Rootstock Investment Management (Pty) Ltd

8 Helderberg Street, Stellenbosch
7600, South Africa
PO Box 722, Stellenbosch
7599, South Africa

T +27 (0)21 883 9256
E info@rootstockinvestments.co.za
www.rootstockinvestments.co.za

ROOTSTOCK INVESTMENT MANAGEMENT PROPRIETARY LIMITED

(the "Company")

PERSONAL INFORMATION PROTECTION POLICY

Contents

1. INTRODUCTION

1.1. The Company is an authorised financial services provider whose business includes the collection of Personal Information from its clients, suppliers and employees. The Company endeavours to comply with all the relevant legislation and regulations relating to the protection of Personal Information.

1.2. This Personal Information Protection Policy (the "Policy") documents and records the principles and policies the Company follows when collecting and Processing Personal Information, describes the required business activities relating to Personal Information Processing and specifies the responsibilities of the Company when complying with the relevant legislation and regulations.

1.3. The Company acknowledges that it must comply with South African legislation, in the form of the Protection of Personal Information Act, 2013 (Act no. 4 of 2013) ("POPIA") as it Processes Personal Information in South Africa. In addition, the Company acknowledges that it has to comply with the European Union General Data Protection Regulation ("GDPR") as GDPR impacts South African based companies which Process Personal Information of EU residents, and due to the fact that convergence of these various data protection legislation and regulations are imminent.

2. DOCUMENTS OF REFERENCE

2.1. Protection of Personal Information Act, 2013 (Act no. 4 of 2013)

2.2. European Union General Data Protection Regulation (**"GDPR"**)

2.3. Promotion of Access to Information Act, 2000 (Act no.2 of 2000)

2.4. Personal Information Breach Register

2.5. Privacy Notice

2.6. Personal Information Access Request Form

2.7. Personal Information Breach Register

2.8. Personal Information Risk Questionnaire

2.9. Register of Personal Information Processing Activities

3. DEFINITIONS

3.1. **"Anonymization"** or **"De-identify"** means irreversibly De-identifying Personal Information such that the person cannot be identified by using reasonable time, cost and technology. Personal Information Processing principles do not apply to Anonymized data.

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

3.3. **"Encryption"** means scrambling the entire contents of a set of information using mathematical techniques.

3.4. **"Operator"** means a natural or juristic person, public authority or any other institution which Processes Personal Information on behalf of the Responsible Party.

3.5. **"Personal Information"** means any information relating to an identifiable natural person, or to the extent applicable, a juristic person. This includes, but is not limited to information relating to race, gender, sex, pregnancy, marital status, ethnic and social origin, colour, sexual orientation, age, physical or mental health, religion, disability, language, information relating to educational, medical, financial, criminal or employment history, any identifying number, email address, physical address, telephone number, location information, online identifier or biometric Personal Information.

3.6. **"Personal Information Access Request"** means a process designed to ensure the Company complies with its legal obligations when providing Data Subjects with access to their Personal Information.

3.7. **"Personal Information Breach(es)"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to Personal Information transmitted, stored or otherwise Processed.

3.8. **"Personal Information Risk and Impact Assessment"** means a process designed to describe the Processing activities, assess the risks and the impact of the identified risks, and to help manage the risks to the rights and freedoms of Data Subject(s) resulting from the Processing of Personal Data.

3.9. **"Processing"** means any activity concerning Personal Information including the 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 form, or merging, linking, as well as restriction, degradation, erasure or destruction of information.

3.10. **"Pseudonymization"** means the Processing of Personal Information in such a manner that the Personal Information can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately.

3.11. **"Re-identify"** means to resurrect any information that has been De-identified.

3.12. **"Regulatory Authority"** means the Information Regulator as established by POPIA or any other relevant Regulatory Authority.

3.13. **"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 REGARDING PERSONAL INFORMATION PROCESSING

4.1. Accountability

4.1.1. The Company acknowledges that, as a Responsible Party, it must ensure compliance with the relevant regulations. The Information Officer has been designated with this responsibility.

4.2. Lawful Processing of Personal Information

4.2.1. The Company will ensure that Personal Information is Processed lawfully, fairly and transparently in relation to the Data Subject. Personal Information collected must not be excessive, must be legally justifiable and not collected from third parties without good reason.

4.3. Purpose limitation

4.3.1. Personal Information collected is limited and relevant in relation to the specific purpose for which it is Processed. Personal Information will not be stored for any longer than necessary.

4.4. Data minimization

4.4.1. The Company will ensure that Personal Information is adequate and limited to what is necessary in relation to the purpose for which it is Processed.

