MAKING A DIFFERENCE

DATA PROTECTION AND INFORMATION SHARING POLICY

THE AMBITON GROUP CONSISTS OF:

AMBITON FINANCIAL SERVICES (PTY) LTD (FSP 8777)

AMBITON MEDICAL HEALTH SERVICES (PTY) LTD (FSP 8776)

AMBITON DIRECT (PTY) LTD (FSP 51790)

AMBITON ACCOUNTING ADVISORY SERVICES (PTY) LTD

OBJECTIVE:

This Data Protection and Information Sharing Policy describes the way that The Ambiton Group (the "Group"), will meet its legal obligations and requirements concerning confidentiality and information security standards, as well as the processes for access to information held by The Ambiton Group. The requirements within the Policy are primarily based upon the Protection of Personal Information Act, No 4 of 2013 as well as the Promotion of Access to Information Act, No 2 of 2000.

POLICY INDEX

No	Policy Forms	Effective date	Review date	Responsible Person
1	Ambiton Data Protection and Information Sharing Policy	01/03/2022	01/03/2023	Ashton De Kock

GLOSSARY

Abbreviations & Definitions	
Consent	means the voluntary, specific and informed expression of will
Data Subject	means the natural or juristic person to whom the Personal Information relates
Direct Marketing	means approaching a Data Subject personally for the purpose of selling them a product or service, or requesting a donation
Group	means Ambiton Group, comprising of Ambiton Financial Services Pty Ltd, Ambiton Medical Health Services Pty Ltd, Ambiton Direct, and Ambiton Accounting Advisory Services Pty Ltd
Personal Information	means information relating to an unidentifiable, living, natural person, or an identifiable, existing juristic person, as defined by the POPI Act
Processing	means an operation or activity, whether or not by automatic means, concerning Personal Information
Special Information	means personal information of a special nature as defined by the POPI Act

LEGISLATION

	Abbreviations & Legislation
POPI / POPIA	Protection of Personal Information Act, No. 4 of 2013 (as amended)
PAIA	Promotion of Access to Information Act, No. 2 of 2000 (as amended)

REVIEW

Review Date	By Whom	Reason	Next Review Date
15 June 2021	Ashton De Kock	Creation on new policy v202106	30 June 2022
01 March 2022	Ashton De Kock	Incorporation of PAIA v202203	01 March 2023

Contents

IMPORTANT CONTACT INFORMATION:

Head of body:	Leonie Billson (Managing Director)
Information Officer:	Ashton De Kock
Postal Address:	PO Box 40036, Walmer, 6065
Telephone Number:	+27 41 581 7170
Email address:	compliance@ambiton.co.za

DETAILS OF THE INFORMATION REGULATOR:

Postal Address:	P.O Box 31533, Braamfontein, Johannesburg, 2017
Telephone Number:	+27 10 023 5200
Email Address:	enquiries@inforegulator.org.za

1. SCOPE OF THE POLICY

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

2. POLICY STATEMENT

The Group collects and uses Personal Information of the individuals, Trusts, and corporate entities with whom it works in order to operate and carry out its business effectively. The Group regards the lawful and appropriate processing of all Personal Information as crucial to successful service delivery and essential to maintaining confidence between the Group and those individuals and entities who deal it. The Group therefore fully endorses and adheres to the principles of the Protection of Personal Information Act ("POPIA"). While the right to protection of personal information is acknowledged, the right to access to information under specific circumstances – as defined in PAIA - is equally acknowledged. The Group undertakes to protect both rights at all times, to the best of our ability and in accordance with the underlying Legislation.

3. PROCESSING OF PERSONAL INFORMATION

Purpose of Processing

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

- Providing advice and intermediary services in relation to financial products
- Providing advice and administration of deceased estates
- Providing advice and administration in relation to accounting and taxation services
- Detecting and prevention of fraud, crime, money laundering and other malpractice
- Sharing information with 3rd parties pursuant to complying with contractual requirements, including Financial product providers, the Master's Office, email / storage / backup service providers, external Compliance Officers, and the like.
- Conducting market or customer satisfaction research
- Marketing and sales, and statistics related thereto
- In connection with legal proceedings
- Staff administration
- Keeping of accounts and records
- Complying with legal and regulatory requirements

- Due diligence

3.1. Categories of Data Subjects and their Personal Information

The Group may possess records relating to suppliers, shareholders, contractors service providers, staff and customers which may contain the following information:

