LUNAR CAPITAL PRIVACY NOTICE

1 INTRODUCTION AND PURPOSE

Lunar Capital (Pty) Ltd ("Lunar", "we", "us" or "our") is committed to protecting the confidentiality, integrity, and availability of personal information in accordance with the **Protection of Personal Information Act 4 of 2013 ("POPIA")**, the **Financial Advisory and Intermediary Services Act ("FAIS")**, the **Financial Intelligence Centre Act ("FICA")**, and all other applicable legislation.

The purpose of this Privacy Notice is to provide data subjects with transparent information regarding:

- what personal information we collect;
- how and from whom it is collected;
- the lawful purposes for which it is processed;
- how it is stored, shared, and retained; and
- the rights of data subjects in relation to their personal information

2 CATEGORIES OF PERSONAL INFORMATION COLLECTED

Depending on the nature of our relationship and services rendered, Lunar may collect and process the following categories of personal information:

Client and Investor Information

- Full names, identity numbers, passport numbers, dates of birth
- Contact details (physical, postal and email addresses, telephone numbers)
- Employment, occupational and income details
- Financial information, including asset and liability information
- Bank account details and payment instructions
- Risk profile, investment objectives and mandate-related information
- Information required on application, onboarding, mandate, and portfolio management forms
- Correspondence, queries, instructions, complaints and claims records

FICA and Regulatory Information

- Identity verification documentation
- Proof of address
- Source of funds and source of wealth information
- Tax residency and tax identification numbers
- Politically Exposed Person (PEP) and sanctions screening information
- Ongoing due diligence and monitoring records

Juristic Persons and Representatives
Where the client is a juristic person, we may collect:

- Registration and constitutional documents
- Details of directors, trustees, members, shareholders and beneficial owners
- Details of authorised, juristic or mandated representatives
- Mandates, resolutions and letters of authority

Intermediaries and Third Parties

- Details of appointed financial services intermediaries
- Licensing and accreditation information
- Contact and professional information required to perform services

3 METHODS OF COLLECTION

Personal information is collected through various lawful and reasonable means, including:

- Directly from clients, investors, representatives or employees
- Via our website, including "Contact Us" enquiries
- Through authorised financial services intermediaries
- When Lunar assists with form completion, onboarding, administration and portfolio management
- Through email correspondence, queries, complaints and claims
- From third-party service providers, regulators or public sources where permitted
- Where juristic or mandated representatives are appointed on behalf of a client

4 LAWFUL PURPOSE FOR PROCESSING PERSONAL INFORMATION

Personal information is processed strictly for legitimate business purposes and in accordance with applicable law. Processing is limited to what is necessary, relevant, and adequate for the purpose for which the information is collected.

Where required, consent will be obtained. In many instances, processing is necessary to comply with legal obligations or to perform contractual obligations and therefore does not rely on consent alone.

Clients (Prospective and Existing Clients, Beneficiaries, and Related Parties)
Personal information is processed for the following purposes:

- Providing discretionary and non-discretionary financial services
- Portfolio management and investment decision implementation
- To conduct client onboarding, identification and verification in line with KYC and anti-money laundering requirements

- To comply with obligations under applicable legislation, including FAIS, FICA, tax laws, and other regulatory requirements
- To source, structure, and implement appropriate financial products and solutions
- To facilitate transactions, administration, and investment management
- To engage with product suppliers, administrators, and other providers on behalf of clients
- To maintain client records and relationship management systems
- To communicate with clients regarding products, services, updates, and regulatory disclosures
- To process and manage disbursements, claims, benefits, and pay-outs, including assisting beneficiaries
- To handle client queries, complaints, and dispute resolution processes
- To comply with audit, governance, and internal control requirements
- To conduct risk management, fraud prevention, and detection activities
- To perform data analytics, research, and service improvement initiatives
- To comply with reporting obligations to regulators, including the Financial Sector Conduct Authority
- To enable business continuity, record keeping, and legal compliance processes
- To establish, exercise, or defend legal rights and obligations, including engagement with courts, legal advisors, and dispute resolution bodies
- Detecting, preventing and reporting fraud, financial crime and regulatory breaches
- Internal governance, risk management, audit and recordkeeping

Client personal information is retained for as long as required by applicable legislation, contractual obligations, and legitimate business needs, including the resolution of disputes, audits or regulatory enquiries.