4.5. Information quality

4.5.1. All Personal Information collected will be complete and accurate and the Company will take reasonable steps to ensure that inaccurate data is corrected in a timely manner.

4.6. Lawful processing of personal information

4.6.1. The Company will ensure that Personal Information is processed lawfully, fairly and transparently. Personal Information collected must not be excessive, must be legally justifiable and not collected from third parties without good reason.

4.7. Security safeguard relating to integrity and Personal Information confidentiality

4.7.1. The Company will ensure that Personal Information is Processed securely and will use appropriate information technology measures to protect Personal Information against accidental or unlawful destruction, loss, amendment or unauthorized access. Notification of any data breaches will occur timeously.

4.8. Restriction on further Processing

4.8.1. Personal Information may only be Processed for the purpose for which it was collected under specific conditions.

4.9. Transparency

4.9.1. The Company will Process Personal Information in a transparent manner.

4.10. Data Subject participation

4.10.1. Data Subjects will be allowed to access their Personal Information and request that it is corrected or deleted if inaccurate. The Company acknowledges that Personal Information that is inaccurate, irrelevant, inappropriate, ambiguous or unlawfully obtained is to be corrected or deleted.

4.11. Storage period limitation

4.11.1. Personal Information must be stored for no longer than necessary for the purposes for which it is Processed.

5. INFORMATION PROTECTION PROCESSES

5.1. Communication to Data Subjects

5.1.1. The Company is responsible for communicating to Data Subjects which types of Personal Information is collected, the purposes of the Processing of the Personal Information, the Processing methods, the Data Subjects' rights and the retention periods. The Information Officer will ensure that the Data Subjects are notified when Personal Information is shared with third parties. Refer to the Privacy Notice.

5.1.2. The Information Officer will authorise which Personal Information is Processed. The Company will perform a Data Protection Impact Assessment for each Personal Information Processing activity.

5.2. Data Subject's consents

5.2.1. The Information Officer will be responsible for retaining the records of the Data Subject's consents regarding the Processing of Personal Information. In addition, the Information Officer will ensure that any request to correct, change or destroy Personal Information is dealt with within a reasonable time frame and keep records thereof. The Company will ensure that any consents given by the Data Subjects are voluntary, specific and an informed expression of will. Refer to Personal Information Consent Form.

5.3. Personal Information collection

5.3.1. The Company will attempt to collect the minimum amount of Personal Information possible. If any Personal Information is collected from a third party, the Information Officer will ensure that the information is collected lawfully.

5.4. Personal Information use, retention and deletion

5.4.1. All Personal Information will be used, retained and deleted or destroyed in a manner consistent with the purpose as described in the Company's Privacy Notice. The Company will ensure that Personal Information remains accurate and confidential when being Processed.

5.5. Data Subject's access rights

5.5.1. The Company's Information Officer will ensure that Data Subjects are provided with reasonable access to their Personal Information. The Company will further ensure that its Data Subjects can update, correct, delete or transfer their Personal Information if required.

5.6. Personal Information transferability

5.6.1. Data Subjects have the right to receive a copy of their Personal Information provided to the Company. The Information Officer will ensure that the Data Subject's Personal Information can be transmitted to another party if so required and will ensure that such requests are processed timeously.

5.7. Third-party disclosures

5.7.1. In instances where the Company utilizes third parties to Process Personal Information, the Information Officer will ensure that the third parties have adequate security measures in place to safeguard Personal Information.

5.8. Right to delete or destroy Personal Information

5.8.1. The Company will ensure that Personal Information of the Data Subject can be deleted or destroyed upon the Data Subject's request. Personal Information destruction will occur as soon as reasonably practical after the request has been made.

5.9. Privacy Notice

5.9.1. A Privacy Policy will be available to Data Subjects of the Company and will be written in clear, plain language. The Privacy Notice will be made available through the Company's website and will include details of how Personal Information is Processed.

5.9.2. The Privacy Notice will also include the name and contact details of the Company's Information Officer, the nature of Personal Information that is collected, the purpose for its collection and the rights of the Data Subject.

5.10. Security measures

5.10.1. The storage and transfer of Personal Information will occur in a secure environment. The Company will ensure that a risk assessment is completed in order to identify all reasonably foreseeable internal and external risks to Personal Information under its control. Technical measures will be utilised to secure Personal Information, and such measures may consist of De-identification (anonymization) or Encryption. The Company will ensure that the Information Regulator is notified of any data breaches as soon as reasonably possible, and will also notify all Data Subjects affected by such breaches.