Entity Type	Personal Information Processed
Customers, Staff, Candidates, and Directors: **Natural Persons**	Names; contact details; physical and postal addresses; date of birth; ID number; biometric and psychometric information; race; religion and dietary requirements; hobbies; smoking status; allergies; education; occupation and income information; spouse, children's, siblings, and linked identities information; financial products and services information; medical and health information; tax and accounting related information; nationality; gender; opinions; criminal record; general and confidential correspondence
Customers: **Juristic Persons / Entities**	Names of contact persons; names of legal entity; physical and postal address and contact details; financial information; company identification information; tax and accounting related information; authorised signatories; beneficial owners and linked identities; shareholding and constitutional information; BBBEE information; general and confidential correspondence
Contracted Service Providers:	Names of contact persons; names of legal entity; physical and postal address and contact details; financial information; company identification information; tax and accounting related information; authorised signatories; information required in the discharging of contractual obligations; BBBEE information ; general and confidential correspondence; statistical information

3.2. Categories of Recipients for Processing the Personal Information

The Group 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 Group may supply the Personal Information to any party to whom the Group may have assigned or transferred any of its rights or obligations under any agreement, and/or to service providers who render the following services:

- Issuing, maintenance, and sourcing proposals in relation to Financial and non-Financial Products as required contractually
- Storing and backing up of data;
- Sending and receiving of emails and other correspondence;
- Conducting due diligence checks;
- Administration of the Medical Aid and Pension Schemes;
- Legal Compliance auditing or oversight;
- In the discharge of reporting obligations as required by Legislation.

3.3. Actual or Planned Transborder Flows of Personal Information

Personal Information may be transmitted transborder to the Group's service providers 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. While The Group endeavours to ensure that its service providers and suppliers make all reasonable efforts to secure said data and Personal Information, there may be factors outside of the Group's control in enforcing such security. Such examples include software provisioned as a service through Corporate Citizens such as the Microsoft Corporation and others.

3.4. Retention of Personal Information Records

The Group may retain certain Personal Information records indefinitely, unless the Data Subject objects thereto. If the Data Subject objects to indefinite retention of its Personal Information the Group shall retain the Personal Information records to the extent permitted or required by law.

3.5. General Description of Information Security Measures

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

- Firewalls;
- Malicious software protection and update protocols;
- Logical and physical access control;
- Encryption and backing up of data;
- Secure configuration of hardware and software making up the IT infrastructure;
- Staff Awareness and training

4. ACCESS TO PERSONAL INFORMATION

All individuals and entities may request access, amendment, or deletion of their own Personal Information held by the Group. Requests to amend Personal Information must be communicated through the Group's regular service channels (monitored email addresses, phoning the office directly).

Any requests to access or delete Personal Information other than One's own should be directed, on the prescribed form, to the Information Officer. Information freely available on The Group's website does not require submission of a request form.

The Regulator has, in terms of section 10(1) of PAIA, as amended, updated and made available the revised Guide on how to use PAIA ("Guide"), in an easily comprehensible form and manner, as may reasonably be required by a person who wishes to exercise any right contemplated in PAIA and POPIA. The Guide is available in each of the official languages and in braille on request from https://www.inforegulator.org.za/ or from The Group's website (https://www.ambiton.co.za) or on request from The Group's offices in English and Afrikaans.

4.1. Categories of records available for request

We post the following information to our website, which requires no request form to view:

Blogs and articles from various sources, our mission and values, our service offerings, our sales and management teams, corporate social responsibility, client testimonials, various forms and brochures, available vacancies, information on each of our product lines, and our contact information.

The following information is available for request from the Information Officer:

Corporate Governance information, various policies and procedures, HR information, client information, sales information, legal information, and internal communications.

4.2. Remedies available if request for access to Personal Information is refused

4.2.1. Internal Remedies

The Group 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.

4.2.2. External Remedies

A requestor or third party that is dissatisfied with The Group's refusal to disclose information, may within 30 days of notification of the decision lodge a complaint with the Information Regulator or 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.

4.3. Grounds for Refusal

The Group may legitimately refuse to grant access to a requested record that falls within a certain category. Grounds on which the Group may refuse access include:

- Protecting personal information that the Group holds about a third person (who is a natural person) including a deceased person, from unreasonable disclosure;
- Protecting commercial information that the Group holds about a third party or the Group (for example trade secret: financial, commercial, scientific or technical information that may harm the commercial or financial interests of the organisation or the third party);
- If disclosure of the record would result in a breach of a duty of confidence owed to a third 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 Group;
- Disclosure of the record would put the Group at a disadvantage in contractual or other negotiations or prejudice it in commercial competition;
- The record is a computer program; or
- The record contains information about research being carried out or about to be carried out on behalf of a third party or the Group.

4.4. Records that cannot be found or do not exist

If the Group has searched for a record and it is believed that the record does not exist or cannot be found, the requester will be notified by way of an affidavit or affirmation. This will include the steps that were taken to try to locate the record.