5 VENDORS, SUPPLIERS AND SERVICE PROVIDERS

Lunar collects and processes personal information relating to vendors, suppliers, contractors and service providers engaged to support its business operations.
This may include, where applicable:

- Contact details of directors, members, partners, authorised signatories and employees
- Identity and verification information required for due diligence and onboarding
- Company registration details and related constitutional documents (where relevant)
- Bank account details and payment-related information
- Tax, compliance and regulatory information
- Contractual, commercial and correspondence records

- Information required for risk management, governance, audit and business continuity purposes

Personal information relating to vendors and suppliers is collected:

- directly from the vendor or supplier;
- through onboarding, contracting and procurement processes; or
- from publicly available or regulatory sources, where lawful.

The processing of such information is undertaken for lawful and necessary business purposes, including:

- To conduct vendor onboarding, due diligence, and risk assessments
- To verify vendor identity, ownership, and regulatory status
- To perform contract negotiation, management, and administration
- To facilitate procurement and supply chain management processes
- To process payments, invoicing, and financial administration
- To manage service delivery, performance monitoring, and service level agreements
- To ensure compliance with legal, regulatory, and governance requirements
- To conduct background checks, including sanctions screening where applicable
- To manage access to systems, infrastructure, and facilities
- To maintain vendor records and audit trails
- To support internal and external audit processes
- To comply with tax and financial reporting obligations
- To manage disputes, claims, and contractual enforcement
- To support business continuity and operational resilience planning
- To establish, exercise, or defend legal rights, including engagement with legal representatives and courts

6 REGULATORS AND SUPERVISORY AUTHORITIES

In the course of conducting its regulated business, Lunar may collect and process limited personal information relating to regulators, supervisory authorities, and officials acting in an official or representative capacity. This may include, where applicable:

- Names, titles and designations of regulatory officials
- Official contact details, including email addresses, telephone numbers and business addresses
- Correspondence records, submissions, reports and supporting documentation
- Information contained in regulatory enquiries, inspections, supervisory engagements or enforcement-related communications

This personal information is obtained:

- directly through formal engagement, correspondence and regulatory processes;

- via official regulatory platforms, portals and public records; or
- as contained in documentation lawfully provided to or received from regulatory authorities.

The processing of personal information relating to regulators is conducted strictly for lawful and legitimate purposes, including:

- fulfilling statutory, regulatory and supervisory obligations;
- responding to regulatory enquiries, inspections and information requests;
- submitting applications, reports, notifications and regulatory returns;
- managing regulatory relationships, governance oversight and compliance assurance; and
- maintaining accurate records of regulatory interactions for audit, risk management and accountability purposes.

Personal information of regulators is processed in accordance with POPIA, taking into account that such information is generally collected in an official or public capacity.

7 EMPLOYEES, CONTRACTORS AND REPRESENTATIVES

Lunar collects and processes personal information relating to its employees, independent contractors, temporary staff, secondees, interns and appointed representatives for legitimate operational, regulatory and governance purposes.

