PURE LEGACY FOUNDATION

PROTECTION OF PERSONAL INFORMATION POLICY

TABLE OF CONTENTS

1. Introduction

The right to privacy is an integral human right recognised 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 by providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner.

Through the provision of quality goods and services, the organisation is necessarily involved in the collection, use and disclosure of certain aspects of the 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 organisation 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 (such as a company), including, but not limited to information concerning:

- race, gender, 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 contents 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 organisation with products or other goods.

2.3. Responsible Party

The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case, the organisation 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. For example, a third-party service provider that has contracted with the organisation to shred documents containing personal information. When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.

2.5. Information Officer

The Information Officer is responsible for ensuring the organisation's compliance with POPIA. Where no Information Officer is appointed, the head of the organisation 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 can also be appointed to assist the Information Officer.

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, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- dissemination by means of transmission, distribution or making available in any other form; or
- merging, linking, as well as any restriction, degradation, erasure or destruction of information.

2.7. Record

This 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, plan, 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

This 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

This means any identifier that is assigned to a data subject and is used by a 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

This 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

This 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

This 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

It 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 organisation from the compliance risks associated with the protection of personal information which, includes:

- Breaches of confidentiality. For instance, the organisation could suffer loss in revenue and public confidence, where it is found that the personal information of data subjects 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 organisation uses information relating to them.

- Reputational damage. For instance, the organisation could suffer a decline in public confidence following an adverse event, such as personal information held by the organisation being stolen and used by a third party.

This policy demonstrates the organisation'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 an organisational 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 organisational practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate operational needs of the organisation.

- By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer, and where necessary, Deputy Information Officers in order to protect the interests of the organisation 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 applies to:

- The organisation's governing body;
- All departments of the organisation;
- All employees and volunteers;
- All contractors, suppliers and other persons acting on behalf of the organisation.

The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as the organisation's PAIA Policy as required by the Promotion of Access to Information Act (Act No 2 of 2000).

The legal duty to comply with POPIA's provisions is activated in any situation, and can be summarised as follows:

- processing of personal information;
- entered into a record;

- by or for a responsible person;
- who is domiciled in South Africa.

POPIA does not apply in situations where the processing of personal information:

- Is concluded in the course of purely personal or household activities, or
- Where the personal information has been de-identified.

5. Rights of Data Subjects

Where appropriate, the organisation will ensure that its clients and customers are made aware of the rights conferred upon them as data subjects. The organisation will ensure that it gives effect to the following seven rights.

5.1 The Right to Access Personal Information

The organisation recognises that a data subject has the right to establish whether the organisation holds personal information related to them, including the right to request access to that personal information. Information regarding requesting personal information may be found in Pure Legacy Foundation's Promotion of Access to Information Act (PAIA) Manual at Annexure A.

5.2 The Right to have Personal Information Corrected or Deleted

The data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where the organisation is no longer authorised to retain the personal information.

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 his, her or its personal information.

In such circumstances, the organisation will give due consideration to the request and the requirements of POPIA. The organisation 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 his, her or its 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 his, her or its personal information.

An example of a “POPI Complaint Form” can be found under Annexure B.

5.6 The Right to be Informed

The data subject has the right to be notified that his, her or its personal information is being collected by the organisation. The data subject also has the right to be notified in any situation where the organisation 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 organisation 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 damage the organisation’s reputation or expose the organisation to a civil claim for damages. The protection of personal information is therefore everybody’s responsibility.

The organisation will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, the organisation 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 outlined in this policy.

6.2 Processing Limitation

The organisation 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 organisation will inform the data subject of the reasons for collecting his, her or its personal information and obtain written consent prior to processing personal information.

The organisation will under no circumstances distribute or share personal information with separate legal entities, associated organisations or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected, without the written consent of the data subject.

Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other aspects of the organisation'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.

