PROTECTION OF PERSONAL INFORMATION POLICY

Implemented for:

Company Name	Olympus Mobile (Pty) Ltd
Company	**2004/012954/07**
Document Author Created	Access Bank South Africa Limited
Date Created	2021-07-01
Date Reviewed	2021-07-01
Version	1.0

(Hereinafter referred to by name or as “the company”)

TABLE OF CONTENTS

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").*** It 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 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 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 company is committed to the effective management of personal information and in accordance with POPIA's provisions. The Policy sets out the way the company deals with personal information collected, how it is stored and the purpose for which said information is used. This policy is made available by request from the head office of the company.

2. DEFINITIONS

1.1 **"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, sex, pregnancy, marital status, national or ethnic origin, color, 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.

1.2 **"Data Subject"** 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.

1.3 **"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. The company is the responsible party.

1.4 **"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 company to share documents containing personal information. When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.

1.5 **"Information Officer"** is responsible for ensuring the company's compliance with POPIA. Where no Information Officer is appointed, the Chief Executive Officer 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 can also be appointed to assist the Information Officer.

1.6 **"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, organizing, 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.

1.7 **"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, 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.

1.8 **"Filing System"** means any structured set of personal information, whether centralized, decentralized or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

1.9 **"Unique Identifier"** 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.

1.10 **"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.

1.11 **"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.

1.12 **"PAIA"** refers to The Promotion of Access to Information Act, 2 of 2000.

1.13 **"Consent"** means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

1.14 **"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.

1.15 **"Biometrics"** means a technique of personal identification that is based on physical, physiological, or behavioral characterization including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

3. POLICY OBJECTIVES

The objective of this policy is to protect the company's information assets from threats, whether internal or external, deliberate or accidental, to ensure business continuation, minimize business damage and maximize business opportunities. This policy establishes a general standard on the appropriate protection

of personal information within the company and provides principles regarding the right of individuals to privacy and to reasonable safeguards of their personal information.

4. POLICY APPLICATION

This policy and its guiding principles apply to the company's governing body, administrative staff members, all business units, branches and divisions within the company as well as all contractors, suppliers and persons acting on behalf of the company in the rendering of any services. The policy should be read together with the company's PAIA Policy as required by the ***Promotion of Access to Information Act, 2 of 2000.*** The legal duty to comply with POPIA's provisions is initiated in any situation where there is - ***a 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 during purely personal or household activities,
- or where the personal information has been de-identified.

5. RIGHTS OF DATA SUBJECTS

The company will ensure that its clients and customers are made aware of the rights conferred upon them as data subjects. The company will ensure that it gives effect to the following legal rights:

THE RIGHT TO ACCESS PERSONAL INFORMATION

The company recognizes 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.

The **"Personal Information Request Form"** is attached hereto and marked as **Appendix "A"**

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 company is no longer authorized to retain the personal information.

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 situations, 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.

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.

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.

The **"POPI Complaint Form"** is attached hereto and marked as **Appendix "B"**

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 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 unauthorized person.

6. THE CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

The company is committed to processing personal information lawfully and to comply with the following conditions;

CONDITION 1: ACCOUNTABILITY (section 8)

The company maintains an approach of transparency of operational procedures that controls the collection and processing of personal information. The company will ensure that the provisions of POPIA and the principles outlined herein are complied with. The company will also 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. Failing to comply with POPIA could potentially damage the company's reputation or expose the company to a civil claim for damages. The protection of personal information is everyone in the company's responsibility.

CONDITION 2 & 3: PROCESSING LIMITATION (sections 9 – 12) & FURTHER PROCESSING LIMITATION (section 15)

The company undertakes to collect personal information in a legal and reasonable way and to process the personal information obtained from data subjects only for the purpose for which it was obtained in the first place. Processing of personal information obtained will not be undertaken in an insensitive or wrongful way that can intrude on privacy. Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose and additional consent is obtained.

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 his, her or its personal information and obtain written consent prior to processing personal information. Alternatively, where services or transactions are concluded over the telephone or electronically, the company will maintain a voice recording of the stated purpose for collecting the personal information followed by the data subject's subsequent consent. 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.

