Manual in terms of the Promotion of Access to Information Act, No. 2 of 2000 for Financial Services Provider (FSP) Trisure Risk Administrator (Pty) Ltd, FSP Number 52161.

1. Introduction

The Promotion of Access to Information Act 2 of 2000 ("PAIA" or "the Act") gives effect to the constitutional right of access to any information held by the state and any information that is held by another person and that is required for the exercise or protection of any rights. The Protection of Personal Information Act 2013 has amended the PAIA and also requires private bodies to disclose certain information through the relevant organisation's PAIA Manual.

Specifically, section 51(1) of the Act, read with the Protection of Personal Information Act of 2013, requires a private body to compile a manual that must contain information as specified and required by both PAIA and POPI. In addition, the PAIA manual must set out the formal procedure that a person must follow in order to request to view, update or delete personal information held by the private body.

In this context, a "private body" is defined as any natural person who carries or has carried on any trade, business, or profession, but only in such capacity or any partnership which carries or has carried on any trade, business, or profession or any former or existing juristic person (e.g. any company, close corporation, or business trust).

This organisation falls within the definition of a "private body" and this Manual has been compiled in accordance with the said provisions and to fulfil the requirements of the Act.

In terms of the Act, where a request for information is made to a body, there

is an obligation to provide the information, except where the Act expressly provides that the information may not be released. In this context, Section 9 of the Act recognises that access to information can be limited. In general, the limitations relate to circumstances where such release would pose a threat to the protection of privacy, commercial confidentiality, and the exercising of efficient governance.

Accordingly, this manual provides a reference to the records held and the process that needs to be adopted to access such records..

All requests for access to information (other than information that is available to the public) must be addressed to the Head of the organisation named in section 2 of this Manual.

2. Business and Contact Details

2.1. Name of Business - Trisure Risk Administrator (Pty) Ltd

2.2. Head of Business – Mr. Zulfikar Nakhooda

2.3 Position – Director / Key Individual

2.4 Physical Address - 1st Floor, Gateview House A1, Constantia Office Park, Weltevreden Park, Johannesburg, 1709

2.5 Postal Address - 1st Floor, Gateview House A1, Constantia Office Park, Weltevreden Park, Johannesburg, 17098

2.6 Contact Details - Phone Number 031 944 5553 / 066 1295511

E-mail address zulfi@trisurerisk.co.za

3. Section 51(1) of the Promotion to Access to Information Act (THE ACT)

3.1. The Act grants a requester access to records of a private body, if the record is required for the exercise or protection of any rights. If a public body lodges a request, the public body must be acting in the public interest.

3.2. Requests in terms of the Act must be made in accordance with the prescribed procedures, at the rates provided. The forms and tariff are dealt with in regulations 6 and 7 of the Act.

3.3. Requesters are referred to the Guide which, in terms of Section 10 as amended, has been compiled by the Information Regulator established in terms of section 39 of the Protection of Personal Information Act, 2013, and which contains information for the purposes of exercising Constitutional Rights.

A "Request for a copy of the Guide (Form 1)" is available at:
https://www.justice.gov.za/inforeg/docs2-f.html

The Guide is also available at:

Address:	JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001
Postal Address:	PO Box 31533, Braamfontein, Johannesburg, 2017
Tel. No:	010 023 5200
Email Address:	PAIACompliance@infoRegulator.org.za

4. Records available in terms of Section 52(2) of THE ACT

Not applicable

5. Records that are held at the offices of the business

The following is a list of records held at the offices

5.1. Administration

- Attendance registers
- Correspondence
- Founding Documents
- Licences (categories)
- Minutes of Management Meetings
- Shareholder Register
- Statutory Returns

5.2. **Human Resources**

- Conditions of Service
- Employee Records
- Employment Contracts
- General Correspondence
- Information relating to Health and Safety Regulations
- Personnel Guidelines, Policies and Procedures
- Remuneration Records and Policies
- Skills Requirements
- Statutory Records
- Training Records

