Applicable to Financial Services Provider acting as Category I and II Financial Services Provider in terms of the Financial Advisory and Intermediary Services Act
May 2023
Implemented for:

DSFPS (PTY) LTD
FSP: 52842
(Hereinafter referred to as "The Group")

DECLARATION OF IMPLEMENTATION AND COMPLIANCE

I, the undersigned, being the authorised and approved Managing Director of DSFPS, hereby declare as follows:

I have made myself aware of the contents of this document
I will ensure that the processes herein contained are implemented in our business
I will ensure that all staff in our business are trained on the aspects and importance of the protection of personal information as condensed in this document
I will ensure that this document is updated and reviewed on at least an annual basis.

EA (Renske) Lindeque

CONTENTS

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 ("POPI"). 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 financial services, our group is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, 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, our group is committed to the effective management of personal information and in accordance with POPI's provisions. This Policy sets out the way our group deals with personal information collected, how it is stored and the purpose for which said information is used.

DEFINITIONS:

"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, 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.

"Data Subject" refers to the natural or juristic person to whom personal information relates, such as an individual client or a company that supplies the GROUP with products or other services.

"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. Our GROUP is the responsible party in this context.

"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 GROUP 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.

"Information Officer" is responsible for ensuring the GROUP's compliance with POPI. Where no Information Officer is appointed, the Key Individual of the group 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 POPI prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.

"Processing" the act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes: the collection, receipt, recording, organising, collation, storage, updating or modification, retrieval, 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.

"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.

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

"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.

"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.

"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.

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

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

"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 donate any kind for any reason.

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

POLICY OBJECTIVES:

The objective of this policy is to protect our Group's information assets from threats, whether internal or external, deliberate, or accidental, to ensure business continuation, minimise business damage and maximise business opportunities.

This policy establishes a general standard on the appropriate protection of personal information within our group and provides principles regarding the right of individuals to privacy and to reasonable safeguards of their personal information.

POLICY APPLICATIONS:

This policy and its guiding principles apply to our group's senior management, Key Individuals, Representatives, administrative staff members, all business units, branches, and divisions within the group as well as all contractors, suppliers and persons acting on behalf of the group in the rendering of any services.

This policy should be read together with the group's PAIA Policy as required by the **Promotion of Access to Information Act, 2 of 2000**. The legal duty to comply with POPI'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.

POPI 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.

RIGHTS OF DATA SUBJECTS:

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

THE RIGHT TO ACCESS PERSONAL INFORMATION

Our group recognises that a data subject has the right to establish whether the group holds personal information related to him/her including the right to request access to that personal information.

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 group is no longer authorised 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, our group will give due consideration to the request and the requirements of POPI. Our group 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 POPI and to institute civil proceedings regarding the alleged non-compliance with the protection of his/her or its personal information.

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

CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

Our group is committed to processing personal information lawfully and to comply with the following conditions:

CONDITION 1: ACCOUNTABILITY (Section 8)

Our group maintains an approach of transparency of operational procedures that controls the collection and processing of personal information. We will ensure that the provisions of POPI and the principles outlined herein are complied with. Our GROUP 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 POPI could potentially damage the Group's reputation or expose the group to a civil claim for damages. **The protection of personal information is everyone in the group's responsibility.**

CONDITION 2 & 3: PROCESSING LIMITATION (Sections 9 – 12) & FURTHER PROCESSING LIMITATION (Section 15)

Our group 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.

Our group 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.

Our group 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 group 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 areas of the group's business and be provided with the reasons for doing so.

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 group. Our group is compelled to keep effective record of personal information and undertakes not to retain information for a period longer than prescribed by legislation, specifically the FAIS Act and as dictated by best business practice. All personal information will be disposed of at the end of the retention period in such a way that it cannot be reconstructed. Our group will inform data subjects of these requirements prior to collecting or recording the data subject's personal information.

CONDITION 5: INFORMATION QUALITY (Section 16)

Our group will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading. We 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)

Our group 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. Our group 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 group holds related personal information, or
Request access to related personal information, or
Request the group to update or correct related personal information, or
Make a complaint concerning the processing of personal information.

CONDITION 7: SECURITY SAFEGUARDS (Sections 19 – 22)

Our group 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 minimise the risk of loss, unauthorised 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 reports, the greater the security required. Our group will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the group's IT network. We will furthermore 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 group is responsible. All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment contracts containing the relevant consent and confidentiality clauses.