6. RESPONSIBILITIES OF THE COMPANY

6.1. The Company, as the Responsible Party, is committed to principles of accountability, transparency and consensual and responsible Processing of Personal Information.

6.2. It is the intention of the Company that this Policy will protect a Data Subject's Personal Information from being compromised in any way and this Policy is consistent with the privacy laws applicable in South Africa.

6.3. The board of directors of the Company is responsible for approving this Policy and the Information Officer is responsible for managing and implementation of the Personal Information protection processes.

6.4. The Company's Compliance Officer will monitor Personal Information protection regulation to ensure that all developments are incorporated into the Company's business activities.

6.5. The Information Officer of the Company will ensure that employees' awareness of Personal Information protection is raised and will further ensure that employee Personal Information protection takes place.

7. INFORMATION OFFICER/CONTACT DETAILS

7.1. Any questions relating to the Company's Privacy Policy or the treatment of an individual's Personal Information should be addressed to the Information Officer, whose contact details are:

Information Officer : Retha de Villiers

Telephone number : +2721 883 9256

Postal address : PO Box 722, Stellenbosch, 7599

Physical address	: 8 on Helderberg, Helderberg Street, Stellenbosch, 7600
E-mail address	: retha@rootstock.com.mt
Website	: rootstockinvestments.co.za

8. BREACH PROCEDURE

8.1. Breach Response

8.1.1. The Information Officer must ensure that resources, with the relevant skills and knowledge, are established in order to respond to any Personal Information Breaches.

8.1.2. The resources, together with the Information Officer, are responsible for ensuring that a Personal Information Breach response process exists and that a response to any Personal Information Breach can be executed timeously.

8.1.3. The Information Officer has the authority to utilise the services of external parties in order to deal with Personal Information Breaches.

8.2. Breach Response Duties

8.2.1. The Information Officer and the resources responsible for Personal Information Breaches must implement the following processes:

- Validation;
- Investigation;
- Requirements to mitigate;
- Resolution tracking;
- Reporting;
- Coordination with the relevant regulatory authorities; and
- Notification to the relevant Data Subjects.

8.3. Breach Response Process

8.3.1. The Information Officer and the responsible resources for Personal Information Breaches must ensure that a breach response process is initiated as soon as anyone notices that a suspected/ actual Personal Information Breach has occurred.

8.3.2. The Information Officer must ensure that all information relating to the Personal Information Breach is documented.

8.4. Breach Notifications

8.4.1. Notifications from the Operator to the Responsible Party

8.4.1.1. The Information Officer of the Responsible Party must report any actual or suspected breach of Personal Information to the Responsible Party.

8.4.1.2. The notification must include the following:

- A description of the Personal Information Breach;
- The types of Personal Information affected;
- The consequences of the Personal Information Breach;
- The number of Data Subjects affected by the Personal Information Breach; and
- Processes implemented to remedy any future Personal Information Breaches.

8.4.2. Notifications from the Responsible Party to the Regulatory Authority

The Information Officer must:

8.4.2.1. Ensure that the Personal Information Breach is reported to the relevant Regulatory Authority;

8.4.2.2. Perform a Personal Information Protection Risk and Impact Assessment;

8.4.2.3. Record the Personal Information Breach in the Personal Information Breach Register; and

8.4.2.4. Notify the relevant Regulatory Authority of the Personal Information Breach within 72 (seventy two) hours of its occurrence.

8.4.3. Notification from the Responsible Party to the Data Subject

8.4.3.1. The Information Officer must notify Data Subjects of Personal Information Breaches.

8.4.3.2. The notification must contain the following information:

- A description of the Personal Information Breach;
- Types of Personal Information affected;
- The consequences of the Personal Information Breach;

- Number of Data Subjects affected by the Personal Information Breach; and
- Processes implemented to remedy any future Personal Information Breaches.

9. ACCESS REQUEST PROCEDURE

9.1. Access request from the data subject

9.1.1. A Personal Information Access Request is a request made by an individual or a juristic entity via its authorised representative for Personal Information held by the Company.

9.1.2. The Personal Information Access Request provides the Data Subject with the right to view or request copies of Personal Information Processed by the Company.

9.1.3. The Personal Information Access Request must be made in writing to the Information Officer of the Company.

9.1.4. The Data Subject can make a Personal Information Access Request by:

- Sending an e-mail to the Information Officer at retha@rootstock.com.mt.

9.2. Access request process

9.2.1. The individual requesting access to their Personal Information will need to complete a Personal Information Access Request form and provide it to the Information Officer.

9.2.2. The Information Officer will verify the identity of the individual making the Personal Information Access Request to ensure that the individual has the right to view the Personal Information.