5.3. **Operations**

- Client and Customer Registry
- Contracts

- Client Policy documentation
- General Correspondence
- Marketing Records
- Production Records
- Policy contracts and wordings
- Policies required in terms of the FAIS Act
- Sales Records
- Suppliers' Registry

5.4. Finances

- Annual Financial Statements
- Asset Register
- Banking Records
- Contracts
- Financial Transactions
- General Correspondence
- Insurance Information
- Management Accounts
- Tax Records (company and employee)

5.5. Information Technology

- IT Policies and Procedures

5.6. **Statutory Records:**

At present these include records (if any) held in terms of:

- Administration of Estates Act 66 of 1965
- Basic Conditions of Employment 75 of 1997
- Close Corporations Act 69 of 1984
- Collective Investment Schemes Control Act 45 of 2002
- Companies Act 71 of 2008
- Compensation for Occupational Injuries and Health Diseases Act 130 of 1993
- Consumer Protection Act 68 of 2008
- Currency and Exchanges Act 9 of 1933
- Finance Act 35 of 2000
- Financial Advisory and Intermediary Services Act 37 of 2002/General Code of Conduct
- Electronic Communications and Transactions Act 25 of 2002
- Financial Intelligence Centre Act 38 of 2001
- Financial Services Board Act 97 of 1990
- Harmful Business Practices Act 23 of 1999
- Income Tax Act 95 of 1967
- Insolvency Act 24 of 1936
- Financial Institutions (Protection of Funds) Act 28 of 2001
- Financial Services Ombud Schemes Act 37 of 2004
- Labour Relations Act 66 of 1995
- Long Term Insurance Act 52 of 1998

- Inspection of Financial Institutions Act 80 of 1998
- Medical Schemes Act 131 of 1998
- Occupational Health & Safety Act 85 of 1993
- Pension Funds Act 24 of 1956
- Protection of Businesses Act 99 of 1978
- National Credit Act 34 of 2005
- Short Term Insurance Act 53 of 1998
- Skills Development Levies Act 9 of 1999
- Promotion of Access to Information Act 2 of 2000
- Skills Development Act 97 of 1998
- The Securities Services Act 36 of 2004)
- Tax on Retirement Funds Act 38 of 1996
- Unemployment Insurance Act 63 of 2001

6. Processing of personal information

6.1. Purpose of Processing

- Fulfilling statutory obligations in terms of applicable legislation
- Historical record keeping, research and recording statistics necessary for fulfilling your business objectives.
- Keeping of accounts and records
- Marketing and advertising
- Monitoring, maintaining and managing our contractual obligations to customers, clients, suppliers, service providers, employees, directors and other third parties

- Obtaining information necessary to provide contractually agreed services to a customers and clients
- Resolving and tracking complaints
- Staff administration
- Verifying information provided to us

6.2. Categories of Data Subjects

- Clients and client's employees, representatives, agents, contractors and service providers
- Existing and former employees (including contractors, agents, temporary and casual employees)
- Healthcare patients and healthcare providers associated with patients
- Our stakeholders
- Suppliers and service providers and their respective authorised employees, representatives, agents, contractors and service providers of such suppliers and service providers

6.3. Categories of Personal Information processed

Natural Persons

- Names
- Physical and postal addresses
- Date of birth
- ID number
- Tax related information
- Medical, dental, mental and/or other healthcare related information

- Nationality
- Gender
- Confidential correspondence
- Email address
- Telephone number

Juristic Persons

- Names of contact persons
- Name of Legal Entity
- Registration Number
- Physical and Postal address and contact details
- Financial information
- Founding documents
- Tax related information
- Authorised signatories, beneficiaries, ultimate beneficial owners
- BBBEE information

6.4. Categories of special information processed

- Racial / ethnic origin
- Physical / mental health details

6.5. Possible Recipients of Personal Information

- Auditors
- Banks and other financial institutions.
- Claims investigators
- Educators and examining bodies

