PROTECTION OF PERSONAL INFORMATION, DATA, INFORMATION SHARING & RETENTION OF DOCUMENTS POLICY

MOKOROSI FINANCIAL CONSULTING (PTY) LTD

(Registration No. 2013/137509/07)

(Hereinafter referred to as “MFC” or “The Company”)

CONTENTS

1. INTRODUCTION

1.1 This Protection of Personal Information and Data Policy, Information Sharing Policy & Retention of Documents describes the way that Mokorosi Financial Consulting (Pty) Ltd ("MFC" or the "Company"), will meet its legal obligations and requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the Protection of Personal Information Act, no 4 of 2013 (POPIA), as that is the key piece of legislation covering security and confidentiality of personal information.

1.2 The Company is obligated to comply with POPIA because we render financial services to clients.

1.3 The POPIA requires the Company to inform their clients as to the manner in which their personal information is used, disclosed and destroyed.

1.4 The Company guarantees its commitment to protecting its client's privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

1.5 The Policy sets out the manner in which the Company deals with their client's personal information and stipulates the purpose for which said information is used. A PAIA Manual is made available on the Company's website www.mfinconsult.com and other Policies by request from the Company's head office.

2. SCOPE OF THE POLICY

2.1 The Policy applies to all employees, Directors, sub-contractors, agents, appointees and clients of the Company. The provisions of the Policy are applicable to both on and off-site processing of personal information.

3. DEFINITIONS

Word	Definition
Client	includes, but are not limited to, shareholders, debtors, creditors as well as the affected personnel and/or departments related to a service division of the Company.
Confidential information	refers to all information or data disclosed to or obtained by the Company by any means whatsoever and shall include, but not be limited to financial information, records and all other information including information relating to the structure, operations, processes, intentions, product information, know-how, trade secrets, market opportunities, customers and business affairs but excluding the exceptions listed in paragraph 4.1 hereunder.
Constitution	Constitution of the Republic of South Africa Act, Act no 108 of 1996.
Data	refers to electronic representations of information in any form.
Documents	include books, records, security or accounts and any information that has been stored or recorded electronically, photographically, magnetically, mechanically, electro-mechanically or optically, or in any other form.
ECTA	Electronic Communications and Transactions Act, 25 of 2002.
Electronic communication	refers to a communication by means of data messages.
PAIA	Promotion of Access to Information Act, 2 of 2000
POPIA	Protection of Personal Information Act, no 4 of 2013
CEO	Chief Executive Officer

4. POLICY STATEMENT

4.1 The Company collects and uses Personal Information of the individuals and corporate entities with whom it works in order to operate and carry out its business effectively. The Company regards the lawful and appropriate processing of all Personal Information as crucial to successful service delivery and essential to maintaining confidence between the Company and those individuals and entities who it deals with. The Company therefore fully endorses and adheres to the principles of the POPIA.

5. PROCESSING OF PERSONAL INFORMATION

5.1 PERSONAL INFORMATION COLLECTED

5.1.1 Section 9 of the POPIA states that "Personal Information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive". The Company collects and processes client's personal information pertaining to the service required from the client. The type of information will depend on the need for which it is collected and will be processed for that purpose only. Whenever possible, the Company will inform the client as to the information required and the information deemed optional. Examples of personal information we collect include, but is not limited to:

- Personal information of employees as required by law;
- Personal Information of our client's details as agreed to in our agreement with the client to render our services;
- Any other information required by the Company, suppliers in order to provide clients with our service.

5.1.2 The Company also collects and processes the client's personal information for marketing purposes in order to ensure that our products and services remain relevant to our clients and potential clients.

5.1.3 The Company aims to have agreements in place with all product suppliers, insurers and third (3rd) party service providers to ensure a mutual understanding with regard to the protection of the client's personal information. The Company's suppliers will be subject to the same regulations as applicable to the Company.

5.1.4 With the client's consent, the Company may also supplement the information provided with information the Company receives from other providers in order to offer a more consistent and personalized experience in the client's interaction with the Company.

5.1.5 For purposes of this Policy, clients include potential and existing clients.

5.2 PURPOSE OF PROCESSING

5.2.1 The Company uses the Personal Information under its care in the following ways:

- Administration of agreements and or services;
- Providing client care and service delivery to clients;
- Conducting market or client satisfaction research;
- Marketing and sales;
- In connection with legal proceedings;
- Staff administration;
- Keeping of accounts and records;
- Complying with legal and regulatory requirements;
- Profiling Clients for the purposes of direct marketing.