6.3 Purpose Specification

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

The organisation will process personal information only for specific, explicitly defined and legitimate reasons. The organisation will inform data subjects of these reasons prior to collecting or recording the 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 organisation 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 organisation will first obtain additional consent from the data subject.

6.5 Information Quality

The organisation will take reasonable steps to ensure that all personal information collected is complete, accurate, justified and necessary.

Where personal information is collected or received from third parties, the organisation will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources.

6.6 Open Communication

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

The organisation will ensure that it establishes and maintains a “contact us” facility, for instance via its website, email or through a helpdesk (reception), for data subjects who want to:

- Enquire whether the organisation holds related personal information, or
- Request access to related personal information, or
- Request the organisation to update or correct related personal information, or
- Make a complaint concerning the processing of personal information.

6.7 Security Safeguards

The organisation will manage the security of its filing 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.

The organisation uses Off-site Windows server with VPN access control as the primary e-filing storage systems. Both platforms have security measures in place to ensure integrity of data storage. All personal information is processed, catalogued, managed and stored on Off-site Windows server with VPN access control. Access to personal information is limited.

Any data collected via paper is processed and entered into the relevant platform for data management, and the paper record is destroyed, unless needed for legislative reasons (e.g. SARS).

Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, the greater the security required. This is particularly important regarding information related to children and vulnerable people.

The organisation will regularly review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the organisation’s IT network. This will be done in consultation with the IT service provided, Shinray Digital (Pty) Ltd.

The organisation will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.

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 organisation is responsible.

All existing employees will be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses.

The organisation's operators and third-party service providers will be required to enter into service-level agreements with the organisation where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

An example of "Employee Consent and Confidentiality Clause" for inclusion in the organisation's employment contracts can be found under Annexure D.

An example of an "SLA Confidentiality Clause" for inclusion in the organisation's service level agreements can be found under Annexure E.

6.8 Data Subject Participation

A data subject may request the correction or deletion of his, her or its personal information held by the organisation. This may be done via forms on the PAIA manual available at the office or on the organisation's website.

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

7. Information Officers

The organisation will appoint an Information Officer and where necessary, a Deputy Information Officer to assist the Information Officer. The Organisation's Information Officer is Rene Bosman, director of Pure Legacy Foundation. The Organisation's Deputy Information Officer is the Charmaine Erasmus, Foundation Manager.

The organisation's Information Officers are responsible for ensuring compliance with POPIA.

Consideration will be given on an annual basis to the reappointment or replacement of the Information Officer and the reappointment or replacement of any Deputy Information Officers.

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

Registration of the organisation's Information officers is completed online at https://www.justice.gov.za/inforeg/portal.html

8. Specific Duties and Responsibilities

8.1 Governing Body

The organisation's governing body cannot delegate its accountability and is ultimately answerable for ensuring that the organisation meets its legal obligations 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 must appoint and review and reappoint the Information Officers.

The governing body is responsible for ensuring that all persons responsible for the processing of personal information on behalf of the organisation:

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

The governing body must ensure data subjects who want to make enquires about their personal information are made aware of the procedure that needs to be followed should they wish to do so.

The governing body must ensure that the Information Officer carried out an annual periodic POPI Audit in order to accurately assess and review the ways in which the organisation collects, holds, uses, shares, discloses, destroys and processes personal information.

8.2 Information Officer

The organisation's Information Officer is responsible for:

- Taking steps to ensure the organisation's reasonable compliance with the provision of POPIA.

- Keeping the governing body updated about the organisation'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 organisation's personal information processing procedures. This will include reviewing the organisation's information protection procedures and related policies.

- Ensuring that POPI Audits are scheduled and conducted on a regular basis.

- Ensuring that the organisation makes it convenient for data subjects who want to update their personal information or submit POPI-related complaints to the organisation. For instance, maintaining a "contact us" facility on the organisation's website and publishing the PAIA manual.

- Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the organisation. This will include overseeing the amendment of the organisation'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 organisation are fully aware of the risks associated with the processing of personal information and that they remain informed about the organisation'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 organisation.

- Addressing employees' POPIA-related questions.

- Addressing all POPIA-related requests and complaints made by the organisation'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 or her duties.

8.3 Information Technology Management

The organisation's IT management is outsourced to a third party, and is overseen by the CEO, Raymond Nunes. With regards to IT, the consultant, Shinray Digital (Pty) Ltd is thus responsible for:

- Ensuring that the organisation's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.

- Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to 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 back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious hacking attempts.

- Ensuring that personal information being transferred electronically is transferred securely.

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

- Performing regular IT audits to ensure that the security of the organisation'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 any unauthorised persons.

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

8.4 Communication Manager / Foundation Manager

The organisation's Communication Manager / Foundation Manager is responsible for:

- Approving and maintaining the protection of personal information statements and disclaimers that are displayed on the organisation's website, including those attached to communications such as emails and electronic newsletters.

- Ensuring that public communication is compliant with the POPIA, especially regarding the use of names and pictures of data subjects.

- Addressing any personal information protection queries from journalists or media outlets such as newspapers.

- Where necessary, working with persons acting on behalf of the organisation to ensure that any outsourced marketing initiatives comply with POPIA.

8.5 Employees and other Persons acting on behalf of the Organisation

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

Employees and other persons acting on behalf of the organisation may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the organisation 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 organisation must request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

Employees and other persons acting on behalf of the organisation 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 the legitimate interests of the organisation.

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

- Clearly understands why and for what purpose his, her or its personal information is being collected; and

- Has granted the organisation with explicit written or verbally recorded consent to process his, her or its personal information.

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 and other persons acting on behalf of the organisation will under no circumstances:

- Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties.

- Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer.

- Transfer personal information outside of South Africa without the express permission from the Information Officer.

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

- Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.

- Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing 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 organisation, 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 is password protected and never left unattended. Passwords must be changed regularly and 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 where personal information is stored on removable storage media such as external drives, CDs or DVDs that these are kept locked away securely when not being used.

- Ensuring that where 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, in a locked drawer of a filing cabinet.

- Ensuring that where 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. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.

- 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 line manager or the

Information Officer to delete or dispose of the personal information in the appropriate manner.

- Undergoing POPI Awareness training from time to time.

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

Any incident must be recorded in the POPI Incident Register found in Annexure F.

The Data Subject must be informed, and if necessary and of a serious enough nature, the Information regulator must be notified.

9. POPI Audit

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

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

In performing the POPI Audit, Information Officers will liaise with line managers in order to identify areas within the organisation'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 organisation'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 organisation holds about them and why.
- Request access to their personal information.
- Be informed on 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" in the PAIA Manual.

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 requests will be processed and considered against the organisation's PAIA as outlined in the PAIA manual.

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 organisation 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 organisation in writing. Where so required, the Information Officer will provide the data subject with a "POPI Complaint Form", Annexure B.

- 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 organisation's data subjects.

- Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with the organisation's governing body where after 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 organisation's governing body within 7 working days of receipt of the complaint. In all instances, the organisation 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 occurrences giving rise to POPI related complaints.

12. Disciplinary Action

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

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

Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which the organisation 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 damages caused.

13. Data Retention Requirements and Destruction of Documents

Documents may be destroyed after the termination of the retention period mandated by law, or as determined by the Organisation from time to time.

Each department is responsible for attending to the destruction of its documents and electronic records, which must be done on a regular basis. Files must be checked in order to make sure that they may be destroyed and also to ascertain if there are important original documents in the file. Original documents must be returned to the holder thereof, failing which, they should be retained by the Company pending such return.

Deletion of electronic records must be done in consultation with the Information Officers and IT contractor to ensure that deleted information is incapable of being reconstructed and/or recovered.

Statutory requirements regarding data retention can be found in Annexure G.