A **"POPI Notice and Consent Form"** is attached hereto and marked as **Appendix "C"**

CONDITION 4: ***PURPOSE SPECIFICATION (sections 13 – 14)***

Personal information will only be collected for a specific, explicitly defined and lawful purpose and related to the business of the company. The company is compelled to keep effective record of personal information and undertakes not to retain information for a period longer than prescribed by legislation and as dictated by business practice. All personal information will be disposed at the end of the retention period in such a way that it cannot be reconstructed. The company will inform data subjects of these reasons prior to collecting or recording the data subject's personal information.

CONDITION 5: ***INFORMATION QUALITY (section 16)***

The company will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading. The company 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, where the personal information is collected or received from third parties.

CONDITION 6: ***OPENNESS (sections 17 - 18):***

The company 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 company will ensure that it establishes and maintains a "contact us" facility, for instance via its website or through an electronic helpdesk, for data subjects who want to:

- ***Enquire whether the company holds related personal information, or***
- ***Request 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.***

CONDITION 7: ***SECURITY SAFEGUARDS (sections 19 – 22)***

The company will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented to minimize the risk of loss, unauthorized access, disclosure, interference, modification or destruction. Security measures 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 authorized 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 unauthorized 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 clauses. The company's operators and third-party service providers will be required to enter into service level agreements with the company where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement. Ensure that all employment contracts are reviewed and contains an employee consent and confidentiality clause. All service level agreements with third party suppliers to contain a confidentiality clause.

***CONDITION 8:* DATA SUBJECT PARTICIPATION (sections 23 – 25)**

The company will ensure that it provides a capability for data subjects who want to request the correction of or deletion of their personal information. The company will provide an option to data subjects to "unsubscribe" from any of its electronic newsletters or marketing material. A data subject may request the correction or deletion of his, her or its personal information held by the company.

7. THE USAGE OF PERSONAL INFORMATION

The Personal Information of each data subject will only be used for the purpose for which it was collected and as agreed.

This may include, but are not limited to:

- *Providing products or services to clients and to carry out the transactions requested;*
- *Conducting reference searches and/or- verification;*
- *Confirming, verifying and updating client details;*
- *For the detection and prevention of fraud, crime, money laundering or other malpractices;*
- *For audit and record keeping purposes;*
- *In connection with legal proceedings;*
- *To maintain and constantly improve the relationship;*
- *Providing communication in respect of the business of the company and any related regulatory matter/s that may affect the client directly and or indirectly; and*
- *In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.*

According to section 10 of POPIA, personal information may only be processed if certain conditions, listed below, are met along with supporting information for the processing of Personal Information:

I. The client's consents to the processing: - consent is obtained from clients during the introductory stage of the relationship;
II. Processing complies with an obligation imposed by law on the company;
III. Processing is necessary for pursuing the legitimate interests of the company or of a third party to whom information is supplied.

8. DISCLOSURE AND SAFEGUARDING OF PERSONAL INFORMATION

The company may disclose a client's personal information to any of the company's group of companies or subsidiaries, joint venture companies and or approved product or third-party service providers whose services or products clients elect to use. The company has agreements in place to ensure that compliance with confidentiality and privacy conditions are met. The company may also share client personal information with, and obtain information about clients from third parties for the reasons already discussed herein above. The company may also disclose a client's information where it has a duty or a right to disclose in terms of applicable legislation, the law, or where it may be deemed necessary in order to protect the rights of the company. It is a requirement in terms of the POPIA to adequately protect personal information. The company will continuously review its security controls and processes to ensure that personal information is secure.

The following procedures are in place in order to safeguard the personal information of both Employees and Clients of the company:

- ✓ Each new employee will be required to sign an Employment Contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPIA;
- ✓ All existing employees, will be required to sign an Addendum to their Employment Contracts containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPIA;
- ✓ Any archived client information is stored at the offices of the company and is also governed by the POPIA, access to these documents is limited to authorized staff members only, the Information Officer has a list of names of these staff members and periodic control checks are performed to ensure compliance.