5.3 THE USAGE OF PERSONAL INFORMATION

5.3.1 The Client's Personal Information will only be used for the purpose for which it was collected and as agreed, this may include:

- Providing products or services to clients and to carry out the clients requests;
- Confirming, verifying and updating client details;
- Conducting market or client satisfaction research;
- In connection with legal proceedings;
- Providing services to clients, to render the services requested and to maintain and constantly improve the relationship;
- Providing communication in respect of the Company and regulatory matters that may affect clients; and
- In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

5.3.2 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 Company's processing of Personal Information:

- The client's consents to the processing, consent is obtained from clients during the introductory, appointment and needs analysis stage of the relationship.
- The necessity of processing, in order to conduct an accurate analysis of the client's needs.
- Processing complies with an obligation imposed by law on the Company.
- Processing protects a legitimate interest of the client whilst providing them with an applicable and beneficial product or service.
- Processing is necessary for pursuing the legitimate interests of the Company or of a third (3rd) party to whom information is supplied in order to provide the Company's clients with products and or services both the Company and any of our product suppliers require certain personal information from the clients in order to make a decision on the unique and specific product and or service required.

5.4 CATEGORIES OF CLIENTDATA SUBJECTS AND THEIR PERSONAL INFORMATION

5.4.1 The Company may possess records relating to clients, suppliers, shareholders, contractors service providers, staff and customers:

Entity Type	Personal Information Processed

Natural Persons	Names; contact details; physical and postal addresses; date of birth; ID number; tax related information; nationality; gender; confidential correspondence
Juristic Persons / Entities	Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; BBBEE information
Contracted Service Providers	Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; BBBEE information
Employees / Directors	Gender; pregnancy; marital status; colour, race; age; language; education information; financial information; employment history; ID number; physical and postal address; contact details; opinions; criminal record; well-being

5.5 CATEGORIES OF RECIPIENTS FOR PROCESSING THE PERSONAL INFORMATION

5.5.1 The Company may share the Personal Information with its agents, affiliates, and associated companies who may use this information to send the Data Subject information on products and services. The Company may supply the Personal Information to any party to whom the Company may have assigned or transferred any of its rights or obligations under any agreement, and/or to service providers who render the following services:

- Capturing and organising of data;
- Storing of data;
- Sending of emails and other correspondence to clients;
- Conducting due diligence checks;

5.6 DISCLOSURE OF PERSONAL INFORMATION

5.6.1 The Company may disclose a client's personal information to subsidiaries, joint venture companies and/or approved product or third (3rd) party service providers whose services or products the Company elect to use. The Company has agreements in place to ensure that compliance with confidentiality and privacy conditions are adhere to.

5.6.2 The Company may also share client personal information with, and obtain information about clients from third (3rd) parties for the reasons already discussed above.

5.6.3 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 Company's rights.

5.7 SAFEGUARDING CLIENT INFORMATION

5.7.1 It is a requirement of POPIA to adequately protect personal information. The Company will continuously review its security controls and processes to ensure that personal information is secure.

5.7.2 The following procedures are in place in order to protect personal information:

- The Company's Information Officer is the Chief Executive Officer (CEO) whose details are available below and who is responsible for the compliance with the conditions of the lawful processing of personal information and other provisions of POPIA.
- This Policy has been put in place for the Company and training on this policy and the POPIA is provided.
- Each new employee will be required to sign an Employment Contract containing relevant consent clauses for the use and storage of personal information, or any other action so required, in terms of the POPIA.
- Client personal information is stored on site, which is also governed by POPIA, access is limited to these areas to authorised personal.
- The Company's product suppliers, insurers and other third (3rd) 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 by the Company's IT support which is also responsible for system and information security that protects third (3rd) party access and physical threats.

5.7.3 Consent to process client information is obtained from clients (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.

5.8 THE DETAILS OF THE COMPANY'S INFORMATION OFFICER AND HEAD OFFICE

5.8.1 Information officer details Jolly Mokorosi

5.8.2 Head office details:

- Postal Address: Box 783163

Sandton
2146

- Physical Address: 52 Winston Avenue
  Robin Hills
  Randburg
  JOHANNESBURG
  2194
  - Telephone 011 057 1701
  - E-mail jmokorosi@mfinconsult.com
  - Website www.mfinconsult.com

5.9 ACCESS AND CORRECTION OF PERSONAL INFORMATION

5.9.1 Clients have the right to:

- Access the personal information the Company holds about them;
- Update and correct their personal information;
- Delete their personal information on reasonable grounds.

