FINLEYS

OUTSOURCED BUSINESS SERVICES

Protection of Personal Information Act (POPI Act / POPIA)

POLICY

of

FINLEYS OUTSOURCED BUSINESS SERVICES (PTY) LTD

REGISTRATION NUMBER 2010/023622/07

Table of Contents

1.	**INTRODUCTION**	4
2.	**DEFINITIONS**	4
2.1	**Personal Information**	4
2.2	**Data Subject**	5
2.3	**Responsible party**	5
2.4	**Operator**	5
2.5	**Information Officer**	5
2.6	**Processing**	5
2.7	**Record**	6
2.8	**Filing System**	6
2.9	**Unique Identifier**	6
2.10	**De-Identify**	6
2.11	**Re-Identify**	6
2.12	**Consent**	6
2.13	**Direct Marketing**	7
2.14	**Biometrics**	7
3.	**POLICY PURPOSE**	7
4.	**POLICY APPLICATION**	8
5.	**RIGHTS OF DATA SUBJECTS**	8
5.1	**The Right to Access Personal Information**	8
5.2	**The Right to have personal Information Corrected or Deleted**	9
5.3	**The Right to Object to the processing of Personal Information**	9
5.4	**The Right to Object to Direct Marketing**	9
5.5	**The Right to Complain to the Information Regulator**	9
5.6	**The Right to be Informed**	9
6.	**GENERAL GUIDING PRINCIPLES**	9
6.1	**Accountability**	10
6.2	**Processing Limitation**	10
6.3	**Purpose Specification**	11
6.4	**Further Processing Limitation**	11
6.5	**Information Quality**	11
6.6	**Open Communication**	11
6.7	**Security Safeguards**	12
6.8	**Data Subject Participation**	12
7.	**INFORMATION OFFICERS**	13
8.	**SPECIAL DUTIES AND RESPONSIBILITIES**	13
8.1	**Accountability**	13
8.2	**Information Officer**	14
8.3	**IT Manager**	15
8.4	**Employees and other Persons acting on behalf of the Company**	15
9.	**POPI AUDIT**	18
10.	**REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE**	19
11.	**POPI COMPLAINTS PROCEDURE**	19
12.	**DISCIPLINARY ACTION**	20

POLICY STATEMENT

- This Policy forms part of the policy owners' internal business processes and procedures.

- Any reference to the "company" shall be interpreted to include the "policy owner".

- The organization's governing body, its employees, volunteers, contractors, suppliers and any other person acting on behalf of the company are required to familiarize themselves with the policy's requirements and undertake to comply with the stated processes and procedures.

- Risk owners and control owners are responsible for overseeing and maintaining control procedures and activities.

- The company will:

    - Comply with both the law and good practice;
    - Respect individuals' rights;
    - Be open and honest with individuals whose data is held;
    - Provide training and support for staff who handle personal data, so that they can act confidently and consistently.

- The Company recognizes that its first priority under the POPI Act is to avoid causing harm to individuals. In the main this means:

    - Keeping information securely in the right hands;
    - Retention of good quality information.

- The Act aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are considered. In addition to being open and transparent, the company will seek to give individuals as much choice as is possible and reasonable, over what data is held and how it is used.

1. INTRODUCTION

The right to privacy is an integral human right recognized and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 ("POPIA").

POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a content-sensitive manner.

Through the provision of quality goods and services, the company is necessarily involved in the collection, use and disclosure of certain aspects of personal information of clients, customers, employees and other stakeholders.

A person's right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions.
Given the importance of privacy, the company is committed to effectively managing personal information in accordance with POPIA's provisions.

2. DEFINITIONS

2.1 Personal Information

Personal information is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person, including but not limited to information concerning:

- Race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person;

- Information relating to the education or the medical, financial, criminal or employment history of the person;

- Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

- The biometric information of the person;

- The personal opinions, views or preferences of the person;

- Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the content of the original correspondence;

- The views or opinions of another individual about the person;

- The name of the person if it appears with other personal information relating to the person, or if the disclosure of the name itself, would reveal information about the person.

2.2 Data Subject

This refers to the natural or juristic person to whom personal information relates, such as an individual client, customer or a company that supplies the Company with products or other goods. The rights of data subjects are set out in clause 5 (page 9) of this policy.