7.1 Categories of Personal Information Collected

Depending on the nature of the engagement, this may include:

- Identification information, including names, identity numbers, passport numbers and dates of birth
- Contact details, including residential, postal and email addresses and telephone numbers
- Employment, contractual and engagement details, including role, responsibilities, remuneration and benefits
- Banking, payroll, tax and statutory deduction information
- Qualifications, professional registrations, licensing and fit and proper information
- Performance, training, competency and disciplinary records
- System access credentials, usage logs and information security records
- Leave, attendance, time-tracking and capacity management information
- Health and emergency contact information where required by law or for operational necessity
- Correspondence and records relating to employment, engagement or termination

7.2 Purpose of Processing

Personal information of staff and contractors is processed strictly in accordance with POPIA for lawful and necessary purposes, including:

Staff (Employees, Contractors, Temporary Staff, and Applicants)

Processing is undertaken on the basis of legal obligation, contractual necessity, legitimate interests and, where applicable, consent, including:

- To conduct recruitment, selection, and onboarding processes
- To verify identity, qualifications, references, and background checks
- To comply with fit and proper requirements (where applicable in financial services)
- To manage employment contracts and employment relationships
- To administer payroll, remuneration, and employee benefits
- To comply with tax, labour, and employment legislation
- To manage leave, attendance, and performance management processes
- To support training, development, and competency requirements
- To ensure workplace health and safety compliance
- To manage disciplinary processes, grievances, and internal investigations
- To engage with labour advisors and dispute resolution bodies, including the Commission for Conciliation, Mediation and Arbitration
- To manage access to systems, infrastructure, and information security controls
- To monitor IT usage, cybersecurity, and data protection compliance
- To conduct internal audits, risk management, and governance processes
- To comply with regulatory reporting obligations
- To maintain employee records and statutory registers
- To support business continuity and operational requirements
- To establish, exercise, or defend legal rights and obligations, including litigation and dispute resolution

8 PROCESSING OF PERSONAL INFORMATION IN COMPLAINTS HANDLING

Lunar collects and processes personal information when managing queries, complaints, disputes or expressions of dissatisfaction, whether received from clients, investors, intermediaries, representatives, vendors, staff or other stakeholders. This may include:

- identification and contact details of the complainant and affected parties;
- details of the complaint, supporting documentation and correspondence;
- transactional, contractual and portfolio-related information;
- investigation records, internal assessments and decision outcomes; and
- records of remedial actions, responses and regulatory reporting (where applicable).

Personal information collected in the complaints process is processed strictly for lawful and legitimate purposes, including:

- investigating and resolving complaints fairly and timeously;
- complying with FAIS complaints management obligations and conduct standards;
- responding to regulatory enquiries or supervisory requests;
- maintaining accurate records for audit, governance and risk management purposes; and
- defending or enforcing legal rights where required.

Complaints-related personal information is retained for the periods prescribed under FAIS, FICA and other applicable legislation, and for longer periods where reasonably necessary to address future disputes, legal proceedings or regulatory reviews.

9 THIRD-PARTY PERSONAL INFORMATION

Where you provide us with personal information relating to another individual (for example, a spouse, dependent, director, employee, or authorised user), you warrant that:

- you are authorised to provide such information to us;
- the information has been collected and shared in a lawful manner; and
- the relevant individual has been informed of this privacy notice and, where required, has consented to the processing of their personal information.

You indemnify us against any loss or claim arising from your failure to comply with these requirements.

10 PERSONAL INFORMATION OF MINORS

We do not knowingly collect or process personal information relating to a minor without the involvement of a parent or legal guardian. Where personal information of a minor is provided to us, the parent or legal guardian confirms that:

- they have the authority to act on behalf of the minor;
- they consent to the collection and processing of the minor's personal information for the purposes set out in this notice; and
- they will ensure that the minor's personal information provided is accurate and kept up to date.

We reserve the right to request proof of such authority or consent at any time.

11 WEBSITE INFORMATION

11.1 Personal Information

Personal information submitted via our website (for example through enquiries or complaints) is processed strictly for the purpose for which it was provided and will not be used for unrelated activities.

11.2 Automatically Collected Non-Personal Information

During website visits, limited non-personal information may be automatically collected, including:

- Internet domain and IP address
- Browser and operating system type
- Date, time and pages visited
- Referring website addresses

This information is used solely for statistical analysis, security monitoring, and website optimisation. No individual is personally identified through this process.