5.9.2 Once a client objects to the processing of their personal information, the Company may no longer process said personal information.

5.9.3 The Company will take all reasonable steps to confirm its clients' identity before providing details of their personal information or making changes to their personal information.

5.10 REMEDIES AVAILABLE IF REQUEST FOR ACCESS TO PERSONAL INFORMATION IS REFUSED

5.10.1 Internal Remedies:

The Company does not have internal appeal procedures. As such, the decision made by the Information Officer pertaining to a request is final, and requestors will have to exercise such external remedies at their disposal if a request is refused, and the requestor is not satisfied with the response provided by the Information Officer.

5.10.2 External Remedies:

A requestor that is dissatisfied with the Information Officer's refusal to disclose information, may within thirty (30) days of notification of the decision, apply to a court for relief. Likewise, a third (3rd) party dissatisfied with the Information Officer's decision to grant a request for information, may within thirty (30) days of notification of the decision, apply to a court for relief. For purposes of the Act,

courts that have jurisdiction over these applications are the Constitutional Court, the High Court or another court of similar status.

5.11 GROUNDS FOR REFUSAL

5.11.1 The Company may legitimately refuse to grant access to a requested record that falls within a certain category, grounds on which the Company may refuse access include:

- Protecting personal information that the Company holds about a third (3rd) person (who is a natural person) including a deceased person, from unreasonable disclosure;
- Protecting commercial information that the Company holds about a third (3rd) party or the Company (for example trade secret: financial, commercial, scientific or technical information that may harm the commercial or financial interests of the organisation or the third (3rd) party);
- If disclosure of the record would result in a breach of a duty of confidence owed to a third (3rd) party in terms of an agreement;
- If disclosure of the record would endanger the life or physical safety of an individual;
- If disclosure of the record would prejudice or impair the security of property or means of transport;
- If disclosure of the record would prejudice or impair the protection of a person in accordance with a witness protection scheme;
- If disclosure of the record would prejudice or impair the protection of the safety of the public;
- The record is privileged from production in legal proceedings, unless the legal privilege has been waived;
- Disclosure of the record (containing trade secrets, financial, commercial, scientific, or technical information) would harm the commercial or financial interests of the Company;
- Disclosure of the record would put the Company at a disadvantage in contractual or other negotiations or prejudice it in commercial competition;
- The record is a computer programme; and
- The record contains information about research being carried out or about to be carried out on behalf of a third (3rd) party or the Company.

5.11.2 Records that cannot be found or do not exist, if the Company has been requested to search for a record by a reasonable requester and it is believed that the record does not exist or cannot be found, the requester will be notified by way of a written document or affirmation. This will include the steps that were taken to try to locate the record.

5.12 ACTUAL OR PLANNED TRANSBORDER FLOWS OF PERSONAL INFORMATION

5.12.1 Personal information may be transmitted transborder to the Company's authorised dealers and its suppliers in other countries, and personal information may be stored in data servers hosted outside South Africa, which may not have adequate data protection laws. The Company will endeavour to ensure that its dealers and suppliers will make all reasonable efforts to secure said data and personal information.

5.13 RETENTION OF PERSONAL INFORMATION RECORDS

5.13.1 The Company may retain personal Information records indefinitely, unless the Data Subject objects thereto. If the Data Subject objects to indefinite retention of its Personal Information the Company shall retain the Personal Information records to the extent permitted or required by law as summarised in **Annexure A** below.

5.14 GENERAL DESCRIPTION OF INFORMATION SECURITY MEASURES

5.14.1 The Company employs up to date technology to ensure the confidentiality, integrity and availability of the Personal Information under its care. Measures include:

- Firewalls;
- Virus protection software and update protocols;
- Logical and physical access control;
- Secure setup of hardware and software making up the IT infrastructure.

6. IMPLEMENTATION GUIDELINES

6.1 TRAINING & DISSEMINATION OF INFORMATION

6.1.1 This Policy has been put in place for the Company, training on the Policy and POPIA will take place with employees.

