SIP nordic
SOUTH AFRICA

PROTECTION OF PERSONAL INFORMATION POLICY AND PROCEDURE

(Information Privacy)

For internal use

Approved by the Governing Body: 7 June 2021

Structured Investment Products South Africa (Pty) Ltd T/A SIP Nordic South Africa
Spaces, Sunclare Building, 4th Floor, 21 Dreyer Street, Claremont, 7780
Telephone: +27 (0)21 013 3616 I E-mail: info@sipnordic.co.za I www.sipnordic.co.za

FSP No. 51065
Reg. No. 2016 / 218894 / 07
Directors: M.N.T. Halvorsen; P Steele

SIP nordic
SOUTH AFRICA

Table of Contents

1. DEFINITIONS

In this policy the following terms and expressions shall have the meanings assigned to it, and if required, any other term or expression shall be interpreted in accordance with POPIA:

1.1. **Data Subject** – Means the person to whom the Personal Information relates, including both a natural and juristic person.

1.2. **Company** – Means Structured Investment Products South Africa (Pty) Ltd a company duly incorporated within the Republic of South Africa under registration number 2016/218894/07, trading as SIP Nordic South Africa, an authorised financial services provider (FSP 51065).

1.3. **PAIA** – Means the Promotion of Access to Information Act, No 2 of 2000.

1.4. **Personal Information** – Means information relating to an identifiable Data Subject's:

1.4.1. Race, gender, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth;

1.4.2. Education, medical, financial, criminal or employment history;

1.4.3. Unique identifying numbers including identity/registration/passport numbers and numbers allocated to the Data Subject by companies and institutions, for e.g. bank account, client or member account numbers;

1.4.4. Contact particulars including physical address, phone numbers, email and other social media addresses or handles and GPS locations;

1.4.5. Private communications and opinions;

1.4.6. Any other information connected to a Data Subject that says something about the person, for e.g. biometric information, personal preferences, idiosyncrasies and names on lists like credit black lists.

1.5. **POPIA** – Means the Protection of Personal Information Act, No 4 of 2013.

1.6. **Public Record** – Means information deliberately made publicly available by the Data Subject, or information contained in records freely accessible to the public, for e.g. web pages, sanction lists, court records, police records, etc.

2. BACKGROUND AND APPLICABILITY

2.1. POPIA governs the processing, meaning the collection, use, dissemination, management, storage and protection, of all Personal Information by responsible persons.

2.2. As a result, the Company has approved and implemented the following policy and procedures to be adhered to when processing Personal Information of a Data Subject.

2.3. This policy applies to all employees of the Company, regardless of seniority or status, and includes those persons on secondment or contracted to the Company.

2.4. This policy must be read with the Company's PAIA Policy where required.

3. COLLECTION OF PERSONAL INFORMATION

3.1. The Data Subjects of the Company:

3.1.1. The Company shall only collect Personal information from the following Data Subjects:

3.1.1.1. Employees of the Company;

3.1.1.2. Clients of the Company; and

3.1.1.3. Service Providers to the Company.

3.1.2. The Company shall not, without the prior consent of the Information Officer collect and/or store any Personal Information from any other person.

3.2. How and from whom Personal Information may be collected:

3.2.1. POPIA requires all Personal Information to be collected either:

3.2.1.1. directly from the Data Subject, and where the Data Subject is a minor, with the permission of the minor's legal guardian;

3.2.1.2. from a person authorised by the Data Subject; or

3.2.1.3. from Public Record.

3.2.2. All Personal Information collected on:

3.2.2.1. Employees and potential employees are collected by the Company directly from the Data Subject, employment brokers and/or Public Record.

3.2.2.2. Clients are collected by the Company, directly from the Data Subject and/or Public Record.

3.2.2.3. Service providers are collected by the Company directly from the Data Subject and/or Public Record.

3.2.3. The Company must at all times ensure that any third party providing the Company with Personal Information of a Data Subject, subscribes to the principles of POPIA, has the Data Subject's authority, and has confidentiality measures in place to protect the Personal Information.

3.3. When and what Personal Information is collected

3.3.1. POPIA requires that the Company only collects such Personal Information as may be authorised by the Client, and as may be required for the purpose it is collected.

3.3.2. Personal Information is only collected when it is required to enter into a transaction with the Data Subject, or once a transaction is concluded with the Data Subject. For:

3.3.2.1. Employees – During the review process of the potential employee and thereafter during the annual review process by the board and management.

3.3.2.2. Clients – During the Company RMCP KYC process and thereafter in line with the Company continued client review process in terms of the RMCP.

3.3.2.3. Service providers – Upon review of the service provider for potential appointment, and thereafter in line with the Company's service delivery review process.

3.3.3. For each of the following Data Subjects the Personal Information required by the Company is limited to:

3.3.3.1. Employees:

3.3.3.1.1. Full names, race and gender.

3.3.3.1.2. Unique numbers: Identity number, bank account number, Income tax numbers and any professional body membership numbers.

