic communication awareness on POPI Act responsibilities takes place;
- Ensuring that Privacy Notices for internal and external purposes are developed and published;
- Handling Data Subject access requests;
- Approving unusual or controversial disclosures of Personal information;
- Approving contracts with Data Operators;
- Ensuring that appropriate policies and controls are in place for ensuring the Information Quality of Personal information;
- Ensuring that appropriate Security Safeguards in line with the POPI Act for Personal information are in place;
- Handling all aspects of relationship with the Information Regulator as foreseen in the POPI Act; and
- Provide direction to the Deputy Information Officer.

- **Information Officer:** Robert Coombe
- **Deputy Information Officer:** Faieka Slemming.

3.2 CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

3.2.1 ACCOUNTABILITY

MFM must ensure that all the conditions for lawful processing are complied with:

- when the purpose and means of processing are determined, and
- during the actual processing.

3.2.2 PROCESSING LIMITATION

Personal information must be processed ***lawfully*** and in a reasonable manner that does not infringe the privacy of the Data Subject. Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant, and ***not excessive***. MFM undertakes to gain written consent where appropriate; alternatively, a recording must be kept of verbal consent.

3.2.2.1 Consent, justification, and objection:

- Personal information may only be processed if—
  - the Data Subject or a Competent person where the Data Subject is a child consents to the processing;
  - processing is necessary to carry out actions for the conclusion or performance of a contract to which the Data subject is party;
  - processing complies with an obligation imposed by law on the Responsible party;
  - processing protects a legitimate interest of the data subject;
  - processing is necessary for the proper performance of a public law duty by a public body; or
  - processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied

3.2.2.2 Collection directly from the Data Subject

- Personal information must be collected directly from the Data Subject, unless:
  - information is derived from a public record or has deliberately been made public by the Data Subject;
  - the Data Subject or a competent person where the data subject is a child has consented to the collection of the information from another source;
  - collection from another source would not prejudice the Data Subject;
  - collection from another source is necessary;
  - collection from the Data Subject would prejudice a lawful purpose of the collection, or
  - it is not reasonably practical in the circumstances

3.2.3 PURPOSE SPECIFICATION

3.2.3.1 Collection for specific purpose:

- Personal information must be collected for a specific, explicitly defined, and lawful purpose related to a function or activity of MFM.

- If Personal information is collected, MFM must take reasonably practicable steps to ensure that the Data subject is aware of the following:
  - the information being collected and where the information is not collected from the data subject, the source from which it is collected;
  - the name and address of the responsible party;
  - the purpose for which the information is being collected;
  - whether or not the supply of the information by that data subject is voluntary or mandatory;
  - the consequences of failure to provide the information;
  - any particular law authorising or requiring the collection of the information;
  - the fact that, where applicable, the responsible party intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation;
  - any further information such as the—
    - recipient or category of recipients of the information;
    - nature or category of the information;
    - existence of the right of access to and the right to rectify the information collected;
    - existence of the right to object to the processing of personal information as referred to in section 11(3); and
    - right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator, which is necessary, having regard to the specific circumstances in which the information is or is not to be processed, to enable processing in respect of the data subject to be reasonable.

- MFM does not have to ensure that Data Subject is aware of the purpose, if:
  - the Data Subject has consented to collection from another source;
  - non-compliance would not prejudice the Data Subject;
  - non-compliance is necessary;
  - compliance would prejudice a lawful purpose of the collection;
  - it is not reasonably practical in the circumstances;
  - the information will not be used in a form in which the Data Subject may be identified, or
  - the information will be used for historical, statistical or research purposes.

3.2.3.2 Retention and restriction of records:

- Records of personal information must not be retained longer than necessary for achieving the purpose for which it was collected and processed unless:

- Retention is required or authorised by law;
- MFM reasonably requires the record for the lawful purposes related to its functions or activities;
- Retention is required by a contract between parties thereto; or
- the Data Subject or a competent person where the data subject is a child consents to the retention of the record.

- Records may be retained for longer periods for historical, statistical or research purposes if MFM has established safeguards to prevent the records being used for any other purpose.

- If MFM has used a record to make a decision about a Data Subject the record must be retained in compliance with applicable law or code of conduct if applicable or for a reasonable period.

- MFM must destroy or delete personal information records or de-identify personal information records as soon as reasonably practical after MFM is no longer authorised to retain the record.

- The destruction or deletion of a personal information record must be done in a manner that prevents its reconstruction in an intelligible form.

- MFM must restrict processing of personal information if:
  - Its accuracy is contested by the Data Subject, for a period enabling MFM to verify;
  - MFM no longer needs the personal information for achieving the purposes, but the personal information must be retained for the purposes of proof; and
  - The processing was unlawful, and the Data Subject opposes its destructions or deletion and requests the restriction instead.