11.3 Embedded and Third-Party Content

Our website may contain embedded content (such as videos or articles) hosted on third-party platforms. Such content operates as if the user has accessed the third-party website directly. These platforms may collect data independently in accordance with their own privacy policies, over which Lunar has no control.

11.4 External Links

Our website may contain links to third-party websites. Lunar is not responsible for the privacy practices or content of such external sites, and users are encouraged to review their privacy notices before providing personal information.

12 PERSONAL DATA SHARING

Personal information may be shared with third parties only where lawful and necessary, including:

- Financial services intermediaries and product providers
- Administrators and platform providers
- Auditors, insurers and professional and legal advisers
- Collective investment scheme managers and administrators
- Regulators, supervisory bodies and statutory authorities
- Professional advisers, insurers, auditors and compliance service providers
- Technology, hosting and systems service providers
- Payroll, human resources and benefits service providers;

All third parties are required to implement appropriate confidentiality, security and POPIA-aligned safeguards. Personal information may also be disclosed where required by law, court order, or to protect legitimate interests such as fraud prevention or enforcement of agreements.

13 CROSS BORDER TRANSFERS

Personal information may be transferred to, stored, or processed in jurisdictions outside of the Republic of South Africa where this is necessary for legitimate business purposes, including the use of cloud-based systems and service providers. Personal information may be processed using platforms provided by global technology providers such as Microsoft Corporation. These providers operate global infrastructure, and personal information may be stored or processed in data centres located in, inter alia:

- Ireland
- The Netherlands
- Germany
- Finland
- The United Kingdom
- The United States of America

Due to the nature of cloud computing and redundancy architectures, personal information may also be transferred to or accessed from other jurisdictions in which these providers maintain operations from time to time. Where personal information is transferred across borders, the organisation will ensure that:

- The recipient is subject to a law, binding corporate rules, or binding agreement that provides an adequate level of protection that upholds principles substantially similar to those contained in POPIA; or
- The data subject has consented to the transfer; or
- The transfer is necessary for the performance or conclusion of a contract between the data subject and the organisation; or
- The transfer is otherwise permitted in terms of applicable law

14 TECHNICAL AND ORGANISATION SAFEGUARDS

Lunar Capital implements a combination of technical and organisational security measures designed to protect personal information against loss, unauthorised access, misuse, alteration, or destruction. These measures are aligned with applicable legal requirements, industry standards, and recognised information security practices.

14.1 Governance and Risk Management

- Information security governance framework aligned to applicable regulatory requirements and industry standards
- Information security responsibility is assigned at a senior management level, with oversight and reporting to the board or equivalent governing body
- Regular risk assessments are conducted to identify, assess, and mitigate information security risks, including cyber risks
- A formal incident response and breach management process is in place

14.2 Access Control and Identity Management

- Access to personal information is restricted on a need-to-know and role-based basis
- Users are authenticated using secure login credentials, including multi-factor authentication (MFA) where appropriate
- User access rights are reviewed regularly and revoked upon termination or change of role
- Privileged access is strictly controlled, monitored, and logged
- Physical access to systems and records is restricted to authorised personnel only

14.3 Data Protection and Encryption

- Personal information is protected through encryption technologies during transmission and, where appropriate, at rest
- Secure communication protocols (e.g. HTTPS, TLS) are used for electronic data exchange
- Sensitive personal information is subject to enhanced protection measures
- Data masking or anonymisation techniques are used where appropriate

14.4 Network and System Security

- Firewalls, intrusion detection and prevention systems, and endpoint protection
- Systems are protected against malware, ransomware, and other cyber threats
- Regular patch management and system updates are performed to address vulnerabilities
- Secure configuration standards are applied to systems and devices
- Continuous monitoring and logging of system activity is implemented

Where cloud-based services are utilised, Lunar Capital relies on providers that implement industry-standard security controls, certifications, and safeguards.