- ✓ Product suppliers and all other third-party service providers will be required to sign a Service Level Agreement guaranteeing their commitment to the Protection of Personal Information; this is however an ongoing process that will be evaluated as needed.
- ✓ All electronic files or data are backed up.
- ✓ Consent to process client information is obtained from each individual client (or a person who has been given authorization from the client to provide the client's personal information) during the introductory stage of the relationship.

9. INFORMATION OFFICERS

The company's Information Officer is responsible for ensuring compliance with POPIA. The company will appoint a POPIA Information Officer and if needed, a Deputy Information Officer to assist the Information Officer in the execution of his/her duties. There are no legal requirements under POPIA for a company to appoint an Information Officer. Appointing an Information Officer is however, considered to be a good business practice, particularly within larger companies. Where no Information Officer is appointed, the Chief Executive Officer of the company will assume the role of the Information Officer. On an annual basis, the company will review the appointment, re-appointment or replacement of the Information Officer and the reappointment or replacement of any Deputy Information Officers.

Once appointed, the FSP will register the Information Officer with the South African Information Regulator established under POPIA prior to performing his or her duties. An **"Information Officer Appointment Letter"** are attached hereto and marked as **Appendix "D".**

10. ROLES AND RESPONSIBILITIES OF KEY ROLEPLAYERS WITHIN THE COMPANY

GOVERNING BODY

The company's governing body cannot delegate its accountability and is ultimately responsible for ensuring that the company meets its legal obligations in terms of POPIA. The governing body may 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: (a) are appropriately trained and supervised to do so, (b) understand that they are contractually obligated to protect the personal information they come into contact with, and (c) are aware that a willful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.
- ✓ 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 scheduling of a periodic POPI Audit to accurately assess and review the ways in which the FSP collects, holds, uses, shares, discloses, destroys and processes personal information.

INFORMATION OFFICER

The company's Information Officer is responsible for;

- ✓ Taking steps to ensure the company's reasonable compliance with the provision of POPIA.
- ✓ Keeping the governing body updated about the company's information protection responsibilities under POPIA.

- ✓ 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 or submit changes to their personal information.
- ✓ Managing all POPI related complaints to the company.
- ✓ Ensuring the maintenance of 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 the 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.
- ✓ Organizing 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 act as the main contact person to 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 related matters. The Deputy Information Officer will assist the Information Officer in performing his or her duties.

IT MANAGER

The Company's IT Manager is responsible for:

Ensuring that the company'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 unauthorized access, accidental deletion.
- ✓ 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 protection 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 any unauthorized 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 company's behalf.

EMPLOYEES AND OTHER PERSONS ACTING ON BEHALF OF THE COMPANY

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

- ✓ Keeping all personal information 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 company, with the sending or sharing of personal information to or with authorized 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 must be changed regularly and may not be shared with unauthorized 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 medias 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 unauthorized 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 unauthorized 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. Where a data subject's information is found to be out of date, authorization 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, authorization 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 company, becomes aware or suspicious of any security breach such as the unauthorized 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.

11. **POPIA COMPLIANCE AUDITS**

The company's Information Officer will schedule periodic POPIA compliance Audits.

<u>The purpose of a POPIA compliance audit is to;</u>

- ✓ Identify the processes used to collect, record, store, disseminate and destroy personal information.
- ✓ Determine the flow of personal information throughout the company.
- ✓ 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 extend of compliance with POPIA and this policy.
- ✓ Monitor the effectiveness of internal controls established to manage the company's POPI related compliance risk.

The Information Officers will liaise with line 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.

12. 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 requests made for personal information will be processed and considered against the company's PAIA Policy. The Information Officer will process all requests within a reasonable time.

13. RETENTION PERIODS OF CERTAIN DOCUMENT TYPES IN TERMS OF DIFFERENT LEGISLATION

Documents need to be retained in order to prove the existence of facts and to exercise rights the company may have. It is also needed to exercise effective control over the retention of documents and electronic transactions

- as prescribed by legislation; and
- as dictated by business practice.

Documents are also necessary for defending legal action, for establishing what was said or done in relation to business of the company and to minimize reputational risks, to ensure that the company's interests are protected and that the clients' rights to privacy and confidentiality are not breached.

