POLICY COMPLIANCE MANUAL
FOR PROTECTION OF PERSONAL INFORMATION ACT OF 2013
FOR
AMFI AGENCIES CC t/a AMF FREIGHT INTERNATIONAL and all its BRANCHES
(Hereinafter referred to as AMFI)

1. INTRODUCTION

The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 ('POPIA")

POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner.

AMFI is a company operating within the Transport/Clearing and Forwarding Industry that is obligated to comply with the POPI Act. Through the provision of services, AMFI is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees and other stakeholders.

Given the importance of privacy, AMFI guarantees its commitment to protecting the privacy of all its stakeholders, and as such undertakes to ensure that their personal information is used appropriately, transparently, securely and in accordance with POPIA's provisions.

This Policy sets out the framework for our company's compliance with the POPI act, and will be made available on the AMFI website at www.amfi.co.za and by requesting it from AMFI's head office.

2. DEFINITIONS

2.1 Personal Information

Personal Information is any information that can be used to reveal a person's identity. Personal Information relates to an identifiable, living, natural person and where applicable, an identifiable existing juristic person (such as a company) including, but not limited to information concerning:

- Race, gender, 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 that 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 that person
- The name of the person if it appears with the other personal information relating to the person or if the disclosure of the name itself will reveal information about the person

2.2 Data Subject

This refers to the person to whom the personal information relates.

2.3 Responsible Party

This is the entity that needs the personal information for a particular reason and determines the purpose of and means of processing the personal information. In this case, the organisation is the responsible party.

2.4 Operator

This means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under direct authority of that party.

2.5 Information Officer

The Information Officer is responsible for ensuring the organisation's compliance with POPI.

2.6 Processing

The act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes:

- The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

- Dissemination by means of transmission, distribution or making available in any other form or;
- Merging, linking as well as any restriction, degradation, erasure or destruction of information.

2.7 Record

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, marketing or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
- Book, map, plan, graph or drawing
- Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced.

2.8 Consent

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

3. PURPOSE

The purpose of this policy is to protect AMFI from compliance risks associated with the protection of personal information which includes:

- Breaches of confidentiality.
- Failure to offer choice
- Reputational damage

The policy demonstrates AMFI's commitment to protecting the privacy rights of data subjects in the following manner:

- Through stating desired behaviour and directing compliance with the provisions of POPI and best practice
- By cultivating an organisational culture that recognises privacy as a valuable human right
- By developing and implementing internal controls for the purposes of managing the compliance risk associated with the protection of personal information.

- By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of AMFI.
- By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer
- By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

4. ORGANISATIONAL SCOPE

This policy and its guiding principles applies to:

- AMFI's governing body
- All branches, business units and divisions of AMFI
- All employees and volunteers
- All contactors, suppliers and other persons acting on behalf of AMFI

5. RIGHTS OF DATA SUBJECTS

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

5.1 The rights to access Personal Information
5.2 The right to have Personal Information corrected or deleted
5.3 The right to object to the processing of Personal Information
5.4 The right to object to Direct Marketing
5.5 The right to complain to the Information Regulator
5.6 The right to be informed

6. GENERAL GUIDING PRINCIPLES

All employees and persons acting on behalf of AMFI will at all times be subject to, and act in accordance with, the following guiding principles:

6.1 Accountability

Failing to comply with POPI could potentially damage AMFI's reputation or expose the organisation to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

AMFI will ensure that the provisions of POPI and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, AMFI will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/ or omissions fail to comply with the principles and responsibilities outlined in this policy.

6.2 Processing Limitations

AMFI will ensure that personal information under its control is processed:

- In a fair, lawful and non-excessive manner
- Only with the informed consent of the data subject
- Only for a specifically defined purpose

AMFI will inform the data subject of the reasons for collecting the personal information and obtain written consent prior to processing personal information.

AMFI will under no circumstances distribute or share personal information between separate legal entities, associated organisations or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other aspects of the organisation's business and be provided with the reasons for doing so.

6.3 Purpose specification

Personal information must be collected for a specific, explicitly defined and lawful purpose related to the function or activity of the responsible party. Where necessary, AMFI will inform data subjects of these reasons prior to collecting or recording the data subject's personal information.