2.3 Responsible party

The responsible party is the entity that needs the personal information for a particular reason and determines the purpose for, and means for processing information. In this case, the Company is the responsible party.

2.4 Operator

An operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

2.5 Information Officer

The information Officer is responsible for ensuring the Company's compliance with POPIA.

Where no Information Officer is appointed, the head of the Company will be responsible for performing the Information Officer's duties.

Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers may also be appointed to assist the Information Officer. The Duties of the information Officer is set out in clause 8.2 (page 15) of this policy.

2.6 Processing

The Act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes:

- The collection, receipt, recording, organising, collation, storage, updating or modification, retrieval, alternation, consultation or use;

- Dissemination by means of transmission, distribution or making available in any other form; or

- Merging, linking, as well as any restriction, degradation, erasure or destruction of information.

2.7 Record

Means any recorded information, regardless of form or medium, including:

- Writing on any material;
- Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device and any material subsequently derived from information so produced, recorded or stored;
- Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
- Book, map, graph or drawing;
- Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced.

2.8 Filing System

Means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

2.9 Unique Identifier

Means any identifier that is assigned to a data subject and is used by the responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

2.10 De-Identify

Means to delete any information that identifies a data subject or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.

2.11 Re-Identify

In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

2.12 Consent

Means any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information.

2.13 Direct Marketing

Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

- Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or

- Requesting the data subject to make a donation of any kind for any reason.

2.14 Biometrics

Means a technique of personal identification that is based on physical, physiological or behavioural characterisation; including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

3. POLICY PURPOSE

The purpose of this Policy is to protect the company from compliance risks associated with the protection of personal information which includes:

- Breaches of confidentiality:
    - For instance, the company could suffer loss in revenue where it is found that personal information of a data subject has been shared or disclosed inappropriately.

- Failing to offer choice:
    - For instance, all data subjects should be free to choose how and for what purpose the Company uses information relating to them.

- Reputational damage:
    - For instance, the company could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by the company.

This policy demonstrates the company's commitment to protecting the privacy rights of data subjects in the following manner:

- Through stating desired behaviour and directing compliance with the provisions of POPIA and best practice;

- By cultivating a Company culture that recognises privacy as a valuable human right;

- By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information;

- By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of the company;

- By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and when necessary, Deputy Information Officers in order to protect the interests of the company and data subjects;

- By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

4. POLICY APPLICATION

This Policy and its guiding principles apply to:

- The Company's governing body;
- All branches, business units and divisions of the Company;
- All employees and volunteers;
- All contractors, suppliers and other persons acting on behalf of the Company.

The Policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as the Company's PAIA manual as required by the Promotion of Access to Information Act 2 of 2000.

The legal duty to comply with POPIA's provisions is activated in any situation where there is:

- A **processing** of **personal information** entered into a **record** by a **responsible person** who is **domiciled** in South Africa.

5. RIGHTS OF DATA SUBJECTS

Where appropriate the Company will ensure that its clients and customers are made aware of the rights conferred upon them as data subjects.

5.1 The Right to Access Personal Information

The company recognises that a data subject has the right to establish whether the Company holds personal information related to him, her or it, including the right to request access to that personal information.

All requests for personal information must be made in written form and presented to the Information officer in accordance with clause 10 (page 19) of this policy.

An example of a "Personal Information Request Form" can be found under Annexure A (page 22).

5.2 The Right to have personal Information Corrected or Deleted

The data subject has the right to request, where necessary, that their personal information must be corrected or deleted where the company is no longer authorised to retain personal information under the authority of legislation or agreement with the data subject.

5.3 The Right to Object to the processing of Personal Information

The data subject has the right, on reasonable grounds, to object to the processing of their personal information.

In such circumstances, the Company will give due consideration to the request and the requirements of POPIA. The Company may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

5.4 The Right to Object to Direct Marketing

The data subject has the right to object to the processing of their personal information for purposes of direct marketing by means of unsolicited electronic communications.

5.5 The Right to Complain to the Information Regulator

The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of their personal information.

An example of a "POPI Complaint form" can be found under Annexure B (page 23).

5.6 The Right to be Informed

The data subject has the right to be notified that their personal information is being processed by the Company.