6.1.2 All new employees will be made aware at induction, or through training programmes, of their responsibilities under the terms of this Policy and POPIA.

6.1.3 Modifications and updates to data protection and information sharing policies, legislation, or guidelines will be brought to the attention of employees.

6.2 EMPLOYEE CONTRACTS

6.2.1 New employees will sign an Employment Contract containing the relevant clauses for the use and storage of personal information, and will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information. Failure to comply will result in Disciplinary steps being taken against the employee which could lead to his/her dismissal.

6.2.1 Each employee currently employed within the Company will sign an addendum to their Employment Contract if their current contract did not address POPIA, the addendum will be containing the relevant clauses for the use and storage of personal information, and will be personally responsible for ensuring

there are no breaches of confidentiality in relation to any Personal Information. Failure to comply will result in Disciplinary steps being taken against the employee which could lead to his/her dismissal.

7. EIGHT PROCESSING CONDITIONS

The Company shall abide by these principles in all its possessing activities.

7.1 ACCOUNTABILITY

7.1.1 The Company shall ensure that all processing conditions, as set out in POPIA, are complied with when determining the purpose and means of processing personal information during the processing itself. The Company shall remain liable for compliance with these conditions, even if it has outsourced it processing activities.

7.2 PROCESSING LIMITATION

7.2.1 Lawful grounds

a) The processing of personal information is only lawful if, given the purpose of processing, the information is adequate, relevant and not excessive.

b) The Company may only process personal information if one of the following grounds of lawful processing exists:

- The Data Subject consents to the processing;
- Processing is necessary for the conclusion or performance of agreements with the Data Subject;
- Processing complies with a legal responsibility imposed on the Company;
- Processing protects a legitimate interest of the Data Subject;
- Processing is necessary for pursuance of a legitimate interest of the Company, or a third (3rd) party to whom the information is supplied to.

c) Special Personal Information includes:

- Religious, philosophical, or political beliefs;
- Race or ethnic origin;
- Trade union membership;
- Health or sex life;
- Biometric information (including blood type, fingerprints, DNA, retinal scanning, voice recognition, photographs);
- Criminal behaviour; and

- Information concerning a child.

d) The Company may only process Special Personal Information under the following circumstances:

- The Data Subject has consented to such processing;
- The Special Personal Information was deliberately made public by the Data Subject;
- Processing is necessary for the establishment of a right or defence in law;
- Processing is for historical, statistical, or research reasons;
- If processing of race or ethnic origin is in order to comply with affirmative action laws.

e) All Data Subjects have the right to refuse or withdraw their consent to the processing of their Personal Information, and a Data Subject may object, at any time, to the processing of their Personal Information on any of the above grounds, unless legislation provides for such processing. If the Data subject withdraws consent or objects to processing then the Company shall forthwith refrain from processing the Personal Information.

7.2.2 Personal Information must be collected directly from the Data Subject, unless:

- Personal Information is contained in a public record;
- Personal Information has been deliberately made public by the Data Subject;
- Personal Information is collected from another source with the Data Subject's consent;
- Collection of Personal Information from another source would not prejudice the Data Subject;
- Collection of Personal Information from another source is necessary to maintain, comply with or exercise any law or legal right;
- Collection from the Data Subject would prejudice the lawful purpose of collection;
- Collection from the Data Subject is not reasonably practicable.

7.3 PURPOSE SPECIFICATION

7.3.1 The Company shall only process Personal Information for the specific purposes as set out and defined above at paragraph 7.2.

7.4 FURTHER PROCESSING

7.4.1 New processing activity must be compatible with original purpose of processing. Further processing will be regarded as compatible with the purpose of collection if:

- Data Subject has consented to the further processing;
- Personal Information is contained in a public record;
- Personal Information has been deliberately made public by the Data Subject;
- Further processing is necessary to maintain, comply with or exercise any law or legal right;

- Further processing is necessary to prevent or mitigate a threat to public health or safety, or the life or health of the Data Subject or a third (3rd) party.

7.5 INFORMATION QUALITY

7.5.1 The Company shall take reasonable steps to ensure that Personal Information is complete, accurate, not misleading and updated. The Company shall periodically review their records to ensure that the Personal Information is still valid and correct.

