Protection of Personal Information Policy Manual

Definitions

In order to understand the implications of this document and the objectives of POPIA, please take note of the following definitions as set out under POPIA:

- **''biometrics''** means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.
- **"consent"** means any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of Personal Information.
- **''data subject''** means the person to whom Personal Information relates.
- **"operator"** means a natural person or a juristic person who possess your/ a Data Subject's Personal Information on behalf of the Responsible Party.
- **"person''** means a natural person or a juristic person.
- **"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—
- **"Personal Information relating to Natural Persons"** means —
    - an identifiable, living, natural person:
    - names, any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier, or other particular assignment to the person;
    - visual images and information about expressions of opinion, 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.
- **"Special Personal Information relating to Natural Persons"** means —
    - information relating to the religious or philosophical beliefs, trade union membership, political persuasion or biometric information;
    - the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, culture, language and birth of the person;
    - information relating to the education or the medical, financial, criminal or employment history of the person; and
    - information about a child.

- **"processing"** means any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information, including—
    - 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
    - merging, linking, as well as restriction, degradation, erasure or destruction of information; and
    - sharing with, transfer and further processing, to and with such information.
- **"record"** means any recorded information —
    - Regardless of form or medium, including any of the following:
        - 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, marking or other writing that identifies or describes any thing 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 produced
    - In the possession or under the control of a responsible party
    - Whether or not it was created by a responsible party; and
    - Regardless of when it came into existence.
- **"Responsible Party"** means the person, legal entity, company, or public body that processes another's Personal Information.

1. Introduction

Thorburn Security Solutions (Thorburn) 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, your "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 Thorburn 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 Thorburn'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. In order to effectively govern data protection, we must define, document, communicate our policies, and notices along with other management processes to regulate our compliance while assigning accountability for the management thereof as follows:

2.1 Protection of Personal Information Policy

This Policy must be reviewed and communicated annually to all employees, and subject to annual acknowledgement.

2.2 Protection of Personal Information (POPI) Statement

The Thorburn POPI Statement must be made available to all stakeholders via our website, outlining how we manage and processes Personal Information as well as how to contact us to access Personal Information.

2.3 Employee Protection of Personal Information Notice

All employees must be informed of how we collect, use and protect their PI and SPI including their rights and how to enforce those rights.

2.4 Risk Assessment Process

A Protection of Personal Information Risk Assessment process must be embedded into existing risk management processes in order to periodically identify the risks to the protection of Personal Information and be inclusive of the relevant controls and response strategies to mitigate both internal and external risks.

2.5 Protection of Personal Information Incident Response Plan

In addition to our existing Incident Response Plan, we must define, document and communicate a Protection of Personal Information Incident Response Plan to all employees and relevant stakeholders to manage related incidents as soon as they have been identified.

2.6 Protection of Personal Information Impact Assessments

Impact Assessments have been conducted across Thorburn to establish the PI Impact within the various divisions and departments. Going forward, Impact Assessments must be completed to assess the potential PI impact when new processes, products, services and systems involving personal information are implemented as well as when enhancements and/or amendments are made to such processes, products, services and systems.

2.7 Management of Third Parties

Prior to sharing PI with a Third Party, the third party must be risk ranked in accordance with the parameters defined by Group Risk and Group Compliance and agreed with the Chief Information Officer. A Third Party Due Diligence Questionnaire must be conducted and where applicable, appropriate remediation against controls must be agreed with the Third Party and tracked to completion.

All Third Parties who process PI must do so under a written contractual arrangement which will include obligations on the Third Party in terms of the Protection of Personal Information Act.

2.8 Protection of Personal Information Awareness

Awareness to our Protection of Personal Information Policy and processes must receive an ongoing focus and compulsory training must be provided to all employees.

2.9 Personal Information Champions

Each Division and every department must nominate specific individuals who will act as point of contact into their area, bring relevant matters to the attention of employees in their area as well as be mandated to escalate issues and/incidents to the Personal Information Officer and participate in Protection of Personal Information Awareness Campaigns and initiatives.

3. Consent

Thorburn 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.

Thorburn must:

- Document and manage changes to the data subject's consent preferences.
- Ensure that the data subject's preferences are implemented in a timely manner.
- Address conflicts in the records about the data subject's preferences by providing a process which ensures that preferences are consistently applied by Thorburn and its Third Parties, is in accordance with the data subject's preferences.

4. Collection

We collect PI directly from you, and where lawful and reasonable, we may collect PI about you from third parties and publicly available sources.

When you visit the Thorburn websites or interact with e-mails that we send to you, we may passively collect information from you and store that information on our server logs, including your internet protocol address ("IP address"), browser type, operating system, device identifier, device model, software version, or mobile or ISP carrier information.

Like many other websites or internet service providers ("ISP") we also use Cookies and other technologies to collect information about your visit to the Thorburn websites, such as the date and time of your visit, the information you searched to find the Thorburn websites, or your activity on the Thorburn websites. Cookies are small text files that may be stored on your device when visiting our online service.

In some instances, we may collect or receive information about you from other sources with which you interact (e.g., Facebook), companies that are our partners, other entities within Thorburn or outside the Thorburn company structure who work with or on behalf of Thorburn to update or supplement the information that you provide or that we collect automatically. We may use this information to help us maintain the accuracy of the information we collect, to target our communications so that we can inform you of products and services that we believe may be of interest to you, and for internal business analysis or other business purposes.

