TSHEDZA COMPLIANCE PRACTICE

POPIA POLICY

1. DEFINITIONS

1.1. **DATA SUBJECT** means the person to whom personal information relates to.

1.2. **POPIA** refers to the Protection of Personal Information Act 4 of 2013.

1.3. **PROCESSING** means any operation or activity or any set of operations, whether by automatic means, concerning personal information, including:

a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use.
b) dissemination by means of transmission, distribution or making available in any other form; or
c) merging, linking, as well as restriction, degradation, erasure, or destruction of information.

1.4. **RECORD** means any recorded information-

a) regardless of form or medium, including any of the following.

I. writing of any material.
II. 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.
III. label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means.
IV. book, map, plan, graph, or drawing.
V. photograph, film, negative, tape or other device in which one or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced.

b) in the possession or under the control of a responsible party.
c) whether or not it was created by a responsible party; and
d) regardless of when it came into existence.

1.5. **RESPONSIBLE PARTY** means a public or private body or any other person which, alone or in conjunction with others determines the purpose of and means for processing personal information.

1.6. **PERSONAL INFORMATION** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, colour, sexual orientation, age, physical or mental health, wellbeing, disability, religion, conscience, belief, culture, language, and birth of the person.
b) information relating to the education or the medical, financial, criminal or employment history of the person.

c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier, or other assignment to the person.
d) the biometric information of the person.
e) the personal opinions, views, or preferences of the person.
f) 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.
g) the views or opinions of another individual about the person and,
h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

1.7 **INFORMATION OFFICER** means the person who is responsible for ensuring Tshedza CP' compliance with POPI Act.

2. PURPOSE

2.1 The primary purpose of this policy is to provide guidance to Employees and temporary Employees with regards to requirements and guidelines of processing and storing data subject's personal information.

2.2 Management will therefore ensure that each employee carries out their duties in accordance with the guidelines and performs their duties in accordance with this policy and procedures of the Protection of Personal Information Act. Employees are to maintain and undertake their duties and instructions in line with the applicable South African Privacy Laws.

2.3 This document will therefore be of assistance in regulating the primary functionalities of balancing the right to privacy and the right to access of information. This policy will further assist employees to establish and understand the conditions that must be adhered to when processing and storing client's personal information.

2.4 This document will further assist employees to help remedy any errors or mistakes that are made when processing personal information that is not in accordance with the Act.

3. SCOPE AND OBJECTIVE OF THE POLICY

3.1 This policy is applicable to all Employees of Tshedza CP, including all Fixed Term- and / or temporary Employees, contractors, suppliers, and any persons acting on behalf of the Tshedza CP.

3.2 They abovementioned personnel are required to familiarise themselves with the policy's requirements and undertake to comply with the stated processes and procedures.

4. RIGHTS OF DATA SUBJECTS

4.1 A Data subject has the right to have his / her / its personal information processed in accordance with the conditions for lawfully processing or personal information which includes the right to:

a) Being notified when personal information is collected and when his / her / its personal information has been accessed or acquired by an unauthorised person.
b) To establish whether a responsible party holds personal information of a specific data subject and to request access to his / her / its personal information.
c) To request, where necessary, the correction, destruction, or deletion of his / her / its personal information.
d) To object, on reasonable grounds that relate to his / her / its situation to the procession of his / her / its personal information that has been provided.
e) To object to the processing of his / her or its personal information being used for:
f) Purposes of direct marketing; or
g) Direct marketing by means of unsolicited electronic communications.
h) To not have his, her or its personal information for purposes of direct marketing by means on unsolicited electronic communications.
i) To not be subject, under certain circumstance, to a decision which is based solely based on the automated processing of his, her or its personal information intended to provide a profile of such person.
j) To submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of any data subject or to submit a complaint to the Regulator in respect of a determination of an adjudicator as provided for in the Act.
k) To institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information.

4.2 Should an employee of Tshedza CP be requested access to their personal information, such request should be made on a Personal Information Request Form which is attached hereto marked as Annexure “A”.

5. CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

All employees and persons acting on behalf of Tshedza CP will always be subject to, and act in accordance with, the following guiding principles:

ACCOUNTABLITY

- Tshedza CP’ employees are to ensure that personal information is lawfully processed in accordance with POPI Act at all times.

- As the responsible party, Tshedza CP is required to audit the processes used to collect, record, store, disseminate and destroy personal information.
- Tshedza CP is to ensure the integrity and safekeeping of personal information that is in its possession or under its control.
- Tshedza CP is to take steps to prevent date subject's information from being lost, damaged, or unlawfully accessed.
- All employees of Tshedza CP must ensure that all processing conditions under this heading are complied with when determining the purpose and means of processing Personal Information.

PROCESSING LIMITATION

Lawfulness of processing:

a) Personal information must be processed lawfully and in a reasonable manner that does not infringe the privacy of the date subject.
b) Processing is deemed to be lawful only if it is given a purpose for processing, the information obtained in adequate, that the information obtaining is relevant and not excessive.
c) Personal Information may only be processed by Tshedza CP if one of the following grounds of lawful processing exists:
    i. The Data Subject consents to the processing.
    ii. Processing is necessary for the conclusion or performance of a contract (fee and mandate agreement) with the Data Subject.
    iii. Processing complies with a legal responsibility imposed on Tshedza CP.
    iv. Processing protects a legitimate interest of the Data Subject.
    v. Processing is necessary for pursuance of a legitimate interest of Tshedza CP or correspondent attorneys to whom the information is supplied too.
    vi. Data subject consent is not required if it would prejudice a lawful process or if the information is contained in a public record.

Special Personal Information includes:

a) Religious, philosophical, or political beliefs.
b) Race or ethnic origin.
c) Trade union membership.
d) Health or sex life.
e) Biometric information (including but not limited to blood type, fingerprints, DNA, retinal scanning, voice recognitions, photographs).
f) Criminal behaviour.
g) Information concerning a child.

Tshedza CP may only process Special Personal Information under the following circumstances:

a) The Data Subject has consented to such processing.
b) The Special Personal Information was deliberately made public by the Date Subject.
c) Processing is necessary for the establishment of a right or defence in law.
d) Processing is for historical, statistical or research reasons; and / or
e) If the processing of race or ethnic origin, is to comply with the 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. If the Data Subject withdraws consent or objects to processing then Tshedza CP, shall immediately refrain from processing the Personal Information.

PURPOSE SPECIFICATION

Personal Information must be collected for a specific, explicitly defined, and lawful purpose related to a function or activity that Tshedza CP renders.

Tshedza CP is to ensure that the Data Subjects are made aware of the purpose for which the collection of their Personal Information is for.

The purposes for collecting Data Subjects Personal Information must remain within the ambient of the following:

a) Administration of agreements.
b) Providing products and services to clients.
c) Detecting and prevention of fraud, crime, money laundering and other malpractices (FICA).
d) Conducting market and / customer satisfaction research.
e) Marketing and sales.
f) In connection with any legal proceedings.
g) Staff administration.
h) Keeping of accounts and records.
i) Complying with legal and regulatory requirements.
j) Obtaining Personal Information for bond registrations and transfers of properties; and / or

Retention and Restriction of Records:

a) Subject to the above and Annexure “B” of this policy, records of Personal Information must not be kept longer than is necessary for achieving the purpose for which the information was collected or subsequently processed.
b) Once the time periods have lapsed set out in Annexure “B”, Tshedza CP must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after Tshedza CP is no longer authorised to retain the record in terms of Annexure “B”.
c) Tshedza CP must ensure that the destruction or deletion of Personal Information must be done in a manner that prevents its reconstruction in an intelligible form.