Our group's operators and third-party service providers will be required to enter into service level agreements with the group where both parties pledge their mutual commitment to POPI and the lawful processing of any personal information pursuant to the agreement an also to contain a confidentiality clause

CONDITION 8: DATA SUBJECT PARTICIPATION (Sections 23 – 25)

Our group will ensure that it provides a capability for data subjects who want to request the correction of or deletion of their personal information. Our group will also provide an option to data subjects to "unsubscribe" from any of its electronic newsletters or marketing material.

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 is not limited to:

- *Providing products or services to clients and to carry out the transactions requested.*
- *For underwriting purposes.*
- *Assessing and processing claims.*
- *Conducting credit reference searches and/or- verification.*
- *Confirming, verifying, and updating client details.*
- *For purposes of claims history.*
- *For the detection and prevention of fraud, crime, money laundering or other malpractices.*
- *Conducting market or customer satisfaction research.*
- *For audit and record keeping purposes.*
- *In connection with legal proceedings.*
- *To render financial advice and intermediary services as requested.*
- *To maintain and constantly improve the relationship.*
- *Providing communication in respect of the business of the group 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 POPI, 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, appointment and needs analysis stage of the relationship.

ii. The necessity of processing: to conduct an accurate analysis of the client's needs for purposes of amongst other credit limits, insurance requirements, etc.

iii. Processing complies with an obligation imposed by law on the group.

iv. The Financial Advisory and Intermediary Services Act ('FAIS') requires Financial Service Provider's ('FSPs') to conduct a needs analysis and obtain information from clients about their needs in order to provide them with applicable and beneficial products.

v. Processing protects a legitimate interest of the client — it is in the client's best interest to have a full and proper needs analysis performed in order to provide them with an applicable and beneficial product or service.

vi. Processing is necessary for pursuing the legitimate interests of the group or of a third party to whom information is supplied.

Our group may disclose a client's personal information to any of the group of companies or subsidiaries, joint venture companies and/or approved product or third-party product suppliers or service providers whose services or products clients elect to use. We will ensure that we have agreements in place to comply with confidentiality and privacy conditions.

Our group may also share client personal information with and obtain information about clients from third parties for the reasons already discussed herein above. We 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 to protect the rights of the group. It is a requirement in terms of the POPI to adequately protect personal information. Our group will continuously review its security controls and processes to ensure that personal information is secure.

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

✓ 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 POPI.

✓ 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 POPI.

✓ Any archived client information is stored at the offices of the group and is also governed by the POPI Access to these **documents is limited to authorised staff members only** and 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 to be backed up on a regular basis.

✓ **Consent to process client information** is obtained from each individual client (or a person who has been given authorisation from the client to provide the client's personal information) during the introductory, appointment and needs analysis stage of the relationship.

ROLES AND RESPONSIBILITIES OF KEY ROLEPLAYERS WITHIN THE GROUP:

SENIOR MANAGEMENT

Our group's senior management cannot delegate its accountability and is ultimately responsible for ensuring that the group meets its legal obligations in terms of POPI. Senior management may delegate some of its responsibilities in terms of POPI to management or other capable individuals.

Senior management is responsible for ensuring that:

- ✓ Our group appoints an Information Officer, and where necessary, a Deputy Information Officer.
- ✓ All persons responsible for the processing of personal information on behalf of the group are appropriately trained and supervised to do so, understand that they are contractually obligated to protect the personal information they meet 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.
- ✓ 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.
- ✓ A periodic POPI Audit is scheduled to accurately assess and review the ways in which the group collects, holds, uses, shares, discloses, destroys, and processes personal information.

INFORMATION OFFICER

Our Group's Information Officer is responsible for:

- ✓ Taking steps to ensure the group's reasonable compliance with the provision of POPI.
- ✓ Keeping senior management updated about the group's information protection responsibilities under POPI.
- ✓ Reviewing the group's information protection procedures and related policies.
- ✓ Ensuring that POPI audits are scheduled and conducted on a regular basis.
- ✓ Ensuring that the group 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 group.
- ✓ Ensuring the maintenance of a "contact us" facility on the group's website.
- ✓ Approving any contracts entered with operators, employees and other third parties which may have an impact on the personal information held by the group. This will include overseeing the amendment of the group'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 group are fully aware of the risks associated with the processing of personal information and that they remain informed about the group'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 group.
- ✓ Addressing employees' POPI related questions.
- ✓ Addressing all POPI related requests and complaints made by the group'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 regards to any other related matters.

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

IT MANAGER/SERVICE PROVIDER

Our group's IT Manager/Service Provider is responsible for:

- ✓ Ensuring that the group'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.
- ✓ 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 group'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 group's behalf.