COMPANIES ACT, NO 71 OF 2008

With regard to the Companies Act, no 71 of 2008 and the Companies Amendment Act no 3 of 2011, hardcopies of the documents mentioned below must be retained for 7 years:

- Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Act;
- Notice and minutes of all shareholders meeting, including resolutions adopted and documents made available to holders of securities;
- Copies of reports presented at the annual general meeting of the company;
- Copies of annual financial statements required by the Act;
- Copies of accounting records as required by the Act;
- Record of directors and past directors, after the director has retired from the company;
- Written communication to holders of securities and
- Minutes and resolutions of directors' meetings, audit committee and directors' committees.
- Copies of the documents mentioned below must be retained indefinitely:
- Registration certificate;
- Memorandum of Incorporation and alterations and amendments;
- Rules;
- Securities register and uncertified securities register;
- Register of company secretary and auditors and
- Regulated companies (companies to which chapter 5, part B, C and
- Takeover Regulations apply) – Register of disclosure of person who holds beneficial interest equal to or in excess of 5% of the securities of that class issued.

CONSUMER PROTECTION ACT, (CPA) NO 68 OF 2008

The Consumer Protection Act seeks to promote a fair, accessible and sustainable marketplace and therefore requires a retention period of 3 years for information provided to a consumer by an intermediary such as:

- Full names, physical address, postal address and contact details;
- ID number and registration number;
- Contact details of public officer in case of a juristic person;
- Service rendered;
- Intermediary fee;
- Cost to be recovered from the consumer;
- Frequency of accounting to the consumer;
- Amounts, sums, values, charges, fees, remuneration specified in monetary terms;
- Disclosure in writing of a conflict of interest by the intermediary in relevance to goods or service to be provided;
- Record of advice furnished to the consumer reflecting the basis on which the advice was given;
- Written instruction sent by the intermediary to the consumer;
- Conducting a promotional competition refer to Section 36(11)(b) and
- Regulation 11 of Promotional Competitions;
- Documents Section 45 and Regulation 31 for Auctions.

FINANCIAL INTELLIGENCE CENTRE ACT (FICA) NO 38 OF 2001

Section 22 and 23 of the Act require a retention period of 5 years for the documents and records of the activities mentioned below:

- Whenever an accountable transaction is concluded with a client, the institution must keep record of the identity of the client;
- If the client is acting on behalf of another person, the identity of the person on whose behalf the client is acting and the client's authority to act on behalf of that other person;
- If another person is acting on behalf of the client, the identity of that person and that other person's authority to act on behalf of the client;
- The manner in which the identity of the persons referred to above was established;
- The nature of that business relationship or transaction;
- In the case of a transaction, the amount involved and the parties to that transaction;
- All accounts that are involved in the transactions concluded by that accountable institution in the course of that business relationship and that single transaction;
- The name of the person who obtained the identity of the person transacting on behalf of the accountable institution;
- Any document or copy of a document obtained by the accountable institution.

These documents may also be kept in electronic format.

EMPLOYMENT EQUITY ACT, NO 55 OF 1998

Section 26 and the General Administrative Regulations, 2009, Regulation 3(2) requires a retention period of 3 years for the documents mentioned below:

- Records in respect of the company's workforce, employment equity plan and other records relevant to compliance with the Act;

Section 21 and Regulations 4(10) and (11) require a retention period of 3 years for the report which is sent to the Director General as indicated in the Act.

LABOUR RELATIONS ACT, NO 66 OF 1995

Sections 53(4), 98(4) and 99 require a retention period of 3 years for the documents mentioned below:

- The Bargaining Council must retain books of account, supporting vouchers, income and expenditure statements, balance sheets, auditor's reports and minutes of the meetings;
- Registered Trade Unions and registered employer's organizations must retain books of account, supporting vouchers, records of subscriptions or levies paid by its members, income and expenditure statements, balance sheets, auditor's reports and minutes of the meetings;
- Registered Trade Unions and employer's organizations must retain the ballot papers;
- Records to be retained by the employer are the collective agreements and arbitration awards.

