

Spectra Trust

TM/3246

5 Voorschoten Steet, Dal Josafat, Paarl, 7646
("the Company")

**COMPLIANCE FRAMEWORK & MANUAL IN TERMS OF THE PROTECTION
OF PERSONAL INFORMATION ACT, 2013**

1. DEFINITIONS AND INTERPRETATION

- 1.1. **“the Company”** means **Spectra Trust, TM/3246**;
- 1.2. **“Constitution”** means the Constitution of the Republic of South Africa, 1996;
- 1.3. **“Client”** refers to any natural or juristic person that received or receives services from the Company;
- 1.4. **“Data Subject”** has the meaning ascribed thereto in terms of section 1 of POPIA;
- 1.5. **“Information Officer”** means the duly authorised Information Officer, in terms of POPIA, as per the Information Officer Appointment Document, attached hereto;
- 1.6. **“Manual”** means this manual prepared in accordance with POPIA;
- 1.7. **“Personal Information”** has the meaning ascribed thereto in section 1 of POPIA;
- 1.8. **“POPIA”** means the Protection of Personal Information Act 4 of 2013;
- 1.9. **“POPIA Regulations”** means the regulations promulgated in terms of section 112(2) of POPIA;
- 1.10. **“Processing”** has the meaning ascribed thereto in section 1 of POPIA;
- 1.11. **“Responsible Party”** has the meaning ascribed thereto in section 1 of POPIA;
- 1.12. **“SAHRC”** means the South African Human Rights Commission.
- 1.13. Capitalised terms used in this Manual have the meanings ascribed thereto in section 1 of POPIA as the context specifically requires, unless otherwise defined herein.

2. INTRODUCTION

2.1. POPIA

- 2.1.1. POPIA was assented to on 26 November 2013. Broadly, the purpose of POPIA is to give effect to section 14 of the Constitution, being the constitutional right to privacy by protecting Personal Information and regulating the free flow and Processing of Personal Information.
- 2.1.2. POPIA sets minimum conditions which all Responsible Parties must comply with so as to ensure that Personal Information is respected and protected. These minimum conditions are the Conditions for Lawful Processing and are more fully described in paragraph 4.1 this Manual.

2.2. Purpose of the Manual

- 2.2.1. The purpose of this Manual is to give effect to the constitutional right to privacy in relation to the protection of Personal Information.
- 2.2.2. POPIA recognises that the right to privacy may be limited in accordance with section 36 of the Constitution to the extent that such limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality, and freedom.
- 2.2.3. This Manual, amongst other things, details the purpose for which Personal Information may be processed; a description of the categories of Data Subjects for whom the Company Processes Personal Information as well as the categories of Personal Information relating to such Data Subjects; and the recipients to whom Personal Information may be supplied.
- 2.2.4. This Manual has been compiled by the Information Officer:
- 2.2.4.1. as an integral part of the Company’s compliance framework in terms of Regulation 4(1)(a) of the POPIA Regulations; and

- 2.2.4.2. following the completion of a personal information impact assessment as envisaged by section 4(1)(b) of the POPIA Regulations.

3. THE COMPANY CONTACT DETAILS

- 3.1. Name of Information Officer: **Gerhard J Fourie**
 3.2. Address: 5 Voorschoten Steet, Dal Josafat, Paarl, 7646
 3.3. Postal address: PO Box 267, Paarl, 7646
 3.4. Telephone: 0826571220
 3.5. E-mail: gerhard@spectratrust.co.za

4. PROTECTION OF PERSONAL INFORMATION THAT IS PROCESSED BY THE COMPANY

4.1. Conditions for Lawful Processing

- 4.1.1. Chapter 3 of POPIA provides for the minimum Conditions for Lawful Processing of Personal Information by a Responsible Party. These conditions may not be derogated from unless specific exclusions apply as outlined in POPIA. Below is a description of the eight Conditions for Lawful Processing as contained in POPIA:

- 4.1.1.1. **Accountability** - the Responsible Party has an obligation to ensure that there is compliance with POPIA in respect of the Processing of Personal Information.
- 4.1.1.2. **Processing limitation** - Personal Information must be collected directly from a Data Subject to the extent applicable; must only be processed with the consent of the Data Subject and must only be used for the purposes for which it was obtained.
- 4.1.1.3. **Purpose specification** - Personal Information must only be processed for the specific purpose for which it was obtained and must not be retained for any longer than it is needed to achieve such purpose.
- 4.1.1.4. **Further processing limitation** - further processing of Personal Information must be compatible with the initial purpose for which the information was collected.
- 4.1.1.5. **Information quality** - the Responsible Party must ensure that Personal Information held is accurate and updated regularly and that the integrity of the information is maintained by appropriate security measures.
- 4.1.1.6. **Openness** - there must be transparency between the Data Subject and the Responsible Party.
- 4.1.1.7. **Security safeguards** - a Responsible Party must take reasonable steps to ensure that adequate safeguards are in place to ensure that Personal Information is being processed responsibly and is not unlawfully accessed.
- 4.1.1.8. **Data Subject participation** - the Data Subject must be made aware that their information is being processed and must have provided their informed consent to such processing.