6.4 Further Processing limitation

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose. AMFI will obtain additional consent from the data subject if it intends to process the information for a secondary purpose.

6.5 Information Quality

AMFI will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading. Personal Information must be updated where necessary.

6.6 Open Communication

AMFI 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.

AMFI will ensure that it establishes and maintains a 'contact us' facility, for instance via its website, for data subjects who want to:

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

Where applicable, AMFI will provide a platform to unsubscribe from any of its electronic newsletters or related marketing activities.

6.7 Security safeguards

AMFI will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.

Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information the greater the security required.

AMFI will continuously review the security controls which include regular testing of protocols and measures put in place to combat cyber-attacks on the organisation's IT Network.

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

The personal information of clients and staff must be destroyed timeously in a manner that de-identifies the person.

Our business premises where records are kept must remain protected by access control, burglar alarms and armed response.

All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which the organisation is responsible.

All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses.

The digital work profiles and privileges of staff who have left our employ must be properly terminated.

AMFI's third party service providers will be required to enter into service level agreements with the organisation where both parties pledge their mutual commitment to POPI and the lawful processing of any personal information pursuant to the agreement.
Our current debtor and client information is stored on site by a Third party service Provider, whose premises our AMFI Compliance officer has toured and with whom AMFI has a Service Level Agreement in place with.

AMFI captures all files electronically for back up purposes, and all files will be archived at the AMFI disaster site which will be available in case of a breach.

All electronic files or data are backed up by the AMFI IT Service Provider who is also responsible for system security which protects against third party access and physical threats.

NETWORK CONFIG is the third party service provider who are responsible for Electronic Information security.

6.8 Security Breaches

Should it appear that the personal information of a client has been accessed or acquired by an unauthorised person, AMFI must notify the Information Regulator and the relevant clients, unless the client can no longer be identified. This notification must take place as soon as reasonably possible.

Such notification must be given to the Information Regulator first as it is possible that they or another public body, might required the notification to the client be delayed.

The notification to the client must be communicated in writing in one of the following ways, with a view to ensuring that the notification reaches the client:

1. By mail to the client's last known physical or postal address
2. By email to the client's last known email address
3. By publication on AMFI website or in the news media; or
4. As directed by the Information Regulator

This notification to the client must give sufficient information to enable the client to protect themselves against the potential consequences of the security breach, and must include:

1. A description of the possible consequences of the breach
2. Details of the measures that AMFI intends to take or have taken to address the breach
3. The recommendation of what the client could do to mitigate the adverse effects of the breach; and

4. If known, the identity of the person who may have accessed or acquired the personal information.

A Security Incident Management Register will be kept to log any security incidents and to report on and manage said incidents. This register will be maintained by an Appointed Representative.

Consent to process debtor information is obtained from clients (or a person who has been given authorisation from the client to provide their Personal Information) during the introductory, appointment and needs analysis stage of the relationship.

7. INFORMATION OFFICER RESPONSIBILITIES

The core focus or duties under the POPIA for the Information Officer will be the following but not limited to:

- Encourage compliance with the information protection conditions in terms of Section 55 of POPIA
- Developing, publishing and maintaining a POPIA policy which address all relevant provisions of the POPI Act
- Reviewing the POPI Act and updates as published
- Ensuring that periodic communication awareness of the POPI Act responsibilities takes place
- Ensuring that POPI Act awareness training takes place for all staff and that all employees and other persons acting on behalf of AMFI are fully aware of the risks associated with the processing of personal information and that they remain informed about AMFI's security controls
- Continually analysing privacy regulations and aligning them with the organisation's personal information processing procedures. Ensuring that Privacy notices are developed and published
- Addressing all POPI related requests and complaints made by AMFI's data subjects and ensuring that AMFI makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the organisation. For instance, maintaining a "contact us" facility on the website
- Create and implement procedures to facilitate customer verification of captured and store personal information
- Approving unusual or controversial disclosures of personal data
- Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the organisation. This will include the amendment of AMFI's employment contracts and other service level agreements