3.3.3.1.3. Contact particulars: Physical address, phone numbers and email address.

3.3.3.1.4. Education, medical, financial, criminal and employment history.

3.3.3.2. Clients:

3.3.3.2.1. Full names.

3.3.3.2.2. Unique numbers: Identity/registration number, bank account number and Income tax numbers.

3.3.3.2.3. Contact particulars: Physical address, phone numbers and email address.

3.3.3.2.4. In the case of incorporated persons information on the natural beneficial owner.

3.3.3.2.5. Source of funding and such additional Personal Information as may be required by legislation for enhanced due diligence.

3.3.3.3. Service providers

3.3.3.3.1. Full name.

3.3.3.3.2. Unique numbers: Identity/registration number, bank account number Income tax and VAT numbers, regulatory registration numbers.

3.3.3.3.3. Contact particulars: Physical address, phone numbers and email address.

3.3.3.3.4. Education, financial, criminal and employment history.

3.3.3.3.5. Business audit reports.

3.3.3.3.6. Such additional Personal Information as may be required by the regulators of the Company.

3.4. Section 18 of POPIA

3.4.1. Section 18 of POPIA requires that a Data Subject be informed, prior to the collection of Personal Information, or as soon as possible thereafter on:

3.4.1.1. The source from which the Personal Information is collected if not from the Data Subject;

3.4.1.2. What Personal Information is collected;

3.4.1.3. The purpose for which the Personal Information is collected;

3.4.1.4. If the collection is mandatory or voluntarily or required by legislation;

3.4.1.5. If the Personal Information will be used outside the Republic of South Africa; and

3.4.1.6. the Data Subject's right to object to the Information Regulator on any collection of Personal Information.

3.4.2. The Company ensures that all application forms for clients, agreements with service level providers and employment procedures include all the information required in terms of clause 3.4.1 above.

3.4.3. In the event where Personal Information of a Data Subject must be collected that does not fall within the categories of Data Subjects identified for the Company in clause 3.1, the Information Officer must be notified prior to the collection of such Personal Information.

3.4.4. The Information Officer shall ensure that a Privacy Notice is sent to the specific Data Subject, recording all the requirements of section 18 of POPIA prior to the collection of the Personal Information.

4. USE AND DISSEMINATION OF PERSONAL INFORMATION

4.1. The Company shall use the Personal Information collected for:

4.1.1. Employees to:

4.1.1.1. Verify the person's suitability for the position of employment.

4.1.1.2. Annual review of the suitability of the person in performing his/her duties to the Company.

4.1.1.3. Perform its obligations in terms of the employment agreement by the payment of salaries, determining maternity or paternity leave and sick leave.

4.1.1.4. Fulfil its obligations to governmental institutions including the Receiver of Revenue and the Department of Labour.

4.1.1.5. Where applicable determine the Company's Black Economic Empowerment status.

4.1.2. Clients to:

4.1.2.1. Perform an appropriate KYC and risk assessment as required by FICA.

4.1.2.2. Perform its obligations to the client in accordance with the terms of the mandate.

4.1.2.3. Comply with other regulatory or legislative requirements.

4.1.3. Service providers to:

4.1.3.1. Verify the suitability of the service provider for the services to be rendered.

4.1.3.2. Review the performance of the service provider of the services to the Company.

4.1.3.3. Perform its obligations to the services provider in terms of the service level agreement.

4.1.3.4. Fulfil its obligations to regulatory and governmental institutions including the Receiver of Revenue.

4.2. In fulfilling the purpose, as specified in clause 3.1, for which the Personal Information is collected, the Company disseminates the Personal Information for:

4.2.1. Employees to:

4.2.1.1. Appoint an employment broker to perform background checks.

4.2.1.2. The Company's regulators, including the Financial Sector Conduct Authority, as may be applicable.

4.2.1.3. Its payroll provider.

4.2.1.4. To governmental departments including the Department of Labour and the Receiver of Revenue.

4.2.2. Clients to:

4.2.2.1. The Company's regulators, including the Financial Sector Conduct Authority and the Financial Intelligence Centre, as may be applicable.

4.2.2.2. The governmental departments including the Receiver of Revenue.

4.2.3. Service providers to:

4.2.3.1. The Company's regulators including the Financial Sector Conduct Authority, as may be applicable.

4.2.3.2. The receiver of Revenue.

4.3. All Personal Information collected by the Company is exclusively used for the purposes specified in clause 3.1 above, and exclusively disseminated in accordance with the provisions of clause 3.2 above; and will not be shared with any other third party for any other function, except if so required by an order of a court of law or direction by a regulatory body.

4.4. No employee of the Company shall be allowed to disclose any Personal Information of Data Subjects to any unauthorised third party.