Sections 99, 205(3), Schedule 8 of Section 5 and Schedule 3 of Section 8(a) require an indefinite retention period for the documents mentioned below:

- Registered Trade Unions and registered employer's organizations must retain a list of its members;
- An employer must retain prescribed details of any strike, lock-out or protest action involving its employees;
- Records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions;
- The Commission must retain books of accounts, records of income and expenditure, assets and liabilities.

UNEMPLOYMENT INSURANCE ACT, NO 63 OF 2002

The Unemployment Insurance Act, applies to all employees and employers except:

- Workers working less than 24 hours per month;
- Learners;
- Public servants;
- Foreigners working on a contract basis;
- Workers who get a monthly State (old age) pension;
- Workers who only earn commission.

Section 56(2)(c) requires a retention period of 5 years, from the date of submission, for the

documents mentioned below:

- Employers must retain personal records of each of their current employees in terms of their names, identification number, monthly remuneration and address where the employee is employed.

TAX ADMINISTRATION ACT, NO 28 OF 2011

Section 29 of the Tax Administration Act, states that records of documents must be
retained to:

- Enable a person to observe the requirements of the Act;
- Are specifically required under a Tax Act by the Commissioner by the public notice;
- Will enable SARS to be satisfied that the person has observed these requirements.

Section 29(3)(a) requires a retention period of 5 years, from the date of submission for taxpayers that have submitted a return and an indefinite retention period, until the return is submitted, then a 5-year period applies for taxpayers who were meant to submit a return, but have not.

Section 29(3)(b) requires a retention period of 5 years from the end of the relevant tax period for taxpayers who were not required to submit a return, but had capital gains/losses or engaged in any other activity that is subject to tax or would be subject to tax but for the application of a threshold or exemption.

Section 32(a) and (b) require a retention period of 5 years but records must be retained until the audit is concluded or the assessment or decision becomes final, for documents indicating that a person has been notified or is aware that the records are subject to an audit or investigation and the person who has lodged an objection or appeal against an assessment or decision under the TAA.

INCOME TAX ACT, NO 58 OF 1962

Schedule 4, paragraph 14(1)(a) - (d) of the Income Tax Act requires a retention period of 5 years from the date of submission for documents pertaining to each employee that the employer shall keep:

- Amount of remuneration paid or due by him to the employee;
- The amount of employee's tax deducted or withheld from the remuneration paid or due;
- The income tax reference number of that employee;
- Any further prescribed information;
- Employer Reconciliation return.

Schedule 6, paragraph 14(a)-(d) requires a retention period of 5 years from the date of submission or 5 years from the end of the relevant tax year, depending on the type of transaction for documents pertaining to:

- Amounts received by that registered micro business during a year of assessment;
- Dividends declared by that registered micro business during a year of assessment;
- Each asset as at the end of a year of assessment with cost price of more than R 10 000;
- Each liability as at the end of a year of assessment that exceeded R 10 000.

14. ELECTRONIC STORAGE

The internal procedure requires that electronic storage of information: important documents and information must be referred to and discussed with the IT department who will arrange for the indexing, storage and retrieval thereof. This will be done in conjunction with the departments concerned.