7.5.2 Employees should as far as reasonably practicable follow the following guidance when collecting Personal Information:

- Personal Information should be dated when received;
- A record should be kept of where the Personal Information was obtained;
- Changed to information records should be dated;
- Irrelevant or unneeded Personal Information should be deleted or destroyed;
- Personal Information should be stored securely, either on a secure electronic database or in a secure physical filing system.

7.6 OPENNESS

7.6.1 The Company shall take reasonable steps to ensure that the Data Subject is made aware of:

- What Personal Information is collected, and the source of the information;
- The purpose of collection and processing;
- Where the supply of Personal Information is voluntary or mandatory, and the consequences of a failure to provide such information;
- Whether collection is in terms of any law requiring such collection;
- Whether the Personal Information shall be shared with any third (3rd) party.

7.7 DATA SUBJECT PARTICIPATION

7.7.1 The Data Subject have the right to request access to, amendment, or deletion of their Personal Information. All such requests must be submitted in writing to the Information Officer. Unless there are grounds for refusal as set out in paragraph 5.11, above, the Company shall disclose the requested Personal Information:

- On receipt of adequate proof of identity from the Data Subject, or requester;
- Within a reasonable time;
- On receipt of the prescribed fee, if any;
- In a reasonable format.

7.7.2 The Company shall not disclose any Personal Information to any party unless the identity of the requester has been verified.

7.8 SECURITY SAFEGUARDS

7.8.1 The Company shall ensure the integrity and confidentiality of all Personal Information in its possession, by taking reasonable steps to:

- Identify all reasonably foreseeable risks to information security;
- Establish and maintain appropriate safeguards against such risks.

7.8.2 Written records

- Personal Information records should be kept in locked cabinets, or safes;
- When in use Personal Information records should not be left unattended in areas where non-staff members may access them;
- Employees shall be required to clear their desks of all Personal Information when leaving their desks for any length of time and at the end of the day;
- Personal Information which is no longer required should be disposed of by shredding.

7.8.3 Any loss or theft of, or unauthorised access to, Personal Information must be immediately reported to the Information Officer.

7.8.4 Electronic Records

- All electronically held Personal Information will be saved in a secure database;
- As far as reasonably practicable, no Personal Information will be saved on individual computers, laptops or hand-held devices;
- All computers, laptops and hand-held devices should be access protected with a password, fingerprint or retina scan, with the password being of reasonable complexity and changed frequently;
- Employees shall be required to lock their computers or laptops when leaving their desks for any length of time and to log off at the end of the day;
- Electronical Personal Information which is no longer required must be deleted and may not be recoverable from the individual laptop \ computer and the relevant database except for information that should be stored for a specific period as required by relevant acts.

7.8.5 Any loss or theft of computers, laptops or other devices which may contain Personal Information must be immediately reported to the Information Officer, who shall notify the IT department, who shall take all necessary steps to remotely delete the information, if possible.

8. DIRECT MARKETING make sure you have clients permission

8.1. DIRECT MARKETING

8.1.1 All Direct Marketing communications shall contain the Company's details, and an address or method for the client to opt-out of receiving further marketing communication.

8.2 EXISTING CLIENTS

8.2.1 Direct Marketing by electronic means to existing clients is only permitted:

- If the client's details were obtained in the context of a sale or service; and
- For the purpose of marketing the same or similar products.

8.2.2 The client must be given the opportunity to opt-out of receiving direct marketing on each occasion of direct marketing.

8.3 CONSENT

8.3.1 The Company may send electronic Direct Marketing communication to Data Subjects who have consented to receiving it. The Company may approach a Data Subject for consent only once.

8.4 RECORD KEEPING

8.4.1 The Company shall keep record of:

- Date of consent;
- Wording of the consent;
- Who obtained the consent;
- Proof of opportunity to opt-out on each marketing contact;
- Record of opt-outs.

9. DESTRUCTION OF DOCUMENTS

9.1 Documents may be destroyed after the termination of the retention period specified herein, or as determined by the Company from time to time.

9.2 Each department is responsible for attending to the destruction of its documents and electronic records, which must be done on a regular basis. Files must be checked in order to make sure that they may be destroyed and also to ascertain if there are important original documents in the file. Original documents

must be returned to the holder thereof, failing which, they should be retained by the Company pending such return.