FURTHER PROCESSING LIMITATION

a) Further processing of Personal Information must be in accordance with or compatible with the purpose for which it was collected in its specific purpose.
b) To assess if further processing is compatible with the purpose of collection, Tshedza CP must consider the following:
    i. The relationship between the purpose of the intended further processing and the purpose for which the information has been collected.
    ii. The nature of the information concerned.
    iii. The consequences of the intended further processing for the date subject.
    iv. The way the information has been collected; and
    v. Any contractual rights and obligations between the parties.
c) Further processing of Personal Information is not incompatible with the purpose of collection if:
    i. The Data Subject or a competent person where the Data Subject is a child has consented to the further processing of the information.
    ii. The information is available in or derived from a public record or has been deliberately made public by the data subject.
d) Further processing is necessary in the following instances:
    i. To avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution, and punishment of offences.
    ii. To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue.
    iii. For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or
    iv. Is the interest of national security.

INFORMATION QUALITY

10.1 Tshedza CP must take reasonable steps to ensure that the Personal Information obtained from Data Subjects is complete, accurate, not misleading and updated where necessary.

10.2 By taking the steps referred to in 9.1, Tshedza CP must have regard to the purpose for which Personal Information is collected or further processed.

10.3 Employees should as far as reasonably practicably follow the following guidance when collection Personal Information:

a) Personal Information should be dated when received.
b) A record should be kept of where the Personal Information was obtained.
c) Changes to information records should be dated.
d) Irrelevant or unneeded Personal Information should be deleted or destroyed.
e) Personal Information should be stored securely, either on a secure electronic database or in a secure physical filing system or both.

11. OPENNESS

11.1 Documentation

a) Employees must maintain the documentation of all processing operations under its responsibility as referred under retention and restriction of records.
b) Tshedza CP employees must take reasonable practical steps to ensure that the Data Subjects are aware of:
    i. The reason for which information is being collected and where the information is not collected from the data subject, the source from which it is collected.
    ii. The name and address of the Tshedza CP.
    iii. The purpose for which the information is being collected.
    iv. Whether or not the supply of the information by that data subject is voluntary or mandatory.
    v. The consequences of failure to provide the information.
    vi. Any law authorising or requiring the collection of the information.
    vii. The fact that, where applicable, the Tshedza CP intends to share the information to a third party or international organisation and the level of protection afforded to the information by that third party or international organisation.
    viii. That the Data Subject has the right to access or rectify the information collected.
    ix. That the Data Subject has the right to object to the processing of their Personal Information; and
    x. Tshedza CP has the obligation to inform the Data Subject that should they be unhappy in the way their Personal Information is being processed or stored that they have the right to lodge a complaint to the Information Regulator.

12. SECURITY SAFEGUARDS

12.1. Tshedza CP must ensure the integrity and confidentiality of all Personal Information in its possession, by taking reasonable steps to:

a) Identify all reasonably foreseeable risks to information security.
b) Implementing security controls to minimize the risk of loss, unauthorised access, disclosure, interference, modification, or destruction.
c) Security controls implemented should be context sensitive. This meaning that the more sensitive personal information is – the greater security is required.

12.2. Written records:

a) Personable Information records should be kept in areas that non-staff members have access to.
b) When in use, Personal Information records should not be left unattended in areas where non-staff members may access to.
c) Tshedza CP 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 length of time and at the end of the day.
d) Personal Information which is no longer required should be disposed by shredding.
e) All FICA documents must be uploaded onto Tshedza CP’ online portal and the hard copies must be stored away in a designated secure storage unit.
f) Any loss, theft or unauthorised access to Personal Information must be immediately reported to the Information Officer.

12.3. Electronic Records:

a) All electronically held Personal Information must be saved on an online portal.
b) As far as reasonably practical, no Personal Information should be saved on individual computers, laptops, or hand-held devices.
c) All computers, laptops and hand-held devices should be access protected with a password, fingerprint, retina scan or facial recognition, with the password being of reasonable complexity and changed monthly.
d) Tshedza CP shall implement a “Clean Screen Policy” where all employees shall be required to lock their computes or laptops when leaving their desks for any length of time and to log off at the end of each day.
e) Electronic Personal Information which is no longer required must be deleted from the individual laptop or computer and the relevant database. The employees must ensure that the information has been completely deleted and is not recoverable.
f) 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 will then take all the necessary steps to remotely delete the information, if possible.

g) Tshedza CP will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyberattacks on the IT network.