MARKETING & COMMUNICATION MANAGER (where applicable)

Our Group's Marketing & Communication Manager is responsible for:

- ✓ Approving and maintaining the protection of personal information statements and disclaimers that are displayed on the group's website, including those attached to communications such as emails and electronic newsletters.
- ✓ Addressing any personal information protection queries received from the media and or newspapers.
- ✓ Working with any persons appointed by the group to handle outsourced marketing initiatives to ensure that all such information comply with the POPI.

EMPLOYEES AND OTHER PERSONS ACTING ON BEHALF OF THE GROUP:

Employees and other persons acting on behalf of the group 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, or password protected prior to sending or sharing the information electronically. The IT Manager/ Service Provider will assist employees and where required, other persons acting on behalf of the group, with the sending or sharing of personal information to or with authorised external persons.
- ✓ Ensuring that all computers, laptops, and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords 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. 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, 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 group, 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.

POPI COMPLIANCE AUDITS

Our group's Information Officer will schedule periodic POPI compliance audits.

The purpose of a POPI compliance audit is to:

- ✓ Identify the processes used to collect, record, store, disseminate and destroy personal information.
- ✓ Determine the flow of personal information throughout the group. For instance, the group's various business units, divisions, branches, and other associated groups.
- ✓ Redefine the purpose for gathering and processing personal information.
- ✓ Ensure that the processing parameters are still adequately limited.
- ✓ Ensure that new data subjects are made aware of the processing of their personal information.
- ✓ Re-establish the rationale for any further processing where information is received via a third party.
- ✓ Verify the quality and security of personal information.
- ✓ Monitor the extent of compliance with POPI and this policy.
- ✓ Monitor the effectiveness of internal controls established to manage the group's POPI related compliance risk.

The Information Officer will liaise with line managers to identify areas within in the group'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 group's senior management in performing their duties.

REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

Data subjects have the right to:

- ✓ Request what personal information the group 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 group's PAIA Policy. The Information Officer will process all requests within a reasonable time.

RETENTION PERIODS OF CERTAIN DOCUMENT TYPES IN TERMS OF DIFFERENT LEGISLATION

Documents need to be retained to prove the existence of facts and to exercise rights the group 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 group and to minimise reputational risks, to ensure that the group's interests are protected and that the clients' rights to privacy and confidentiality are not breached.

We have identified the following legislation to be most applicable to our group and the type of business we run and have highlighted the document retention requirements as required and need to take these into account in our data management processes:

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 ADVISORY AND INTERMEDIARY SERVICES ACT, (FAIS) NO 37 OF 2002

Section 18 of the Act requires a retention period of 5 years, except to the extent that it is exempted by the registrar for the below mentioned documents:

- Known premature cancellations of transactions or financial products of the provider by clients;
- Complaints received together with an indication whether or not any such complaint has been resolved;
- The continued compliance with this Act and the reasons for such noncompliance;
- And the continued compliance by representatives with the requirements referred to in section 13(1) and (2).

The General Code of Conduct for Authorised Financial Services Provider and Representatives requires a retention period of 5 years for the below mentioned documents:

- Proper procedures to record verbal and written communications relating to a financial service rendered to a client as are contemplated in the Act, this Code or any other Code drafted in terms of section 15 of the Act;
- Store and retrieve such records and any other material documentation relating to the client or financial services rendered to the client;
- And keep such client records and documentation safe from destruction
- All such records must be kept for a period after termination to the knowledge of the provider of the product concerned or in any other case after the rendering of the financial service concerned.

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 organisations 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 organisations 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 organisations 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

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.

POPI COMPLAINTS PROCEDURE

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

Complaints must be submitted in writing in the prescribed format.
The Information Officer will provide the data subject with a POPI Complaint Form (Refer to Annexure B)

Complaint received by any person other than the Information Officer, must ensure that the full details of the complaint reach the Information Officer within 1 (one) business day of receipt.

The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 (two) business days.

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 POPI.

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 group'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 unauthorised person, the Information Officer will consult with the group's senior management 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 group's senior management within 7 (seven) working days of receipt of the complaint. In all instances, the group 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.

DISCIPLINARY ACTION

Where a POPI complaint or a POPI infringement investigation has been finalised, the group 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 group 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 group 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 to limit any prejudice or damages caused.

PENALTIES FOR NON-COMPLIANCE

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

I. A fine of between R1 million and R10 million and/or imprisonment of one to ten years; or

II. Paying compensation to data subjects for the damage they have suffered.

The other penalties include:

- Reputational damage
- Losing customers (and employees)
- Failing to attract new customers.

AVAILABILITY AND REVISION

This policy is made available on the group's website (www.wealthassociates.co.za) and/or by request from the Deputy Information Officer of the group (Jessica Vermaak, jessica@wealthassociates.co.za). This policy will continually be updated to comply with legislation, thereby ensuring that personal information will be secure.