  MFM must inform the Data Subject before lifting the restriction on processing.

- Restricted personal information may only be accessed for the purposes of proof, or with the Data Subject's consent, or for the protection of the rights of another person or in the public interest.

- Matrix FM will establish retention periods for at least the following categories of Data Subject, in respect of their personal information:
  - Directors
  - Employees
  - Investors/customers/clients
  - Suppliers
  - Service providers

  Detailed coverage of the relevant retention periods will be documented in line with the Act and any other applicable laws (refer to MFM's Data Retention Policy)

3.2.4 FURTHER PROCESSING LIMITATION

3.2.4.1 Further processing to be compatible with purpose for collection

To assess whether further processing is compatible with purpose of collection, MFM must consider:

- The relationship between purpose of the intended further processing and the purpose for which the personal information has been collected;
- Nature of the Personal information;
- Consequences of the intended further processing for the Data Subject;
- Manner in which the personal information was collected; and
- Contractual rights and obligations between the parties.

3.2.4.2 Further processing is not incompatible with purpose of collection if:

- the Data Subject or a competent person where the data subject is a child has consented;
- personal information is available or derived from a public record or has been deliberately made public by the Data Subject;
- Further processing is necessary:
  - To avoid prejudice to the maintenance of the law by a public body;
  - To comply with a legal or SA tax obligation;
  - Court or tribunal proceedings; and
  - To prevent/mitigate a serious threat of public health/safety or the life or health of the Data Subject or another individual.
- Personal information will be used for historical, statistical or research purposes and MFM ensures that information will not be published in identifiable form, or
- Information is exempt by the Information Regulator.

3.2.5 INFORMATION QUALITY

3.2.5.1 MFM must take reasonable steps to ensure that personal information is complete, accurate, not misleading and updated where necessary, taking regard for the purpose for which personal information was collected.

3.2.5.2 MFM will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

- Information systems will be designed, where possible, to encourage and facilitate the entry of accurate data;
- Personal information on any Data Subject will be held in as few places as necessary, and all employees will be discouraged from establishing unnecessary additional data sets;
- Effective procedures will be in place so that all relevant systems are updated when information about any Data Subject changes; and
- Staff who keep more detailed personal information about Data Subjects will be given additional guidance on accuracy in record keeping.

3.2.6 OPENNESS

3.2.6.1 Documentation

MFM must maintain documentation of all processing operations to support the PAIA manual and Data Subjects will generally be informed in the following ways:

- Employees: through this policy; and
- Clients and other interested parties: through the MFM Privacy Notice.

Whenever data is collected, the number of mandatory fields will be kept to a minimum and Data Subjects will be informed which fields are mandatory and why.

3.2.6.2 Notification to the Data Subject when collecting personal information

- If personal information is collected, MFM must take reasonably practical steps to ensure that the Data Subject is aware of:
  - Information collected and the source (if not from the Data Subject);
  - Name & address of MFM as the responsible party;
  - Purpose for collecting the data;
  - Whether the supply of information is voluntary or mandatory;
  - Consequences of failure to provide the information;

- Particular law authorising or requiring the collection;
- The fact that, if applicable, MFM intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation; and
- Any further information, such as:
  - The recipient or categories of recipients of the information;
  - nature or category of information;
  - existence of the right of access to and the right to rectify the information collected;
  - existence of the right to object to the processing of personal information; and the
  - right to lodge a complaint to the Information Regulator.

➢ It is not necessary to notify the Data Subject again when personal information of the same kind and purpose is collected.

3.2.7 SECURITY SAFEGUARDS

3.2.7.1 Security measures on integrity and confidentiality of personal information

➢ MFM must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable measures to prevent:
- loss, damage, unauthorised destruction of personal information; and
- unlawful access to or processing of personal information.

➢ To determine appropriate measures, MFM must:
- identify internal and external risks to personal information in its possession/ under its control;
- establish and maintain safeguards;
- verify that the safeguards are effectively implemented;
- ensure that the safeguards are updated in response to new risks or deficiencies in safeguards; and
- adopt reasonable security practices relative to its industry.

➢ Refer to MFM Information Security Framework for further guidance.

3.2.7.2 Information processed by an operator or person acting under authority

➢ An operator or anyone processing personal information on behalf of MFM must:
- process information only with the knowledge or authorisation of MFM; and
- treat personal information as confidential;

unless required by law or in the course of the proper performance of their duties.

3.2.7.3 Security measures regarding information processed by an operator

➢ MFM must, in terms of written contract, ensure that the operator which processes personal information for them establishes and maintains security measures; and

➢ The operator must notify MFM immediately where there are reasonable grounds to believe that the personal information of a Data Subject has been accessed or acquired by any unauthorised person.