5. IMPLEMENTATION GUIDELINES

5.1. Training & Dissemination of Information

- This Policy has been implemented throughout the Group, and all staff handling information have been trained accordingly and the relevant training registers kept.
- All new employees will be made aware at induction, or through training programmes, of their responsibilities under the terms of this Policy and POPIA.
- Modifications and updates to data protection and information sharing policies, legislation, or guidelines will be brought to the attention of all staff.

5.2. Employee Contracts

Confidentiality is an inherent requirement of FAIS Law, and as such is contained in each staff member's Employment Contract. Each Employee is trained in their departmental processes and are trained on POPIA compliance, and understand that failure to comply will result in disciplinary action.

6. EIGHT PROCESSING CONDITIONS

POPIA is implemented by abiding by eight processing conditions. The Group shall abide by these principles in all its possessing activities.

8.1. Accountability

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

8.2. Processing Limitation

8.2.1. Lawful grounds

The processing of Personal Information is only lawful if, given the purpose of processing, the information is adequate, relevant and not excessive.

The Group 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 a contract with the Data Subject;
- Processing complies with a legal responsibility imposed on the Group;
- Processing protects a legitimate interest of the Data Subject; or
- Processing is necessary for pursuance of a legitimate interest of the Group, or a third party to whom the information is supplied.

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; or
- Information concerning a child.

The Group 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

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 or such processing is a contractual requirement. If the Data subject withdraws consent or objects to processing then the Group shall forthwith refrain from processing the Personal Information, subject to any applicable Legislation preventing The Group from complying with the Data Subject's instruction.

8.2.2. Collection directly from the Data Subject

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.

8.3. Purpose Specification

The Group shall only process Personal Information for the specific purposes as set out and defined above at paragraph 4.1.

8.4. Further Processing

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 party

8.5. Information Quality

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

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

- Personal Information should be received via email or other electronic means so that it is electronically dated, and that the source of the record is kept;
- Where received in person, the records must be filed electronically on the Group's systems as soon as possible;
- Changed to information records should be dated and communicated via internal Update procedures;
- Irrelevant or unneeded Personal Information should be deleted or destroyed;
- Personal Information must be filed correctly on system.

8.6. Openness

The Group 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 party.

8.7. Data Subject Participation

Data Subject have the right to request access to, amendment, or deletion of their Personal Information as set out in Section 4 in this document. Unless there are grounds for refusal as set out in paragraph 6.2, above, the Group 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

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

8.8. Security Safeguards

The Group 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;

8.8.1. 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;
- The Group shall implement and maintain a "Clean Desk Policy" where all employees shall be required to clear their desks of all Personal Information when leaving their desks for any extended length of time and at the end of the day;
- Personal Information which is no longer required should be disposed of by utilising The Group's secure document destruction boxes, only once the information has been verified as correctly stored electronically, or by Management verification that the information is no longer required.
- Any loss or theft of, or unauthorised access to Personal Information must be immediately reported to the Information Officer;
- No unattended guests or contractors shall be allowed past the Reception space in the Ambiton building.

8.8.2. Electronic Records

- All electronically held Personal Information must be saved the Group's secure IT Systems;
- As far as reasonably practicable, no Personal Information to be saved on individual computers, laptops, hand-held devices, or personal cloud storage accounts;
- All computers, laptops and hand-held devices are access protected with a password, fingerprint or retina scan, with the password being of reasonable complexity and changed frequently, as well as encryption;
- The Group requires a "Clean Screen Policy" where all 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;
- Electronic Personal Information which is no longer required must be deleted from the individual laptop or computer and the relevant database, where prescribed retention periods of applicable Legislation permits such deletion. The employee must ensure that the information has been completely deleted and is not recoverable.
- Any loss or theft of, or unauthorised access to, Personal Information must be immediately reported to the Information Officer;

- 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 Executive Team, and shall take all necessary steps to remotely delete the information, if possible.

7. DIRECT MARKETING

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

7.1.1. Existing Customers

Direct Marketing by electronic means to existing customers is only permitted:

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

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

However, receipt of contractual communication cannot be "opted out" as the information is relevant and specific to fulfilling the client's contractual obligations to their applicable product supplier. Such information is not considered Direct Marketing and is critical to The Group discharging it's Legislated obligations.

7.1.2. Consent

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

7.1.3. Record Keeping

The Group 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

8. DESTRUCTION OF DOCUMENTS

- Documents may be destroyed after the termination of the retention period specified herein, or as determined by the Company from time to time.
- Each department is responsible for attending to the destruction of its documents and electronic records, which must be done on a regular basis. Files must be checked in order to make sure that they may be destroyed and also to ascertain if there are important original documents in the file. Original documents must be returned to the holder thereof, failing which, they should be retained by the Company pending such return, unless electronic retention is legally permissible.
- The documents must made available for collection by the Group's approved document disposal company.
- 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.

9. STATUTORY RETENTION PERIODS

Where records are applicable across multiple Legislative retention periods, the record will be subject to the most stringent of the Legislative requirements.