The data subject also has the right to be notified in any situation where the Company has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

6. GENERAL GUIDING PRINCIPLES

All employees and persons acting on behalf of the Company will at all times be subject to and act in accordance with, the following guiding principles:

6.1 Accountability

Failing to comply with POPIA could potentially damages the company's reputation or expose the Company to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

The Company will ensure that the provisions of POPIA and the guiding principles listed in this policy are complied with through the encouragement of desired behaviours. However, the Company will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outline in this Policy.

6.2 Processing Limitation

The scope of this aspect of the policy is defined by the provisions of POPIA under Condition 2 and Sections 9 to 12. The Company will ensure that personal information under its control is processed:

- In a fair, lawful and non-excessive manner; and
- Only with the informed consent of the data subject; and
- Only for a specifically defined purpose.

The company will inform the data subject of the reasons for collecting their personal information and obtain written consent prior to processing the information. Alternatively, where services or transactions are concluded telephonically or by electronic video feed, the Company will maintain a voice recording of the stated purpose for collecting the personal information followed by the data subject's subsequent consent.
Examples of what the company may collect is:

- First Names;
- Surnames;
- Residential or Business addresses;
- Email addresses;
- Telephone or Cellphone numbers;
- User-generated content, posts and other content the data subject may knowingly submit to the company.

The Company will under no circumstances distribute or share personal information between separate legal entities, associated Company's (such as subsidiary companies) or with any individuals that are not directly involved in facilitating the purpose for which the information was originally collected.

Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other aspects of the company's business and be provided with the reasons for doing so.

An example of a "POPI Notice and Consent Form" can be found under Annexure C (page 24).

6.3 Purpose Specification

All of the Company's business units and operations must be informed by the principle of transparency.

The Company will undertake to comply with the POPI Act, conditions 2 in terms of processing limitation, sections 13 and 14. The Company will process personal information only specific, explicitly defined and for legitimate reasons. The Company will inform data subjects of these reasons prior to collecting or recording of a data subject's personal information.

6.4 Further Processing Limitation

Personal Information will not be processed for a secondary purpose unless that processing is compatible with the original purpose.

Therefore, where the Company seeks to process personal information, it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, the Company will first obtain additional consent from the data subject.

The scope of this aspect of the policy is defined by the provisions of POPIA under Condition 4.

6.5 Information Quality

The company will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading and to comply with Section 16 of POPIA in this regard. Where personal information is collected or received from third parties, the Company will take reasonable seps to confirm that the information is correct by certifying the accuracy of the information directly with the data subject or by way of independent sources.
The Company will regularly review its procedures for ensuring that the records remain accurate and consistent and, in particular:

- Systems will be designed, where possible, to encourage and facilitate the entry of accurate data;

- Data on any data subject will be held in as few places as necessary, and all staff will be discouraged from establishing unnecessary additional data sets;

- Staff who keep more detailed information about any data subject will be given additional guidance on accuracy in record keeping as per clause 8.4 (page 15) of this policy.

6.6 Open Communication

The company will take reasonable steps to ensure that the data subjects are notified that their personal information is being collected including the purpose for which it is being collected and processed.

The Company will ensure that it establishes and maintains a "contact us" facility for data subjects who want to:

- Enquire whether the Company holds related personal information; or
- Requests access to related personal information; or
- Request the company to update or correct related personal information; or
- Make a complaint concerning the processing of personal information.

6.7 Security Safeguards

The Company will manage the security of its filling system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.

Security measures will also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as medical information or credit card details, the greater the security required.

The Company will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the Company's IT network. The company will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals to limit cyber-fraud.

All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which the Company is responsible.

All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality causes.

The company's operators and third-party service providers will be required to pledge their commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

6.8 Data Subject Participation

A data subject may request the correction or deletion of his, her or its personal information held by the company.

The company will ensure that it provides a facility for data subjects who want to request the correction or deletion of their personal information.

Where applicable, the company will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

7. INFORMATION OFFICERS

The Company will appoint an information Officer and where necessary, a Deputy Information Officer to assist the Information Officer.

The Company's Information Officer is responsible for ensuring compliance with POPIA.
Where no Information Officer is appointed, the director(s) of the company will assume the role of Information Officer. Consideration will be given on an annual basis to the re-appointment or replacement of the Information Officer and the Re-appointment or replacement of any Deputy Information Officers.

Once appointed, the Company will register the Information Officer with the South African Information Regulator established under POPIA prior to performing his or her duties.

8. SPECIAL DUTIES AND RESPONSIBILITIES

8.1 Accountability

The Company's governing body cannot delegate its accountability and is ultimately answerable for ensuring that the company meets its legal obligation in terms of POPIA.