9.3 The documents will be made available for collection to be disposed.

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

10. ACCESS TO COMPANY DOCUMENTS

10.1 Requests for company information:

- These are dealt with in terms of PAIA, which gives effect to the constitutional right of access to information held by the State or any person (natural and juristic) that is required for the exercise or protection of rights. Private bodies, like the Company, must however refuse access to records if disclosure would constitute an action for breach of the duty of secrecy owed to a third (3rd) party.

- In terms hereof, requests must be made in writing to the Information Officer. The requesting party has to state the reason for wanting the information and may be required to pay an administration fee.

10.2 Confidential Company information may not be disclosed to third (3rd) parties information must be kept strictly confidential at all times.

10.3 The Company views any contravention of this policy very seriously and failure to comply will result in Disciplinary steps being taken against the employee which could lead to his/her dismissal.

11. APPROVAL AND VERSION CONTROL

11.1 This policy is effective from the 01 July 2021.

11.2 Approved by The Company's CEO at _____ on this ____ day of _____ 2021.

_____

Jolly Mokorosi

Mokorosi Financial Consulting (Pty) Ltd

ANNEXURE A: STORAGE OF DOCUMENTS & STATUTORY RETENTION PERIODS

1. HARD COPIES

1.1 Documents are stored in a archive.

1.2 Companies Act, Act no 71 of 2008

1.2.1 The Companies Act, Act no 71 of 2008 and the Companies Amendment Act, Act no 3 of 2011, hardcopies of the documents mentioned below must be retained for seven (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.

1.2.2 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 five percent (5%) of the securities of that class issued.

1.3 Consumer Protection Act, Act no 68 of 2008

1.3.1 The Consumer Protection Act seeks to promote a fair, accessible and sustainable marketplace and therefore requires a retention period of three (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.

1.4 National Credit Act, Act no 34 of 2005

1.4.1 The National Credit Act aims to promote a fair and transparent credit industry which requires the retention of certain documents for a specified period.

1.4.2 Retention for three (3) years from the earliest of the dates of which the registrant created, signed or received the document or from the date of termination of the agreement or in the case of an application for credit that is refused or not granted for any reason, from the date of receipt of the application which applies to the documents mentioned below:

a) Regulation 55(1)(b):

- Records of registered activities such as an application for credit declined;
- Reason for the decline of the application for credit;
- Pre-agreement statements and quotes;
- Documentation in support of steps taken in terms of section 81(2) of the Act;
- Record of payments made;
- Documentation in support of steps taken after default by consumer.

b) Regulation 55(1)(c) in respect of operations:

- Record of income, expenses and cash flow;
- Credit transaction flows;
- Management accounts and financial statements.

c) Regulation 55(1)(d) with regard to the Credit Bureau:

- All documents relating to disputes, inclusive of but not limited to, documents from the consumer;

- Documents from the entity responsible for disputed information;
- Documents pertaining to the investigation of the dispute;
- Correspondence addressed to and received from sources of information as set out in section 70(2) of the Act and Regulation 18(7) pertaining to the issues of the disputed information.

d) Regulation 55(1)(a) with regard to Debt Counsellors:

- Application for debt review;
- Copies of all documents submitted by the consumer;
- Copy of rejection letter;
- Debt restructuring proposal;
- Copy of any order made by the tribunal and/or the court and a copy of the clearance certificate.

e) Regulation 56 with regard to section 170 of the Act:

- Application for credit;
- Credit agreement entered into with the consumer.

f) Regulation 17(1) with regard to Credit Bureau information:

- Documents with a required retention period of the earlier of 10 years or a rehabilitation order being granted:

o Sequestrations
o Administration orders.

- Documents with a required retention period of five (5) years: - Rehabilitation orders

o Payment profile.

- Documents with a required retention period of the earlier of five (5) years or until judgment is rescinded by a court or abandoned by the credit provider in terms of section 86 of the Magistrate's Court Act, Act no 32 of 1944:

g) Civil Court Judgments

- Documents with a required retention period of two (2) years:

o Enquiries.

- Documents with a required retention period of one and a half (1.5) years:

o Details and results of disputes lodged by the consumers.

- Documents with a required retention period of one (1) year:

o Adverse information.

- Documents with an unlimited required retention period:

- o Liquidation.

- Documents required to be retained until a clearance certificate is issued:
- o Debt restructuring.

1.5 Financial Intelligence Centre Act, Act no 38 of 2001:

1.5.1 Section 22 and 23 of the Act require a retention period of five (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 clients 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.