9.2.3. The Information Officer will notify the Data Subject that their Personal Information Access Request will be attended to within 30 (thirty) days.

9.2.4. The Information Officer will ensure all relevant Personal Information is sourced internally or from third parties, if so required.

9.2.5. The Information Officer will provide a response to the Data Access Request form as well as the Personal Information via a secure method.

9.3. Access request rejections

Personal Information Access Requests may be rejected if:

9.3.1. The Personal Information is stored only for statistical purposes and the identification of the Data Subject from the Personal Information is not possible; or

9.3.2. The Personal Information Access Request is made for other non-Personal Information protection purposes.

9.4. Exclusions

9.4.1. A Data Subject does not have the right to access Personal Information recorded about another Data Subject, unless Personal Information is being accessed by the authorized representative of the Data Subject.

9.4.2. The following information will not be disclosed by the Company:

- Information about other Data Subjects;
- Publicly available information;
- Privileged documents; and
- Information protected by copyright law.

10. RETENTION

10.1. Retention period

10.1.1. The Company deems the default retention period for Personal Information to be 5 (five) years, in the absence of any documented information or requirement by specific regulation. The default retention period of 5 (five) years will commence at the date of the termination of the business relationship.

10.2. Protection of Personal Information during the retention period

10.2.1. The Company will ensure that retained Personal Information, stored in electronic format, is protected against unauthorised access or loss. All procedures and systems utilized in the electronic storage of Personal Information will be accessible, within a reasonable time period, during the retention period. The responsibility for the storage and protection of Personal Information is that of the Information Officer.

10.3. Personal Information destruction

10.3.1. The Company will review all its stored Personal Information regularly in order to decide whether to destroy or delete any Personal Information. Personal Information deletion or destruction will only be applicable once the purpose for which the documents or electronic records were collected and stored, is no longer applicable.

10.3.2. The Personal Information Retention Schedule as provided, in the Register of Personal Information Processing Activities, will also describe how Personal Information is to be disposed of. The Company agrees that the destruction of Personal Information may be dealt with internally or externally but that the Company remains responsible for such destruction.

10.3.3. The Company will ensure that appropriate controls are in place to prevent the permanent loss of Personal Information as a result of unintentional, negligent or malicious actions.

10.4. Routine destruction of Personal Information

10.4.1. The Company will routinely destroy the following Personal Information unless the Personal Information is subject to a legal proceeding or regulatory investigation:

- Documents such as application forms, letters and e-mail messages;
- Address lists and distribution lists, and;
- Copies of documents, snapshot printouts or any extract from any Personal Information database of the Company.

10.5. Destruction process

10.5.1. The Information Officer will ensure that all documents retained by the Company are classified as either low- or high-risk documents.

10.5.2. High risk documents will contain information that is confidential and include documents which contain Personal Information. These documents will be destroyed by way of shredding or electronic deletion.

10.5.3. Low risk documents do not contain any Personal or proprietary Information, and include Company published documents. These documents will also be shredded and may be disposed of without an audit trail.

11. RISK AND IMPACT ASSESSMENT

11.1. Responsibilities for the Risk and Impact assessment

11.1.1. Performing a Risk and Impact Assessment is mandatory for Responsible Parties.

11.1.2. The Information Officer is responsible for the Risk and Impact Assessment.

11.1.3. The Risk and Impact Assessment must be concluded by identifying the risks relating to the protection of Personal Information, assessing the identified risks, implementing risk mitigation techniques and reporting the Risk and Impact Assessment results to the Company.

11.2. Risk and Impact assessment process

11.2.1. Identifying all Personal Information Processing activities

- The Information Officer must identify and list all the Personal Information Processing activities and detail these in the Register of Personal Information Processing Activities.

11.2.2. Complete a Risk Assessment Questionnaire

- For each Personal Information Processing activity, the Information Officer will complete the Risk Assessment Questionnaire.

11.2.3. Identify key security risks

- Once the Information Officer has completed the Risk Assessment Questionnaire, the findings to identify key risks need to be documented.

11.2.4. Mitigation of risks

- Once the key risks are identified, the Information Officer must mitigate any high-risk Personal Information Processing activities.

11.2.5. Record the implementation

- All mitigation activities must be documented as completed once implemented by the Information Officer.

11.2.6. Review of the Risk and Impact Assessment

The Information Officer must review the Risk and Impact Assessment in any of the following cases:

- If risks related to Personal Information Processing activities change; or

- If there is a significant change in the Personal Information Processing activities; or
- If there is a change in the legal requirements.