14.5 Data Lifecycle Management

- Personal information is collected, processed, stored, and disposed of in accordance with defined data lifecycle management practices
- Records are retained in line with legal and regulatory retention requirements
- Secure methods are used for the destruction or anonymisation of personal information when no longer required
- Data quality controls are implemented to ensure accuracy and completeness

14.6 Backup, Business Continuity and Disaster Recovery

- Regular data backups are performed and securely stored
- Backup data is tested periodically to ensure recoverability and integrity

- A Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) are maintained and tested
- Systems are designed to ensure availability and resilience, including failover capabilities where appropriate

14.7 Third-Party and Operator Management

- Third-party service providers ("operators") are subject to due diligence assessments prior to engagement
- Written agreements are in place to ensure that operators implement appropriate security measures and process personal information only under instruction
- Ongoing monitoring of service providers is conducted to ensure continued compliance
- Cross-border transfers are subject to appropriate safeguards and contractual protections

14.8 Staff Awareness and Training

- Employees and contractors receive regular training and awareness programmes on data protection, cybersecurity, and information security practices
- Staff are required to adhere to confidentiality obligations and internal policies
- Disciplinary processes are in place for non-compliance with security requirements

14.9 Incident Management and Breach Notification

- Security incidents are identified, reported, and managed through a formal incident response process
- Breaches involving personal information are assessed and, where required, reported to the Information Regulator and affected data subjects in accordance with applicable law
- Root cause analysis and remediation measures are implemented following incidents

14.10 Continuous Improvement

- Lunar Capital adopts a **continuous improvement approach** to information security
- Security measures are regularly reviewed and enhanced in response to:
    - Emerging threats
    - Technological developments
    - Regulatory changes
- Independent assessments, audits, or reviews may be conducted to evaluate the effectiveness of controls

14.11 Cross-border Data Transfer

Safeguards to protect personal information during cross-border transfers, include:

- Entering into data processing and cross-border transfer agreements with service providers
- Ensuring that service providers implement industry-standard security measures, including encryption, access controls, and data segregation
- Limiting transfers to what is necessary and proportionate for the purpose of processing
- Conducting risk-based due diligence on service providers and their international data transfer mechanisms

While Lunar Capital implements appropriate, reasonable technical and organisational measures to safeguard personal information, no method of transmission over the internet or electronic storage is completely secure. Accordingly, the organisation does not guarantee absolute security but undertakes to continuously enhance its safeguards in line with evolving risks and industry best practice.

15 RETENTION OF PERSONAL INFORMATION

Personal information is retained for the duration of the contractual relationship and:

- for as long as required under **applicable legislation**; and
- for extended periods where reasonably necessary for legitimate business purposes to address future servicing queries, complaints, disputes, regulatory enquiries, audits or legal claims.

Regulator personal information is retained for as long as required to demonstrate regulatory compliance, support governance and risk management processes, and meet applicable legal or recordkeeping obligations.

Once retention periods expire, information is securely destroyed or de-identified, unless continued retention is legally required.

16 DATA SUBJECT RIGHTS

Data subjects have the right to:

- request access to personal information held by Lunar;
- request correction or updating of inaccurate information;
- object to certain forms of processing, where applicable; and
- request deletion of personal information where no lawful basis for retention exists.

Requests may be refused where retention is required by law or where information has been lawfully de-identified.

17 COMPLAINTS, QUERIES AND REGULATORY ENGAGEMENT

17.1 Internal Complaints Contact Details

If you have a complaint or query relating to the processing of your personal information or the services provided by Lunar, please contact us in the first instance:

Email: info@lunarcapital.co.za

We are committed to resolving complaints fairly, transparently and in accordance with applicable regulatory requirements.

17.2 Regulatory and Oversight Contact Details

If you are dissatisfied with the outcome of a complaint, or believe that your personal information has been processed unlawfully, you may lodge a complaint with the relevant regulatory authority:

Information Regulator (South Africa)

Responsible for oversight of POPIA compliance.

Website: https://www.justice.gov.za/inforeg https://inforegulator.org.za/complaints

Telephone: 010 023 5200

- Toll Free : 0800 017 160
- enquiries@inforegulator.org.za