13. DATA SUBJECT PARTICIPATION

13.1 Data Subjects have the right to request access to, amendment or deletion of their Personal Information as per Annexure “A”.

13.2 All such requests must be submitted in writing to the Information Officer, unless there are grounds for refusal as set out in below, Tshedza CP shall disclose the requested Personal Information:

a) On receipt of adequate proof of identity from the Data Subject or requestor.

b) Within a reasonable time.

c) On receipt of the prescribed fee, if any.

d) In a reasonable format.

13.3 Personal Information shall not be disclosed to any party unless the identity of the requestor has been identified.

14. GENERAL DESCRIPTION OF INFORMATIONS SECURITY MEASURES

14.1 Tshedza CP employs up to date technology to ensure the confidentially, integrity and availability of the Personal Information under its case. These measures include:

a) Firewalls

b) virus protection software and updated protocol

c) Logical and physical access control

d) Outsourced Service Providers who process Personal Information on behalf of Tshedza CP are contracted to implement security controls.

15. ACCESS TO PERSONAL INFORMATION

15.1 All individuals and entities may request access, amendment or deletion of their own Personal Information held by Tshedza CP. Any requests should be directed, on the prescribed form to the Information Officer.

15.2 Remedies available if request for access to Personal Information is refused:

a) Internal Remedies: The Act does not provide any internal remedies should a request for Personal Information is made and is denied by the Information Officer. As such, the requestor must exercise external remedies at their disposal.

b) External Remedies: Should a requestor or third party be dissatisfied with the Information Officer's refusal to disclose information, may within 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.

15.3 An Information Officer may refuse the request to Personal Information on the following grounds:

a) Protecting Personal Information that Tshedza CP holds about a third party (who is a natural person) including a deceased person, from unreasonable disclosure.
b) Protecting commercial information that Tshedza CP holds about a third party or the "trade secrets" that could harm the commercial or financial interest of the organisation or the third party.
c) 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.
d) If disclosure of the record would endanger the life or physical safety of an individual.
e) If disclosure of the record would prejudice or impair the security or property or means of transport.
f) If disclosure of the record would prejudice or impart the protection of the safety of the public.
g) The record is privileged from production in legal proceedings unless the legal privilege has been waived.
h) Disclosure of the record (containing trade secrets, financial, commercial, or technical information) would hard the commercial or financial interest of Tshedza CP.
i) Disclosure of the record would put Tshedza CP, at a disadvantage in contractual or other negotiations or prejudice it in commercial competition.
j) The record is a computer programme, and
k) The record contains information about research being carried out or about to be carried out on behalf of a third party or Tshedza CP

15.4 Records that cannot be found or do not exist:

a) Should a Data Subject request Tshedza CP to search for a record and it is believed that the record does not exist or cannot be found, the requestor must be notified by way of affidavit or affirmation. Steps that were taken to try locating this record must be stated on the affidavit / affirmation.

16. IMPLEMENTATION GUIDELINES:

16.1 TRAINING AND DISSEMINATION OF INFORMATION

a) This Policy has been put in place throughout Tshedza CP. Training on the Policy and POPI will take place with all affected employees.
b) All new employees will be made aware of this policy or through training programmes of their responsibilities under the terms of the is Policy and POPI.
c) Modifications and updates to data protection and information sharing policies, legislation or guidelines will be brought to the attention of all staff.

16.2 EMPLOYEE CONTRACTS

a) Each new employee will sign an Employment Contract containing the relevant consent clauses for the use and storage of employee information and a confidentiality undertaking that the employee will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information that the employee deals with or oversees, however it is stored. Failure to comply will result in the necessary disciplinary action being taken against the contravening employee.
b) Each employee who is currently employed with Tshedza CP will sign an addendum to their Employment Contact containing the relevant consent clauses for the use and storage of employee information and a confidentiality undertaking that the employee will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information that the employee deals with or is in charge of, however it is stored. Failure to comply will result in the necessary disciplinary action being taken against the contravening employee.

