Protection of Personal Information Policy

Applicable to all brands, divisions, joint ventures, subsidiaries, suppliers, directors and employees of the Tsebo group

Message from Chief Executive's Office

The advent of the fourth industrial revolution has resulted in technologies which are rapidly transforming the connected economy in which we operate. Our employees, customers and suppliers are "always on" i.e., always connected to the internet, emails, and apps.

In addition, we offer services that result in our customers providing us their Personal Information (e.g., Visitor entrance process for Protection services). All these technologies result in data being processed and stored. Data has become the new currency according to many thought leaders. Many organisations ranked in the top 10 worldwide are indeed providers of data which demonstrates how valuable data has become in our world.

As a responsible corporate citizen, it is our duty to comply with data laws in the jurisdictions where we operate and believe our efforts to commit to the protection of Personal Information to be a foundation of trust in all our relationships.

Therefore, we must ensure the highest level of personal information protection and security in all we do, irrespective of whether the information belongs to the customer, the supplier, or the employee. Our Protection of Personal Information Policy will enable us to define and enforce standards that seek to ensure the confidentiality and security of such data. It also ensures that we align to the applicable laws. All our employees, regardless of seniority or rank are obliged to adhere to this Policy.

As the joint Chief Executive Officers, it is our duty to ensure that the rules and principles of protection of personal information at Tsebo are followed across the Group.

Tim Walters
Chief Executive Officer

Dr Chris Jardine
Chief Executive Officer

1. Introduction

The Tsebo Group (Tsebo) conducts business with integrity and has built its reputation on a foundation of trust as perceived by our stakeholders, especially our clients, shareholders, and employees. In this Policy, "Personal Information" means Personal Information ("PI") and Special Personal Information ("SPI") as defined in the Protection of Personal Information Act, 4 of 2013 ("POPIA"). PI and SPI will be used synonymously, and the requirements associated with PI also apply to SPI. As such Tsebo is committed to protecting the privacy of the PI and SPI which it processes in line with POPIA. This Policy must be read together with other relevant policies published on the Tsebo's intranet site, and all the relevant policies that apply to specific jurisdictions.

2. Management

Personal Information must be treated with the highest regard to legislation and internal governance and in order to effectively govern the protection of personal information we must define, document, communicate our policies, statement, notices and other management processes to regulate compliance and assign accountability for the management thereof.

3. Consent

Tsebo must obtain and document the voluntary, specific and informed consent for the processing of PI from the data subject or competent person where the data subject is a child.
Consent may be withdrawn at any time, provided that the lawfulness of the processing of Personal Information before such withdrawal or the processing of Personal Information in terms contractual or other legal requirements will not be affected.

4. Collection

Tsebo must collect PI directly from data subjects, and where lawful and reasonable may collect PI about data subjects from third parties and publicly available sources.

Tsebo may passively collect information from data subjects and store that information on server logs, including internet protocol addresses ("IP addresses"), browser type, operating system, device identifier, device model, software version, or mobile or ISP carrier information.

Tsebo also uses Cookies and other technologies to collect information about data subject's visit to the Tsebo websites, such as the date and time of visit, the information searched to find the Tsebo websites, or activity on the Tsebo websites. Cookies are small text files that may be stored on a data subjects' device when visiting Tsebo online service.

In some instances, Tsebo may collect or receive information about data subjects from other sources with which data subjects interact (e.g., Facebook), companies that are Tsebo partners, other entities within the Tsebo Group of companies or outside the Tsebo Group structure who work with or on behalf of Tsebo.

Tsebo may also use PI for reasons not described in this Policy where the reason is compatible with the purpose for which it was originally collected and where such use is lawful.

5. Lawful Processing

Tsebo must use Personal Information for a purpose consistent with the purpose for which it was collected and in a manner that is adequate, relevant, and not excessive in the way which it is processed. Tsebo must only process PI where it is lawful to do so. Tsebo must not process PI for a purpose which is incompatible with the purpose for which it was collected unless the data subject agreed to an alternative purpose or Tsebo is permitted in terms of national legislation of general application dealing primarily with the protection of Personal Information.

6. Information quality

Tsebo is dedicated to keep PI that is processed accurately and, where necessary, up to date. Tsebo must take reasonable steps to ensure we keep complete, accurate and not misleading information that is aligned to the purpose for which it was collected. It is the data subjects responsibility to ensure that the PI submitted to Tsebo is correct. Tsebo must act upon the instructions of its stakeholders in order to assist them in complying with this obligation.