1.5.2 These documents may also be kept in electronic format.

1.6 Compensation for Occupational Injuries and Diseases Act, Act no 130 of 1993:

1.6.1 Section 81(1) and (2) of the Compensation for Occupational Injuries and Diseases Act requires a retention period of 4 years for the documents mentioned below:

- Register, record or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees.

1.6.2 Section 20(2) documents with a required retention period of three (3) years:

- Health and safety committee recommendations made to an employer in terms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation;
- Records of incidents reported at work.

1.6.3 Asbestos Regulations, 2001, regulation 16(1) requires a retention period of minimum 40 years for the documents mentioned below:

- Records of assessment and air monitoring, and the asbestos inventory;
- Medical surveillance records;

1.6.4 Hazardous Biological Agents Regulations, 2001, Regulations 9(1) and (2):

- Records of risk assessments and air monitoring;
- Medical surveillance records.

1.6.5 Lead Regulations, 2001, Regulation 10:

- Records of assessments and air monitoring;
- Medical surveillance records.

1.6.6 Noise - induced Hearing Loss Regulations, 2003, Regulation 11:

- All records of assessment and noise monitoring;
- All medical surveillance records, including the baseline audiogram of every employee.

1.6.7 Hazardous Chemical Substance Regulations, 1995, Regulation 9 requires a retention period of 30 years for the documents mentioned below: - Records of assessments and air monitoring;

- Medical surveillance records.

1.7 Employment Equity Act, No 55 of 1998:

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

- Records in respect of the Company's workforce;
- Employment equity plan;
- Reports send to the Director General; and
- Other records relevant to compliance with the Act.

1.7.2 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.

1.7.3 With regard to the Employment Equity Act, Act no 55 of 1998, hardcopies of the documents mentioned below must be retained for three (3) years:

- Records in respect of the company's workforce, employment equity plan and other records relevant to compliance with the Act;
- Section 21 report which is sent to the Director General

1.8 Labour Relations Act, No 66 of 1995:

1.8.1 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.
- An employer must retain prescribed details of any strike, lock-out or protest action involving its employees indefinitely.
- Records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions must be kept indefinitely.

1.8.2 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.

1.9 Unemployment Insurance Act, No 63 of 2002:

1.9.1 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.

1.9.2 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.

1.10 Tax Administration Act, No 28 of 2011:

1.10.1 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.

1.10.2 Section 29(3)(a) requires a retention period of five (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 five (5) year period applies for taxpayers who were meant to submit a return, but have not.

.

1.10.3 Section 29(3)(b) requires a retention period of five (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.

1.10.3 Section 32(a) and (b) require a retention period of five (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.

1.11 Income Tax Act, Act no 58 of 1962:

1.11.1 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 employees 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.

1.11.2 Schedule 6, paragraph 14(a)-(d) requires a retention period of five (5) years from the date of submission or five (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.

1.12 Value Added Tax Act, Act no 89 of 1991:

1.12.1 Section 15(9), 16(2) and 55(1)(a) of the Value Added Tax Act and Interpretation Note 31, requires a retention period of 5 years from the date of submission of the return for the documents mentioned below:

- Where a vendor's basis of accounting is changed the vendor shall prepare lists of debtors and creditors showing the amounts owing to the creditors at the end of the tax period immediately preceding the changeover period;
- Importation of goods, bill of entry, other documents prescribed by the Custom and Excise Act and proof that the VAT charge has been paid to SARS;
- Vendors are obliged to retain records of all goods and services, rate of tax applicable to the supply, list of suppliers or agents, invoices and tax invoices, credit and debit notes, bank statements, deposit slips, stock lists and paid cheques;
- Documentary proof substantiating the zero rating of supplies;
- Where a tax invoice, credit or debit note, has been issued in relation to a supply by an agent or a bill of entry as described in the Customs and Excise Act, the agent shall maintain sufficient records to enable the name, address and VAT registration number of the principal to be ascertained.

1.13 Basic Conditions of Employment Act. Act no 75 1997

1.13.1 With regard to the Basic Conditions of Employment Act, Act no 75 1997, hardcopies of the documents mentioned below must be retained for three (3) years:

- Section 29(4):

- Written particulars of an employee after termination of employment;

- Section 31:
- Employee's name and occupation;
- Time worked by each employee;
- Remuneration paid to each employee; and
- Date of birth of any employee under the age of eighteen (18) years.