17. DIRECT MARKETING

17.1 All Direct Marketing communications shall contain Tshedza CP details and an address or method for the customer to opt-out or receiving further marketing communication.

17.2 Existing Clients:

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

i. If the client's details were obtained in the context of a service; and

ii. For the purpose of marketing similar products or content.

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

17.3 Consent

Tshedza CP may send electronic Direct Marketing communication to Data Subjects who have consented to receiving it. Tshedza CP may approach a Data Subject for sent only once.

17.4 Record Keeping

Tshedza CP shall keep record of:

i. Date of consent.

ii. Wording of the consent.

iii. Who obtained the consent?

iv. Proof of opportunity to opt-out on each marketing contact.

v. Record of opt-outs.

18. INFORMATION OFFICER:

18.1 Tshedza CP has appointed Avhapfani Mathada whose details appears below as the Information Officer:

Name	**Avhapfani Mathada**
Contacts	**0725056737**
Email	**avhapfani@tshedzacp.co.za**

18.2 The Information Officer is responsible for ensuring compliance with POPI Act.

18.3 Tshedza CP may annually consider a change in the Information Officer and Deputy Officer.

18.4 The Information Officer will be issued with Guidance Notes on their duties and same can be accessed on request to the Information Officer.

18.5 The Information Officer is to attend to any complaints issued to him / her on the prescribed form.

19. INFORMATION TECHNOLOGY:

19.1 Tshedza CP must ensure that their IT department is responsible for:

a) Ensuring that the IT infrastructure, electronic filing system and any other devise used for processing personal information meet acceptable security standards.

b) ensuring that all electronically held personal information is kept only on designated drives and serves and are u-loaded only to approved cloud computing services.

c) Ensuring that all servers containing personal information are stored in a secure location, away from the general office space.

d) Ensuring that all back-ups containing personal information are protected from unauthorised access and malicious hacking attempts.

e) Ensuring that personal information being transmitted electronically is encrypted.

f) Performing regular IT audits to ensure that the security of the firm's hardware and software systems are functioning.

g) Performing regular IT audits to verify whether electronically stored personal information has been access or acquired by any unauthorised persons.

20. EMPLOYEES AND OTHER PERSONS ACTING ON BEHALF OF TSHEDZA CP:

20.1 All employees and other persons acting on behalf of Tshedza CP will, during the course of the scope and duties of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other employees.

20.2 Employees and other persons acting on behalf of Tshedza CP are required to treat Personal Information as a confidential business asset and to respect the privacy of data subjects.

20.3 Employees and other persons acting on behalf of Tshedza CP may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the firm 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.

20.4 Employees and other persons acting on behalf of Tshedza CP must request assistance from the Information Officer if they are unsure about any aspect related to the protection of a data subject's Personal Information.

20.5 Employees and other persons acting on behalf of Tshedza CP must always adhere to the 8 processing conditions of personal information and must always obtain consent from the Data Subject before processing / using or storing their Personal Information.

21. DESTRUCTION OF DOCUMENTS:

21.1 Documents may be destroyed after the termination of the retention period specified in Tshedza CP Record and Retention Policy or as determined by Tshedza CP from time to time.

21.2 Each department is responsible for attending to the destruction of its documents and electronic records, which must be done on regular basis. Files must be checked 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 Tshedza CP pending such return.

21.3 The documents must be shredded or use of another approved document disposal company.

21.4 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.

22. DISCIPLINARY ACTION:

22.1 Where a POPI Act compliant or investigation has been finalised, Tshedza CP may recommend any appropriate administrative, legal and / or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.

22.2 In the case of ignorance or minor negligence, Tshedza CP will undertake to provide further awareness training to the employees.

22.3 Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct which may result in summarily dismissal of the employee responsible,

22.4 Disciplinary procedures will commence where there is sufficient evidence to support an employee’s gross negligence.

23. TRANS BORDER FLOW OF INFORMATION

Tshedza CP may not transfer Personal Information about a data subject to a 3rd party in a foreign country unless certain requirements are met.