SCANNED DOCUMENTS

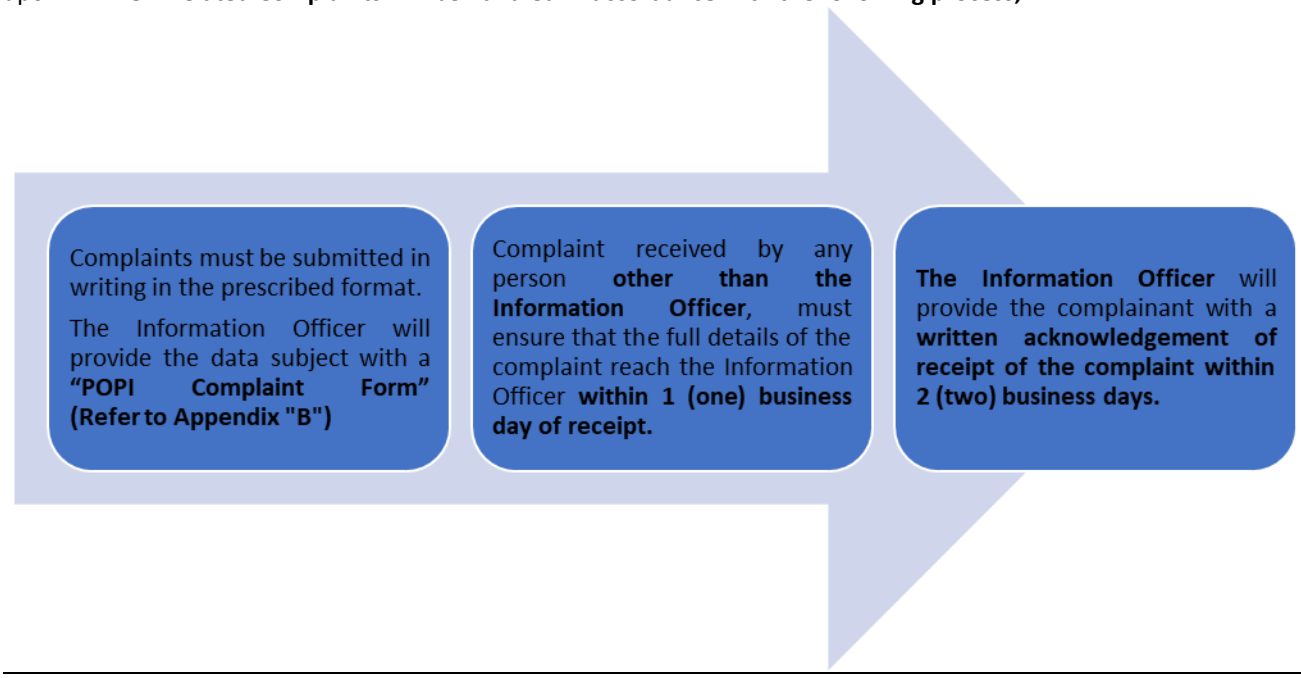
If documents are scanned, the hard copy must be retained for as long as the information is used or for 1 year after the date of scanning, with the exception of documents pertaining to personnel. Any document containing information on the written particulars of an employee, including: employee's name and occupation, time worked by each employee, remuneration and date of birth of an employee under the age of 18 years; must be retained for a period of 3 years after termination of employment.

SECTION 51 OF THE ELECTRONIC COMMUNICATIONS ACT (ECTA) NO 25 OF 2005

The ECTA requires that personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes or stores the information and a record of any third party to whom the information was disclosed must be retained for a period of 1 year or for as long as the information is used. It is also required that all personal information which has become obsolete must be destroyed.

15. POPI COMPLAINTS PROCEDURE

Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. **All POPI related Complaints will be handled in accordance with the following process;**



The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable, fair manner and in accordance with the principles outlined in POPIA.

1. The Information Officer should 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.

2. Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorized person, the Information Officer will consult with the company's governing body and thereafter the affected data subjects and the Information Regulator will be informed of this breach.

3. 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 (seven) 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 occurrences giving rise to POPI related complaints.

16. DISCIPLINARY ACTION

Where a POPI complaint or a POPI infringement investigation has been finalized, the company 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 company will undertake to provide further awareness training to the employee. Any gross negligence or the willful mismanagement of personal information, will be considered a serious form of misconduct 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.

Actions to be taken after 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.**

17. PENALTIES FOR NON-COMPLIANCE

There are essentially two legal penalties or consequences for serious breaches of the POPIA for the responsible party:

I. A fine of between R1 million and R10 million and or imprisonment or one to ten years in jail;
II. Paying compensation to data subjects for the damage they have suffered.

The other penalties include:

- *Reputation damage*
- *Losing customers (and employees)*
- *Failing to attract new customers*

18. AVAILABILITY AND REVISIONS

This policy is made available on the company's website and or by request from the Information Officer or Chief Executive Officer. This policy will continually be updated to comply with legislation, thereby ensuring that personal information will be secure.

APPENDIX "A" PERSONAL INFORMATION REQUEST FORM

PERSONAL INFORMATION REQUEST FORM

Please submit the completed form to the Information Officer

NAME & SURNAME:	
CONTACT NUMBER:	
E-MAIL ADDRESS:	

NOTE! 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.