7. Disclosure to Third Parties/Service Providers/Operators

Tsebo is an international organisation with offices and operations in various geographical locations. In order to ensure consistency in employment activities, maximize the quality and efficiency of its services and business operations, may share PI collected with various divisions, subsidiaries, joint ventures, shareholders, and other stakeholders that are not part of the Tsebo Group structure but work with or on behalf of Tsebo for the purpose stated above and in line with POPIA.

Disclosure must be subject to an agreement between Tsebo and the party whom it is disclosing Personal Information to, which contractually obliges the recipient of the PI to comply with strict confidentiality and obligations set out by the POPI Act.

Prior to sharing PI with a Third Party, Tsebo must conduct a due diligence questionnaire to assess the control environment of said Third Party to identify any possible risks posed by inadequate controls.

8. Cross Border Transfer

Tsebo may transfer PI outside the borders of South Africa, in which the PI was collected so that the recipient may process PI on its behalf. By consenting to Tsebo processing PI, data subjects also agree to secure cross border transfers, where applicable in accordance with the terms of this Policy and applicable data protection laws and regulations.

9. Storage and Retention

Personal Information must be stored and held securely. In this regard Tsebo must conduct regular audits regarding the safety and security of PI. For operational reasons, PI will be accessible to employees within Tsebo on a need-to-know basis. Tsebo must keep PI for as long as necessary for the purposes for which it is processed.

10. Disposal and Destruction

Personal Information which is no longer required must be securely archived and retained, with consideration for the format and retention period requirements relating to the data.

When PI is no longer required for the purposes for which it was collected or when the legal obligations for retention lapse, Tsebo must safely and securely destroy or delete PI in a manner that prevents reconstruction of the PI in an intelligible form.

11. Security Safeguards

Tsebo must take all necessary technical and organisational measures in order to prevent accidental or unlawful alteration or loss, or from unauthorized use, disclosure or access, in accordance with the IT Information Security Policy. Negligent loss or unauthorised disclosure of Personal information, or failure to report such events, may be subject to disciplinary action taken. In addition to the above, physical safeguards to prevent and detect unauthorised entry to premises where Personal Information may be stored or processed must be implemented.

12. Information Retrieval and Management

Records in all formats containing personal Information must be collected, processed, safely and securely stored, deleted and/or disposed of in accordance with Tsebo's records management and retention schedules and any associated principles and procedures in place from time to time.
All records of Personal Information must not be retained for periods longer than the periods permitted by the Retention Schedule unless there is a specific justifiable reason, and such retention is required for operational reasons.

13. Roles and Responsibilities

Roles and responsibilities must be documented for various stakeholder to ensure that appropriate controls are adopted, to actively promote good governance and ensure that the protection of personal information is effectively implemented across Tsebo.

14. Right to Access Personal Information

Tsebo recognises the rights of data subjects to access all the Personal Information that it may hold about them and its responsibility to enable data subjects to access their PI. To this end, the PAIA Manual explains how:

- Access requests must be submitted and acknowledged by Tsebo through the Personal Information Officer in writing
- Access to the requested information must be either granted or denied (depending on the rationale and / or nature of the request) in writing. Reasons for denying the data subject access to their PI must be provided to the data subject concerned based on appropriate and documented exceptions and / or legislation.

15. Correction of Personal Information

A data subject may, in the prescribed manner, request Tsebo to correct or delete Personal Information about them in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or destroy or delete a record of Personal Information about them that Tsebo is no longer authorised to retain.

16. Questions or concerns about this Policy

For any questions or comments about this Policy, please contact POPI@tsebo.com.

17. Policy Deviations

Deviations and / or risk acceptances to this Policy will only be considered in exceptional circumstances. Requests for deviations and / or risk acceptances must be made to the Personal Information Officer and must be processed in consultation with the Chief Information Officer, Group Audit and Risk Executive, Group Legal Officer and Group Compliance officer.

18. Management and Enforcement

In order to manage and monitor compliance with this Policy and associated procedures to address POPI related queries, complaints, disputes and breaches Tsebo must define, document, communicate and assign accountability for all POPI governance.

19. Other Policies and Documents

This Policy should be read in conjunction with other Group Policies such as the:

- Group Protection of Personal Information Policy Manual
- Group IT Information Security Policy
- Group Cyber Security Policy
- Group Protection of Personal Information Statement
- Group Protection of Employee Personal Information Notice
- as well as other related procedures.