- Monitor and control the privacy requirements and responsibilities or information processing service providers or operators in terms of section 20 and 21 of POPIA
- Work with the Regulator in relation to investigations conducted pursuant to Chapter 6 against us
- Identify and govern all privacy related risks and map all privacy laws and industry codes relevant to our activities
- Identify all activities performed concerning the collection and storage of personal information
- If applicable, know, understand and ensure corporate compliance with all relevant laws of foreign jurisdictions in which we conduct business
- Liaise with Human Resources or external consultants and legal consultants to ensure standards of disciplinary action and sanction for non-compliance
- Liaise with Public Relations and Marketing departments to create public information communications and procedures on POPI related issues and breaches
- Create scripts for responding to customer or public enquiries
- Create and implement a Privacy Breach management plan, privacy alerts and other privacy related operational issues, and manage breach and incident investigation processes
- Ensuring that POPIA audits are scheduled and conducted on a regular basis

8. EMPLOYEE RESPONSIBILITIES

Employees and other persons acting on behalf of AMFI will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other employees.

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

Employees and other persons acting on behalf of AMFI may not directly or indirectly utilise, disclose or make public in any manner to any person or third party, either within AMFI or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the employee or person to perform his or her duties.

Employees and other persons acting on behalf of AMFI must request access from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

Employees and other persons acting on behalf of AMFI will only process personal information where:

- The data subject, or a competent person where the data subject is a child, consents to the processing;

- The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party;
- The processing complies with an obligation imposed by law on the responsible party;
- The processing protects a legitimate interest of the data subject
- The processing is necessary for pursuing the legitimate interests of the organisation or of a third party to whom the information is supplied

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

- Clearly understands why and for what purpose his, her or its personal information is being collected
- Has granted the organisation with explicit written or verbally recorded consent to process his, her or its personal information

Consent to process a data subject's personal information will be obtained directly from the data subject except where:

- The personal information has been made public
- Where valid consent has been given to a third party
- The information is necessary for effective law enforcement

Employees or other persons acting on behalf of AMFI will under no circumstances:

- Process or have access to personal information where such processing or access is not a requirement to perform their respective work related tasks or duties
- Save copies of personal information directly to but not limited to their own private computers, laptops , mobile devices, cloud based drives/storage, or forward such personal information to private email accounts. All personal information must be accessed and updated from the organisation's central database or a dedicated server
- Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant line manager or Information Officer
- Transfer personal information outside of South Africa without the express permission from the Information Officer

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

- Keeping all personal information that they come into contact with secure, but taking sensible precautions and following the guidelines outlined within this policy
- Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.
- Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT service provider will assist AMFI with the sending and 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 computer screens and other devices are switched off or locked when not in use or when away from their desks.
- Ensuring that where personal information is stored on removable storage medias such as external drives, CDs or DVDs that these are kept locked away securely when not being used.
- Ensuring there 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.
- Taking reasonable steps to ensure that personal information is kept accurate and up to date. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.
- Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.
- Undergoing POPI Awareness training from time to time

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

9. REQUEST TO ACCESS PERSONAL INFORMATION

Access to information requests can be made by email, addressed to the Information Officer. The Information Officer will provide the date 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 will be processed and considered against the POPI policy. The Information Officer will process all requests within a reasonable time.

10. TRANSBORDER INFORMATION FLOWS

AMFI may not transfer a client's personal information to a third party in a foreign country, unless:

1. The client consents to this or request it; or
2. Such third party is subject to a law, binding corporate rules or a binding agreement which protects the personal information in a manner similar to POPI and such third party is governed by similar rules which prohibit the onward transfer of personal information to a third party in another country; or
3. The transfer or the personal information is required for the performance of the contact between AMFI and the client; or
4. The transfer is necessary for the conclusion or performance of a contract for the benefit of the client entered into between AMFI and the third party; or
5. The transfer of the personal information is for the benefit of the client and it is not reasonably possible to obtain their consent and that if it were possible, the client would like to give such consent

11. DETAILS OF INFORMATION OFFICER

Alternatively

NAME:	SEAN KING
TELEPHONE NUMBER:	031-563 3049
FAX NUMBER:	031-563 3049
POSTAL ADDRESS:	3 ENNISDALE DRIVE, DURBAN NORTH, 4051
PHYSICAL ADDRESS:	3 ENNISDALE DRIVE, DURBAN NORTH, 4051
EMAIL:	sean@amfi.co.za