Legislation	Document Type	Period
Companies Act	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.	7 Years or longer if specified in other public regulation
	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.	Indefinitely
Consumer Protection Act	Information provided to a consumer by an intermediary: 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 or 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 intermediary to the consumer A person who conducts a promotional competition must retain: full details, including identity or registration numbers addresses and contact numbers of the promoter; rules of promotional competition; copy of offer to participate in promotional competition; names and identity numbers of persons responsible for conducting the promotional competition; full list of prizes offered in promotional competition; a representative selection of materials marketing the promotional competition; list of all instances when the promotional competition was marketed, including dates, medium used and places where marketing took place; names and identity numbers of persons responsible for conducting the selection of prize winners in the promotional competition; acknowledgement of receipt, identity number and the date of receipt of the prize by the prize winner; declarations or affirmation that prize winners are not employees, directors, agents, or consultants who directly or indirectly controls or is controlled by the promoter or marketing service provider in respect f the promotional competition, or the spouses, life partners, business partners or immediate family members; basis of determining the prize winners; summary describing the proceedings to determine the winners; whether an independent person oversaw the determination of the prize winners; the means by which the prize winners were announced and frequency; list of names and identity numbers of prize winners; list of dates when prizes were handed over to the prize winners; steps taken by the	3 years

	promoter to contact the winner; reasons for prize winner not receiving or accepting the prize and steps taken by promoter to hand over the prize	
Financial Intelligence Centre Act, Financial Advisory and Intermediary Services Act, and the General Code of Conduct	An authorised financial services provider must maintain the following records regarding known premature cancellations of transactions or financial products by clients of the provider; complaints received together with an indication whether or not any such complaint has been resolved; the continued compliance with the requirements referred to in section 8; cases of non-compliance with this Act, and the reasons for such non-compliance; the continued compliance by representatives with the requirements referred to in section 13(1) and (2). A provider must have appropriate procedures and systems in place to record such 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 service rendered to the client; 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. Providers are not required to keep the records themselves but must ensure that they are available for inspection within seven days of the registrar's request. Records may be kept in an appropriate electronic or recorded format, which are accessible and readily reducible to written or printed form. Whenever an accountable institution establishes a business relationship or concludes a transaction with a client, the accountable 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 other person and that other person's authority to act on behalf of the client and the manner in which the identity of the persons referred to above was established, the nature of that business relationship or transaction, the amount involved, and the parties to that transaction; All accounts that are involved in 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, and any document or copy of a document obtained by the accountable institution; The records may be kept in electronic format.	5 years from date of termination of the business relationship or single transaction
Occupational Health and Safety Act	A health and safety committee shall keep record of each recommendation 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.	3 years
Compensation for Occupational Injuries and Diseases Act	Register, record or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees.	4 years
Basic Conditions of Employment Act	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; Date of birth of any employee under the age of 18 years.	3 years

Unemployment Insurance Act	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	5 years from date of EMP201 submission
Tax Administration Act	Section 29 documents which: • 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	5 years, but indefinite for returns outstanding then additional 5 years
Income Tax Act	In respect of each employee the employer shall keep a record showing 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.	5 years from date of EMP201 submission
Value Added Tax Act	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.	5 years from the date of submission of the return

10. SCHEDULE OF FEES

The schedule of fees in respect of access to information is governed by the Information Regulator:

Fees in Respect of Private Bodies

Item	Description	Amount
1.	The request fee payable by every requester	R140.00
2.	Photocopy/printed black & white copy of A4-size page	R2.00 per page or part thereof.
3.	Printed copy of A4-size page	R2.00 per page or part thereof.
4.	For a copy in a computer-readable form on: (iii) Flash drive (to be provided by requestor) (iv) Compact disc • If provided by requestor • If provided to the requestor	 R40.00 R40.00 R60.00
5.	For a transcription of visual images per A4-size page	Service to be outsourced. Will depend on quotation from Service provider.
6.	Copy of visual images	
7.	Transcription of an audio record, per A4-size page	R24.00
8.	Copy of an audio record on: (v) Flash drive (to be provided by requestor) (vi) Compact disc • If provided by requestor • If provided to the requestor	 R40.00 R40.00 R60.00
9.	To search for and prepare the record for disclosure for each hour or part of an hour, excluding the first hour, reasonably required for such search and preparation. To not exceed a total cost of	R145.00 R435.00
10.	Deposit: If search exceeds 6 hours	One third of amount per request calculated in terms of items 2 to 8.
11.	Postage, e-mail or any other electronic transfer	Actual expense, if any.".

11. FORMS TO REQUEST INFORMATION

Forms relating to the various requests are available from the Information Regulator's website on:

https://www.inforegulator.org.za/docs2-f.html

or on request from the Information Officer.