A. PARTICULARS OF DATA SUBJECT

NAME & SURNAME	
IDENTITY NUMBER:	
POSTAL ADDRESS:	
CONTACT NUMBER:	
EMAIL ADDRESS:	

B. REQUEST

I request the FSP to: **(please tick the appropriate action)**

(a) Inform me whether it holds any of my personal information	
(b) Provide me with a record or description of my personal information	
(c) Correct or update my personal information	
(d) Destroy or delete a record of my personal information	

C. INSTRUCTIONS

D. SIGNATURE PAGE

Signature	
Date	____ / _____ / 20___

APPENDIX "B" POPI COMPLAINT FORM

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 your complaint to the Information Officer at:

NAME AND SURNAME:	
CONTACT NUMBER:	
EMAIL ADDRESS:	

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

THE INFORMATION REGULATOR: Ms Mmamoroke Mphelo
PHYSICAL ADDRESS: SALU Building, 316 Thabo Sehume Street, Pretoria
EMAIL ADDRESS: inforreg@justice.gov.za
WEBSITE: http://www.justice.gov.za/inforeg/index.html

A) PARTICULARS OF COMPLAINANT

NAME & SURNAME	
IDENTITY NUMBER:	
POSTAL ADDRESS:	
CONTACT NUMBER:	
EMAIL ADDRESS:	

B) DETAILS OF COMPLAINT

C) DESIRED OUTCOME

D) SIGNATURE PAGE

Signature	
Date	____ / _____ / 20___

APPENDIX "C" POPI NOTICE AND CONSENT FORM

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 we process your information. 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 AND SURNAME:	
CONTACT NUMBER:	
EMAIL ADDRESS:	

Purpose for Processing your Information

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

- Providing you with products and services that suit your needs as requested
- To verify your identity and to conduct reference searches
- 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 and your banking details.

Consent to Disclose and Share your Information.

We may need to share your information to provide advice, reports, analyses, products or services that you have requested.

Where we share your information, we will take all precautions to ensure that the third party will treat your information with the same level of protection as required by us. Your information may be hosted on servers managed by a third-party service provider, which may be located outside of South Africa.

I hereby authorize and consent to the company sharing my personal information with the following person/s:

_____

_____

SIGNATURE PAGE

NAME & SURNAME:	
SIGNATURE:	
Date	____ / _____ / 20___

APPENDIX "D" POPI INFORMATION OFFICER APPOINTMENT LETTER
***NOTE!* To be placed onto a Company Letterhead**

INFORMATION OFFICER APPOINTMENT LETTER

We, _____ **(insert company name with number)** hereinafter referred to as the "company" herewith and with immediate effect appoint _____ **(insert name and surname of appointment Information Officer)** as the Information Officer as required by the ***Protection of Personal Information Act, 4 of 2013.***

This appointment may at any time be withdrawn or amended in writing.

You are entrusted with the following responsibilities:

I. Taking steps to ensure the company's reasonable compliance with the provision of POPIA;
II. Keeping the governing body updated 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.
III. Continually analyzing privacy regulations and aligning them with the company's personal information processing procedures. This will include reviewing the company's information protection procedures and related policies.
IV. Ensuring that POPIA Audits are scheduled and conducted on a regular basis.
V. Ensuring that POPIA Audits referenced in IV above are properly recorded and should any breaches be found that remedial action is taken to rectify same.
VI. Ensuring that the company makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the company, to do so. For instance, maintaining a "contact us" facility on the company's website.
VII. Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the company. This will include overseeing the amendment of the company's employment contracts and other service level agreements.
VIII. Encouraging compliance with the conditions required for the lawful processing of personal information.
IX. 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.
X. Organizing and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the company.
XI. Addressing employees' POPIA related questions.
XII. Addressing all POPIA related requests and complaints made by the company's data subjects.
XIII. 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.

I HEREBY ACCEPT THE APPOINTMENT AS INFORMATION OFFICER

NAME & SURNAME:	
SIGNATURE:	
DATE OF APPOINTMENT:	____ / _____ / 20___