The governing body may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

The governing body is responsible for ensuring that:

- The Company appoints an Information Officer, and where necessary, a Deputy Information Officer;

- All persons responsible for the processing of personal Information on behalf of the Company:

    - Are appropriately trained and supervised to do so;
    - Understand that they are contractually obliged to protect the personal information they come into contact with; and
    - Are aware that a wilful or negligent breach of this policy processes and procedures may lead to disciplinary action being taken against them.

- Data subjects who want to make enquiries about their personal information are made aware of the procedure that needs to be followed should they wish to do so;

- The scheduling of a periodic POPI audit in order to accurately assess and review the ways in which the Company collects, holds uses, shares, discloses, destroys and processes personal information.

8.2 Information Officer

The Company's Information Officer is responsible for:

- Taking steps to ensure the Company's reasonable compliance with the provisions of POPIA;

- Keeping the governing body updates about the Company's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to POPIA;

- Continually analysing privacy regulations and aligning them with the Company's personal information processing procedure. This will include reviewing the Company's information protection procedures and related policies;

- Ensuring that POPI audits are scheduled and conducted on a regular basis;

- Ensuring that the Company makes it convenient for data subjects who want to update their personal information to submit POPI related to the Company. For instance, maintaining a "contact us" facility on the Company's website;

- Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by Company. This will include overseeing the amendment of the Company's employment contracts and other service level agreements;

- Encouraging compliance with the conditions required for the lawful processing of personal information;

- Ensuring that employees and other persons acting on behalf of the Company are fully aware of the risks associated with the processing of personal information and that they remain informed about the Company's security controls;

- Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the Company;

- Addressing employees POPIA related questions;

- Addressing all POPIA related requests and complaints made by the Company's data subjects;

- Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate with regard to any other matter;

- The Deputy Information Officer will assist the Information Officer in performing his/ her duties.

8.3 IT Manager

The company may choose to outsource the duties of an IT Manager to a responsible third party. Such IT Manager or outsourced party will be responsible for:

- Ensuring that the Company's IT infrastructure, filling system and any other devices used for processing personal information meet acceptable security standards;

- Ensuring that all electronically held personal information is kept only on designation drives and servers and uploaded only on approved cloud computing services;

- Ensuring that servers containing personal information are sited in a secure location, away from the general office space;

- Ensuring that all electronically stored personal information is backed-up and tested on a regular basis;

- Ensuring that all backups containing personal information are protected from unauthorised access, accidental deletion and malicious shacking attempts;

- Ensuring that personal information being transferred electronically is encrypted;

- Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software;

- Performing regular IT audits to ensure that the security of the Company's hardware and software systems are functioning properly;

- Performing regular IT audits to verify whether electronically stored personal Information has been accessed or acquired by unauthorised persons;

- Performing a proper due diligence review prior to contracting with operators, to any third-party service providers, to process personal information on the Company's behalf. For instance, cloud computing services.

8.4 Employees and other Persons acting on behalf of the Company

Employees and other persons acting on behalf of the Company will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other employees.

Employees and other persons acting on behalf of the Company are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

Employees and other persons acting on behalf of the Company may not directly or indirectly, utilise, disclose or make public in a manner to any person or third party, either within the Company or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the employee or person to perform his or her duties.

Employees and other persons acting on behalf of the Company, must request assistance from their respective managers or the Information Officer if they are unsure about any aspect related to the protection of a data subjects' personal information.

Employees and other persons acting on behalf of the Company will only process personal information where:

- The data subject, or a competent person where the data subject is a child, consents to the processing; or

- The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or

- The processing complies with an obligation imposed by law on the responsible party; or

- The processing protects a legitimate interest of the data subject; or

- The processing is necessary for pursuing legitimate interests of the company or third party to whom the information is supplied.

Furthermore, personal information will only be processed where the data subject:

- Clearly understands why and what purpose their personal information is being collected; and

- Has granted the company with explicit written or verbally recorded consent to process their personal information.

Employees and other persons acting on behalf of the Company will consequently, prior or processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.

Informed consent is therefore when the data subject clearly understands for what purpose their personal information is needed and who it will be shared with.

Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, the Company will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

Consent to process a data subject's personal information will be obtained directly from the data subject, except where:

- The personal information has been made public; or
- Where valid consent has been given to a third party; or
- The information is necessary for effective law enforcement.