5. STORAGE AND PROTECTION OF PRIVATE INFORMATION

5.1. The Company retains Private Information required for the purposes specified in clause 3.1 for a period of 7 years after the relationship between the Company and the Data Subject has terminated.

5.2. All Private Information must be stored in electronic format.

5.3. All Data Subjects may at any time, in accordance with the provisions of the Company PAIA Policy, request that they be informed of their Personal Information being stored.

5.4. The Company must ensure that the Private Information retained is stored in a manner so as to prevent loss or unauthorised access and use thereof.

5.5. The Company store the Personal Information in a restricted access server with appropriate monitoring, and use a variety of technical security measures to secure the data.

5.6. Where Data Subjects' Personal Information is stored by a third party on behalf of the Company, such storage facilities must be compliant with the provisions of this policy and POPIA.

5.7. No Private Information may be stored outside the Republic of South Africa without the specific authorisation of the Data Subject.

6. INFORMATION MANAGEMENT AND DELETION

6.1. All Private Information received by the Company but not required for any purpose must be destroyed/deleted immediately.

6.2. In the event of the Company receiving Private Information in hard copy, such information must be converted to electronic copies for storage, and the hard copies destroyed immediately.

6.3. Private Information may only be converted to hard copies if necessary to fulfil the purpose for which it has been collected, or a request by the regulators of the Company, and must be destroyed immediately after such use.

6.4. The Company must ensure that the Private Information retained is correct and up to date and has implemented procedures for the Data Subjects to notify the Company of any changes to their Private Information.

6.5. All Private Information must be destroyed/deleted after the 7 year retention period.

7. REGULATORS

7.1. Information Officer

7.1.1. In accordance with the terms of POPIA the Company CEO is the appointed Information Officer for the purposes of POPIA and PAIA.

7.1.2. The Information Officer may appoint such deputies as he/she may deem appropriate.

7.1.3. The Information Officer and any appointed deputies must be registered with the Information Regulator.

7.1.4. The functions of the Information Officer are to:

7.1.4.1. Ensure the Company complies with POPIA and PAIA.

7.1.4.2. Deal with all information requests directed at the Company from the Information Regulator or in terms of the Company PAIA Manual.

7.1.4.3. Undertake a Personal Information risk impact assessment and implementing a management framework.

7.1.4.4. In all manners co-operate with the Information Regulator.

7.2. Information Regulator

7.2.1. The government has in accordance with the provisions of POPIA established the Information Regulator.

7.2.2. The functions of the Information Regulator are to:

7.2.2.1. Enforce compliance with the provisions of POPIA and PAIA.

7.2.2.2. Provide education on the lawful processing of Private Information.

7.2.2.3. Monitor the use of Private Information by private and public institutions and their processing activities.

7.2.2.4. Monitor the use of Data Subjects' unique identifier numbers.

7.2.2.5. Consult with and act as mediator between Data Subjects and responsible parties, such as the Company, on issues of privacy and the protection of Personal Information.

7.2.2.6. Examine proposed legislation and issue Codes of Conduct that has a bearing on the processing of information.

7.2.2.7. Facilitate cross-border co-operation in the enforcement of privacy laws.

7.2.2.8. Receive complaints of non-compliance, instigate pre-investigations, attend to hearings and issue Enforcement Notices.

7.2.2.9. Appoint an Enforcement Committee to assist in its duties.

8. CONTRAVENTION

8.1. Section 22 of POPIA requires the Company to notify the Information Regulator and the Data Subject, as soon as reasonably possible after any security breach which compromised the Private Information.

8.2. Any person may lodge a complaint, in the prescribed form, with the Information Regulator of non-compliance with the provisions of POPIA or an approved Code of Conduct. The Information Regulator may then:

8.2.1. Initiate an investigation;

8.2.2. Refer the matter to the Enforcement Committee; or

8.2.3. Act as conciliator between the parties.

8.3. Responsible parties as the Company is subject to a fine, imprisonment for a period not exceeding 10 years, or both in instances:

8.3.1. Of obstructing, hindering or unlawfully influencing the Information Regulator.

8.3.2. Knowingly giving false information to the Information Regulator.

8.3.3. Failure to comply with an Enforcement Notice issued by the Information Regulator.

8.3.4. Unlawfully processing account numbers.

8.3.5. Obstructing a person in executing a warrant on behalf of the regulator.

8.3.6. Failure to attend or obstructing a hearing or failure to provide requested information by the Information Regulator.

8.3.7. Failure to notify the Information Regulator of any activity as may be required by legislation.

8.4. As a result, failure to observe or comply with any part of this policy will constitute misconduct warranting disciplinary action, which may include dismissal. Furthermore, employees should note that:

8.4.1. The burden of proof rests with the employee to prove compliance with this policy; and

8.4.2. This policy forms part of the terms and conditions of employment.

8.5. The Company may report contraventions to any other professional bodies it feels are appropriate (e.g. the FSCA, CFA Institute, SAICA, etc).