- Employees of the organisation
- Employment and recruitment agencies
- Family, associates and representatives of the person whose personal information is processed
- Healthcare, social and welfare organisations
- Ombudsman and regulatory authorities
- Patient associated healthcare facilities and professionals
- Police / courts where necessary
- Regulatory, statutory and government bodies
- Suppliers, service providers, vendors, agents and representatives of such entities
- Third party verification agencies and credit bureau

6.5. Trans-border / cross border flows of personal information

It may be required from time to time to share personal information of data subjects with third parties in other countries. Any sharing of personal information of data subjects with third parties in other countries will be done only if the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection which effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person, as set out in the Protection of Personal Information Act and the data subject consents to the transfer.

Any such transfer will have to be shown to be necessary for the performance of a contract between the data subject and the recipient in question, or for the implementation of pre- contractual measures

taken in response to the data subject's request.

6.6. General Description of Information Security Measures

Up to date technology is employed to ensure the confidentiality, integrity and availability of the Personal Information under our care.

Measures include:

- Acceptable usage of personal information
- Access control to personal information
- All third parties with whom any contract exists are required to ensure that appropriate security, privacy and confidentiality obligations are observed.
- Computer and network security including Firewalls, Virus protection software and update protocols
- Governance and regulatory compliance
- Information security and HR policies include confidentiality clauses for employees
- Internal process to report security breach or anticipated security breach
- Investigating and reacting to security incidents.
- Logical and physical access control
- Monitoring access and usage of private information
- Physical security
- Retention and disposal of information
- Secure communications
- Security in the outsourcing of any activities or functions through appropriate contracts

- Training of staff members

We continuously establish and maintain appropriate, reasonable technical and organisational measures to ensure that the integrity of the Personal Information which may be in our possession or under our control, is secure and that such information is protected against unauthorised or unlawful processing, accidental loss, destruction or damage, alteration or access by having regard to the requirements set forth in law, in industry practice and generally accepted information security practices and procedures applicable.

7. Information request procedure

- The requester must use the prescribed form to make the request for access to a record. The prescribed form is available from the Head of Business named in Section 2 above. The form is also available from the website of the Department of Justice and Constitutional Development at www.doj.gov.za
- The request must be made to the Head of Business named in Section 2 above. This request must be made to the address, fax number or electronic mail address of the business.
- The requester must provide sufficient detail on the request form to enable the Head of Business to identify the record and the requester. The requester should also indicate which form of access is required. The requester should also indicate if any other manner should be used to inform the requester. If this is the case, please furnish the necessary particulars to be so informed.
- The requester must identify the right that is sought to be exercised or to be protected and must provide an explanation of why the requested record is required for the exercise or protection of that right.
- If a request is made on behalf of another person, the requester must submit proof of the capacity in which the requester is making the

request to the satisfaction of the Head of Business aforesaid.

- The prescribed request fee must be attached.
- We will respond to your request within 30 days of receiving the request by indicating whether your request for access has been granted or denied.
- Please note that the successful completion and submission of a request for access form does not automatically allow the requestor access to the requested record.

Access will be granted to a record only if the following criteria are fulfilled:

- The record is required for the exercise or protection of any right; and
- The requestor complies with the procedural requirements set out in the Act relating to a request; and
- Access to the record is not refused in terms of any ground for refusal as contemplated in Chapter 4 of Part 3 of the Act.