Employees or other persons acting on behalf of the Company will under no circumstance:

- Process or have access to personal information where such processing or accessing is not a requirement to perform their respective work-related tasks and duties;
- Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from the Company's central database or a dedicated server;
- Share personal information informally or verbally;
- Transfer any personal information outside of South Africa without the express permission of the Information Officer or person to whom the information officer has delegated the authority to approve such transfers.

Employees and other persons acting on behalf of the Company are responsible for:

- Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outline within this policy;
- Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filling systems and data sets should therefore be created;
- Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, other persons acting on behalf of the Company, with the sending or sharing of personal information to or with authorised external persons;
- Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords may not be shared with unauthorised persons;
- Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks;
- Ensuring that when personal information is stored on removable storage media such as external drives, that these are kept locked away securely when not being used;

- Ensuring that when personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, close to the printer;

- Ensuring that when personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer;

- Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email;

- Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant manager or the information officer to delete or dispose of the personal information in the appropriate manner;

- Undergoing POPIA awareness training from time to time.

Where an employee, or a person acting on behalf of the Company, becomes aware or suspicious of any security breach such as the unauthorised access, interference, destruction or the unsanctioned disclosure of personal information, they must immediately report this event or suspicion to the Information Officer or the Deputy Information Officer.

9. POPI AUDIT

The Company's Information Officer will schedule periodic POPI Audits.

The purpose of POPI audit is to:

- Identify the processes used to collect, record, store, disseminate and destroy personal information;

- Determine the flow of personal information throughout the Company. For instance, the Company's various business units, divisions, branches and other associated Companies;

- Redefine the purpose for gathering and processing personal information;

- Ensure that the processing parameters are still adequately limited;

- Ensure that new data subjects are made aware of the processing of their personal information;

- Re-establish the rationale for any further processing where information is received via a third party;

- Verify the quality and security of personal information;
- Monitor the extent of compliance with POPIA and this policy;
- Monitor the effectiveness of internal controls established to manage the Company's POPI related compliance risk.

In performing the POPI Audit, Information Officers will liaise with the managers in order to identify areas within in the Company's operation that are most vulnerable or susceptible to the unlawful processing of personal information.

Information Officers will be permitted direct access to and have demonstrable support from line managers and the Company's governing body in performing their duties.

10. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

Data subjects have the right to:

- Request what personal information the Company holds about them and why;
- Request access to their personal information;
- Be informed how to keep their personal information up to date.

Access to information requests can be made by email, addressed to the *Information Officer*. The Information Officer will provide the data subject with a "Personal Information Request Form".

Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All request will be processed and considered against the Company's PAIA Policy.

The Information officer will process all requests within a reasonable time.

11. POPI COMPLAINTS PROCEDURE

Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. The Company takes all complaints very seriously and will address all POPI related complaints in accordance with the following procedure:

- POPI complaints must be submitted to the Company in writing. Where so required, the Information Officer will provide the data subject with a "POPI Complaint Form". This form may also be found as "Annexure B" on page 23 of this Policy;
- Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 1 working day;

- The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days;

- The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA;

- The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on the Company's data subjects;

- Where the Information Officer has reason to believe that the personal information of data subjects as been accessed or acquired by an unauthorised person, the Information Officer will consult the Company's governing body whereafter the affected data subjects and the Information Regulator will be informed of this breach;

- The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to the Company's governing body within 7 working days of receipt of the complaint. In all instances, the Company will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines;

- The Information Officer's response to the data subject may comprise any of the following:

    - A suggested remedy for the complaint;
    - A dismissal of the complaint and the reasons as to why it was dismissed;
    - An apology (if applicable) and any disciplinary action that has been taken against any employees involved.

- Where the data subject is not satisfied with the information Officer's suggested remedies, the data subject has the right to complain to the Information regulator;

- The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrence giving rise to POPI related complaints.

12. DISCIPLINARY ACTION

Where a POPI complaint or a POPI infringement investigation has been finalised, the Company may recommend any appropriate administrative, legal and/or disciplinary action to be taken against the employee reasonably suspected of being implicated in any non-compliant activity outlined within the policy.

In the case of ignorance or minor negligence, the Company will undertake to provide further awareness training to the employee.