4.2. Purpose of the Processing of Personal Information by the Company

- 4.2.1. As outlined in paragraph 4.1.1.3 above, Personal Information may only be Processed for a specific purpose. The purposes for which the Company Processes or will Process Personal Information is as follows:
- 4.2.2. to provide accounts and/or services to the Client in accordance with terms agreed to by the Client;

- 4.2.3. to undertake activities related to the provision of accounts and/or services to the Client;
- 4.2.4. to verify the identity of the Client;
- 4.2.5. for risk assessment, information security management, statistical, trend analysis and planning purposes;
- 4.2.6. to monitor and record calls and electronic communications with the Client for quality, training, investigation, and fraud prevention purposes;
- 4.2.7. for crime detection, prevention, investigation and prosecution;
- 4.2.8. to enforce or defend the Company's rights;
- 4.2.9. to manage the Company's relationship with the Client, which may include providing information to the Client about the Company's products and/or service;
- 4.2.10. any additional purposes expressly authorised by the Client; and
- 4.2.11. any additional purposes as may be notified to the Client or Data Subjects in any notice provided by the Company.

4.3. **Categories of Data Subjects and Personal Information/special Personal Information relating thereto**

The Company shall Process Personal Information on the following Data subjects:

- 4.3.1. Juristic person:
 - 4.3.1.1. client profile information;
 - 4.3.1.2. account details;
 - 4.3.1.3. payment information;
 - 4.3.1.4. corporate structure;
 - 4.3.1.5. customer risk rating; and
 - 4.3.1.6. client information, including to the extent the categories of information relate to individuals or representatives of Clients (e.g., shareholders, directors, etc.) are required.
- 4.3.2. Natural person:
 - 4.3.2.1. name;
 - 4.3.2.2. contact details (company and home);
 - 4.3.2.3. tax identification number;
 - 4.3.2.4. bank account information (bank account number, bank account name, bank account type);
 - 4.3.2.5. account opening forms; and
 - 4.3.2.6. photographs and other identification and verification data as contained in images of ID card, passport, and other ID documents, including images of customer signature.
- 4.3.3. Employees:
 - 4.3.3.1. name;
 - 4.3.3.2. employee ID number; and
 - 4.3.3.3. business contact details (address/telephone number/email address).

4.4. **Recipients of Personal Information**

The Company may provide a Data Subjects Personal Information to the Company, its affiliates, and their respective representatives.

4.5. **Cross-Border flows of Personal Information**

Section 72 of POPIA provides that Personal Information may only be transferred out of the Republic of South Africa:

- 4.5.1. If the recipient country can offer such data an “adequate level” of protection. This means that its data privacy laws must be substantially similar to the Conditions for Lawful Processing as contained in POPIA; or
- 4.5.2. If the Data Subject consents to the transfer of their Personal Information; or
- 4.5.3. If the transfer is necessary for the performance of a contractual obligation between the Data Subject and the Responsible Party; or
- 4.5.4. If the transfer is necessary for the performance of a contractual obligation between the Responsible Party and a third party, in the interests of the Data Subject; or
- 4.5.5. If the transfer is for the benefit of the Data Subject, and it is not reasonably practicable to obtain the consent of the Data Subject, and if it were, the Data Subject, would in all likelihood provide such consent.

4.6. **Information security measures to be implemented by the Company**

The Company shall implement the following security measures in order to ensure that Personal Information is respected and protected:

4.6.1. **Access Control of Persons**

The Company shall implement suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment where the data is processed.

4.6.2. **Data Media Control**

The Company undertakes to implement suitable measures to prevent the unauthorized manipulation of media, including reading, copying, alteration or removal of the data media used by the Company and containing personal data of clients.

4.6.3. **Data Memory Control**

The Company undertakes to implement suitable measures to prevent unauthorized input into data memory and the unauthorized reading, alteration, or deletion of stored data of the Data Exporter's customers.

4.6.4. **User Control**

The Company shall implement suitable measures to prevent its data processing systems from being used by unauthorized persons by means of data transmission equipment.

4.6.5. **Access Control to Data**

The Company represents that the persons entitled to use the Company's data processing system are only able to access the data within the scope and to the extent covered by their respective access permissions (authorisation).

4.6.6. **Transmission Control**

The Company shall be obliged to enable the verification and tracing of the locations and/or destinations to which the Personal Information is transferred by utilisation of the Company's data communication equipment and devices.

4.6.7. **Transport Control**

The Company shall implement suitable measures to prevent Personal Information from being read, copied, altered, or deleted by unauthorized persons during the transmission thereof or during the transport of the data media.

4.6.8. **Organisation Control**

The Company shall maintain its internal organisation in a manner that meets the

requirements of this Manual.

A preliminary assessment of the suitability of the information security measures implemented or to be implemented by the Company may be conducted in order to ensure that the Personal Information that is processed by the Company is safeguarded and Processed in accordance with the Conditions for Lawful Processing.

4.7. Objection to the Processing of Personal Information by a Data Subject

Section 11(3) of POPIA and regulation 2 of the POPIA Regulations provides that a Data Subject may, at any time object to the Processing of his/her/its Personal Information, in the prescribed form, subject to exceptions contained in POPIA.

The prescribed form is available on request from the Company.

4.8. Request for Correction or Deletion of Personal Information

4.8.1. Section 24 of POPIA and regulation 3 of the POPIA Regulations provides that a Data Subject may request for their Personal Information to be corrected/deleted in the prescribed form.

4.8.2. The prescribed form is available on request from the Company.