8. Denial of Access

Access to any record may be refused under certain limited circumstances. These include:

- The protection of personal information from unreasonable disclosure concerning any natural person;
- The protection of commercial information held concerning any third party (for example trade secrets);
- The protection of financial, commercial, scientific or technical information that may harm the commercial or financial interests of any third party;
- Disclosures that would result in a breach of a duty of confidence owed to a third party;
- Disclosures that would jeopardize the safety or life of an individual;
- Disclosures that would prejudice or impair the security of property or means of transport;
- Disclosures that would prejudice or impair the protection of a person in

accordance with a witness protection scheme;

- Disclosures that would prejudice or impair the protection of the safety of the public;
- Disclosures that are privileged from production in legal proceedings unless the privilege has been waived;
- Disclosures of details of any computer program;
- Disclosures that will put Trisure Risk Administrator (Pty) Ltd at a disadvantage in contractual or other negotiations or prejudice it in commercial competition;
- Disclosures of any record containing any trade secrets, financial, commercial, scientific, or technical information that would harm the commercial or financial interests of Trisure Risk Administrator (Pty) Ltd
- Disclosures of any record containing information about research and development being carried out or about to be carried out by Trisure Risk Administrator (Pty) Ltd

If access to a record or any other relevant information is denied, our response will include:

- Adequate reasons for the refusal; and
- Notice that you may lodge an application with the court against the refusal and the procedure including details of the period for lodging the application.

Right to challenge Decision

The FSP is not a public body referred to in paragraph (a) of the definition of "public body" in section 1 of the Act. Therefore, no internal appeal lies against the decision of the Information Officer regarding access to information.

If a requester does not agree with the decision, the requester may apply, within 180 days of being advised of the Head of Business's decision, to the High Court having jurisdiction, for an appropriate order.

A requester may also seek relief from any court with appropriate jurisdiction in

respect of the following decisions of the Information Officer:

- The amount of fees required to be paid; and / or
- The extension of the period within which the information will be provided.

9. FEES

The applicable fees are prescribed in terms of the Regulations promulgated under the Act. There are two basic types of fees payable in terms of the Act.

Request Fee

The non-refundable request fee of R 50 (excluding VAT) is payable on submission of any request for access to any record. This does not apply if the request is for the personal records of the requestor. No fee is payable in such circumstances.

Access Fee

The access fee is payable prior to being permitted access to the records in the required form. The applicable fees are prescribed in terms of Part III of Annexure A as identified in Government Notice Number 187, Regulation 11.

10. Manual Availability

A copy of this Manual may be obtained from the Head of Business referred to in Section 2 hereof

Any transmission costs or postage required in respect of hard copies of the Manual will be for the account of the requester.

11. Processing of Personal Information in terms of The Protection of Personal Information in terms of the Protection of Personal Information Act No. 4 of 2013

11.1. The FSP must collect and use information, including personal information as defined in the Protection of Personal Information Act, to the extent that it is necessary to properly perform the functions, obligations and duties.

11.2. The FSP processes personal information of the following data subject categories:

- Information required for the rendering of Financial services in terms of Advice and Intermediary services for which the FSP is authorized by the FSCA to render.
- FSP employees and job applicants
- Third party suppliers
- Regulatory bodies that the FSP is governed by
- The following categories of personal information are processed to fulfil the functions:-

1. Identifying number (employee number; company registration numbers, ID number)
2. Email-addresses, physical address, telephone number
3. Names, surname, marital status, nationality, sexual orientation, age, physical health status, mental health status, well-being, disability status, language, birthplace, date of birth.
4. Biometric information
5. Information on your race, ethnic or social origin, criminal recordings /proceedings
6. Education, medical, financial, employment information

11.3. Personal information is only disclosed if it is necessary to fulfil our legislative mandate for business purposes, where there is a legal

obligation, there is a public duty to disclose the information, or the legitimate interests of the data subject require disclosure or consent was provided by data subject to disclose the information.

11.4. The recipients of information include FSP service providers, other regulators (including foreign regulators), law enforcement agencies, and verification agents.

11.5. Personal information may be processed in other jurisdictions outside of South Africa for business purposes, sharing with foreign regulators for fulfilling a legislative mandate or law enforcement agencies for investigation purposes.

11.6. Where appropriate, we request the third parties with whom we share information with, to take adequate measures and comply with applicable data protection laws and protect the information we are disclosing to them. We do this through contractual arrangements with these third parties. We also take internal measures to ensure that the third parties we appoint have appropriate measures to protect the information we provide to them