Any gross negligence or the wilful mismanaged of personal information, will be considered a serious form of misconducted for which the Company may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

Examples of immediate actions that may be taken subsequent to an investigation include:

- A recommendation to commence with disciplinary action;
- A referral to appropriate law enforcement agencies for criminal investigation;
- Recovery of funds and assets in order to limit any prejudice or damage caused.

Annexure A: PERSONAL INFORMATION REQUEST FORM

Please submit the completed form to the Information Officer:	
Name	
Contact Number	
Email Address	

Please be aware that we may require you to provide proof of identification prior to processing your request.
There may also be a reasonable charge for providing copies of the information requested.

Particulars of Data Subject:	
Name & Surname	
Identity Number	
Postal Address	
Contact Number	
Email Address	

B. Request:	
I request the Company to:	
Inform me whether it holds any of my personal information	
Provide me with a record or description of my personal information	
Correct or update my personal information	
Destroy or delete record(s) of my personal information	

C. Instructions:

D. Signature Page:
Signature: Date:

Annexure B: POPI COMPLAINT FORM

We are committed to safeguarding your privacy and the confidentiality of your personal information and are bound by the Protection of Personal Information Act.

Please submit the complaint form to the Information Officer:	
Name	
Contact Number	
Email Address	

Where we are unable to resolve your complaint, to your satisfaction you have the right to complain to the Information Regulator.

The Information Regulator:
Physical address: JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2017
Email: inforeg@justice.gov.za
Website: https://www.justice.gov.za/inforeg/index.html

Particulars of Complainant:	
Name & Surname	
Identity Number	
Postal Address	
Contact Number	
Email Address	

Details of Complaint:

Desired Outcome:

D. Signature Page:
Signature: Date:

Annexure C: POPI NOTICE AND CONSENT FORM

We understand that your personal information is important to you and that you may be apprehensive about disclosing it. Your privacy is just as important to us and we are committed to safeguarding and processing your information in a lawful manner. We also want to make sure that you understand how and for what purpose your information is collected. If for any reason you think that your information is not processed in a correct manner, or that your information is being used for a purpose other than that for what it was originally intended, you can contact our Information Officer.

You can request access to the information we hold about you at any time and if you think that we have outdated information, please request us to update or correct it.

Our Information Officer's Contact Details:	
Name	Marike Smith
Contact Number	+27 (0) 21 882 8571, Ext 320
Email Address	marike@finleys.co.za

Purpose for Processing your Information

We collect, hold, use and disclose your personal information mainly to provide you with the access to the services and products that we provide. We will only process your information for a purpose you have agreed to contractually or would reasonably expect, including:

- Providing you with advice, products and services that suit your needs as requested;
- To verify your identity and to conduct credit reference searches;
- To issue, administer and manage your insurance policies;
- To process insurance claims and to take recovery action;
- To notify you of new products or developments that may be of interest to you;
- To confirm, verify and update your details;
- To comply with any legal and regulatory requirements.

Some of your information that we hold may include, your first and last name, email address, a home, postal or other physical address, other contact information, your title, birth date, gender, occupation, qualifications, past employment, residency status, your investments, assets, liabilities, insurance, income, expenditure, family history, medical information and your banking details.

Consent to Disclose and Share your Information

We may need to share your information to provide you with the services, products or advice you request. In these scenarios, we will take all precautions to ensure that the third party will treat your information with the same level of protection we do. Your information may be hosted on servers managed by third-party service providers, which may be located outside of South Africa.

I hereby authorise and consent to the organisation sharing my personal information with the following persons:
Finleys Trust Services (Pty) Ltd, **Finleys Labour (Pty) Ltd, Finleys Recruitment (Pty) Ltd, Finleys SSW (Pty) Ltd**, as well as the following service providers and government Agencies: **Metrofile (Pty) Ltd** (Who provide Finleys with services relating to the Storage of Client Data); **Othos (Pty) Ltd** (Who provide Finleys with services relating to Telephone Recordings); **Cyberlogic (Pty) Ltd** (Who provide Finleys with services relating to IT Structure, Data, Cloud Servers, Data Protection Software, Internet Protection); **The South African Revenue Service (SARS);** **The Companies and Intellectual Properties Commission (CIPC);** **The Workers Compensation Assistance (WCA);**

As well as any other entity or person who is necessarily involved and required for the fulfilment of the purpose for which the data was provided.
Name & Signature Signature   Date