3.2.7.4 Notification of security compromises

- Where there are reasonable grounds to believe that the personal information of a Data Subject has been accessed or acquired by an unauthorised person, MFM must notify ASAP with sufficient information:
  - Information Regulator; and
  - Data Subject.

- Notification to the Data Subject must be in writing and communicated by post, email, website of MFM or as directed by the Information Regulator.

3.2.8 DATA SUBJECT PARTICIPATION

3.2.8.1 Access to personal information

- MFM must, on request by Data Subject,
  - Confirm whether we have any personal information of that Data Subject;
  - Provide applicable records or description of that personal information,
  - identity of all third parties who have/had that personal information to Data Subject; and
  - MFM must advise Data Subject of his/her right to request correction of the personal information.

Data Subject access requests must be in writing. All employees are required to pass on anything which might be a data subject access request to the Information Officer without delay. Requests for access to personal information will be handled in compliance with the POPI Act and in compliance with the Promotion of Access to Information Act (PAIA).

3.2.8.2 Correction of personal information

- MFM must correct or delete personal information on request about the Data Subject that is
  - Inaccurate
  - Irrelevant
  - Excessive
  - Out of date
  - Incomplete
  - Misleading
  - Obtained unlawfully

- MFM must, on request, delete or destroy personal information about that Data Subject if they no longer have authority to keep it. MFM must evidence action taken to Data Subject.

3.3 PROCESSING OF SPECIAL PERSONAL INFORMATION

3.3.1 General Authorisation

- MFM may not process special personal information as defined unless a general authorisation is obtained where:

  - the Data Subject consents to processing;
  - processing is necessary for establishment, exercise, or defence of a legal right,
  - processing is necessary to comply with an obligation of international public law;
  - processing is necessary for historical, statistical or research purposes to the extent that it is in the public interest or obtaining consent is impossible

- the Data Subject has deliberately made the information public or
- the Information Regulator allows.

3.3.2 Authorisation: Race or Ethnic Origin

- The prohibition on processing personal information concerning a data subject's race or ethnic origin, does not apply if the processing is carried out to:
  - identify data subjects and only when this is essential for that purpose; and
  - comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

3.3.3 Authorisation: Health or Sex Life

- The prohibition on processing personal information concerning a data subject's health and sex life, does not apply to the processing by:
  - medical professionals, healthcare institutions or facilities or social services, if such processing is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional practice concerned;
  - insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations;
  - schools, if such processing is necessary to provide special support for pupils or making special arrangements in connection with their health or sex life;
  - any public or private body managing the care of a child if such processing is necessary for the performance of their lawful duties;
  - any public body, if such processing is necessary in connection with the implementation of prison sentences or detention measures; or
  - administrative bodies, pension funds, employers or institutions working for them, if such processing is necessary for—
    - the implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sex life of the data subject; or
    - the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.
    - comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination

3.4 PROCESSING OF PERSONAL INFORMATION OF CHILDREN

3.4.1 MFM may not process personal information concerning a child unless the processing is:

- a with the prior consent of a competent person;
- Processing is necessary for establishment, exercise, or defence of a legal right or obligation or international public law;
- Processing is necessary for historical or statistical/or research purposes;
- Processing is in the public interest;
- of Personal information which has deliberately been made public by the child, with the consent of Competent person or
- Information Regulator approved.

3.5 DIRECT MARKETING, DIRECTORIES AND AUTOMATED DECISION MAKING

3.5.1 Whenever personal information is first collected which might be used for any marketing purpose, this purpose will be made clear, and the Data Subject will be given a clear opportunity to opt out.

3.6 TRANSBORDER INFORMATION FLOWS

3.6.1 MFM or any responsible party in the Republic may not transfer personal information about a Data Subject to a third party who is in a foreign country unless certain requirements are met.

3.6.2 This has far reaching implications for parties who transact in foreign jurisdictions, multinationals, companies engaged in cloud-computing transactions, outsourcing transactions etc.

3.6.3 However, will also apply to anybody sending an email or other communication containing personal information to a foreign country

3.6.4 Requirements to be met:

- third party must be subject to a law similar to POPIA to ensure adequate level of protection like the principles of POPIA to restrict further transfer;
- the Data Subject consents to the transfer;
- transfer is necessary for the performance of a contract between the Data Subject and the responsible party, concluded in the interest of the Data Subject; and
- the transfer is for the benefit of the Data Subject.

4. APPLICABILITY & AUTHORITY

4.1 This policy applies to the business of MFM wherever it is conducted. It applies to all employees, key individuals, representatives, directors, clients, and other stakeholders.

4.2 This policy is authorised by the Chairperson of the MFM Board and the MFM Information and Compliance Officers are duly authorised to implement and monitor compliance with this policy.