We also may use PI about you for reasons not described in this Policy where the reason is compatible with the purpose for which we originally collected your PI and where such use is lawful.

5. Lawful Processing

We use your PI 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. Thorburn will only process your Personal Information where it is lawful to do so. We will not process your PI for a purpose which is incompatible with the purpose for which it was collected unless you have agreed to an alternative purpose or Thorburn is permitted in terms of national legislation of general application dealing primarily with the protection of Personal Information.

We might process your PI for the below listed purposes:

- Recruitment, in line with our HR minimum standard of recruitment of the best people;
- For providing you with our services and products according to agreed terms and as per your request, hence for the purpose of allowing the commercial terms to be executed between parties and to enable you to have a good customer experience;

- For maintaining our contractual and business relationship with our customers and/or vendors, including the maintenance of contractual relationships with our customers and vendors and their representatives thereto during the delivery and execution of a commercial engagement;
- For facilitating our communication with you to ensure business continuity, including for providing you with necessary information, references and recommendations about our services and products;
- For monitoring your use of our systems to enable us to personalize your experience on our websites and webpages (including monitoring the use of our website and any apps and tools you use);
- For improving the security and functioning of our websites, webpages, networks and information, to ensure that you receive an excellent user experience whilst our networks and information are secure;
- For provisioning you with tailored newsletters and/or notifications, including relevant press releases to help you stay up to date with our products and services;
- For conducting and managing anti-bribery and anti-corruption, checks, to assess and address risk management to avoid non-compliance, setbacks of our business and protecting of our reputation;
- Apply analytics to business operations and data to describe, predict and improve business performance within our tool and/or to provide a better user experience. Specifically, areas within analytics include descriptive analytics, predictive analytics, analytics involving individuals (i.e. clients) use PI, analytics driven by marketing, single customer view and customer journey, talent/employee management analytics, for ensuring the proper functioning of our business operations;
- Marketing our products and services to you, unless you objected against such processing, so that we can ensure that we can conduct and increase our business.

6. Information quality

Thorburn is dedicated to keep PI that is processed accurately and, where necessary, up to date. Thorburn will 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 your responsibility to ensure that the PI submitted to Thorburn is correct. Thorburn will act upon the instructions of its clients in order to assist them in complying with this obligation. To the extent required by law, you may:

- have the right to access certain PI we maintain about you;
- request that we update or correct inaccuracies in PI we have;
- object to or restrict our use of your PI; and
- ask us to delete your PI from our database.

7. Disclosure to Third Parties/Service Providers/Operators

Thorburn is an international organisation with offices and operations in various geographical locations. In order to ensure consistency in our employment activities, maximize the quality and efficiency of our services and our business operations, we may share your PI collected by us with various divisions, subsidiaries, joint ventures, shareholders and other stakeholders that are not part of the Thorburn structure but work with or on behalf of Thorburn for the purpose stated above and in line with POPIA. We will not share your PI save for above unless:

- The law requires it;
- The law permits us to do so;
- To defend the interests, rights or property of Thorburn or related third parties; or
- You agree that we may disclose your information.

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

Prior to sharing your PI with a Third Party, Thorburn will 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

We may transfer your PI outside the borders of South Africa, in which we collected your PI so that the recipient may process PI on our behalf. By providing Thorburn with your PI, you agree to us doing so in accordance with the terms of this Policy and applicable data protection laws and regulations.

Cross border transfer of PI may only take place once the information has been afforded adequate protection from disclosure and unauthorised access in the country of destination.

While your Personal Information is in another country, it may be accessed by the courts, law enforcement and national security authorities in that country in accordance with its laws. In such

circumstances, the recipient of the PI will be bound contractually to a no lesser set of obligations than those imposed by POPIA.

9. Storage and Retention

Personal Information will be stored and held securely. In this regard we undertake to conduct regular audits regarding the safety and security of your PI. For operational reasons, PI will be accessible to employees within Thorburn on a need-to-know basis.

We only keep PI for as long as necessary for the purposes for which it is processed. PI is retained safely and securely under the following circumstances:

- We keep your PI as long as we have an ongoing relationship with you, in particular, if you have an account with us, are an employee of ours or a customer.
- We will only keep your PI for as long as needed to provide services to you.
- We will keep your PI for as long as necessary in order to comply with legal and contractual obligations.

10. Disposal and Destruction

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

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

11. Security Safeguards

We 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 our IT Information Security Policy.

All employees and where applicable, Third Parties, Service Providers, Operators and other persons acting on behalf of Thorburn must before processing Personal Information ensure that the data will be kept secure and that the appropriate measures and safeguards are in place to prevent unauthorised access, disclosure and/or loss of such Personal Information.

Personal Information must not be disclosed unlawfully to any third parties, service providers or operators. Transfers of Personal Information to third parties, must be authorised in writing by the

Functional Head/CEO and such information must be protected by adequate contractual provisions or data sharing/processor agreements.

All losses of Personal Information must be reported to the CEO and relevant Functional Head of the department where the information emanates, the relevant Personal Information Champion and the Personal Information Officer.

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 have been implemented.

The Personal Information Officer, Chief information officer and IT department will continuously review these controls and processes to ensure that all PI is secure.

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 Thorburn's records management and retention schedules and any associated principles and procedures in place from time to time.

All records must be authentic, reliable, useable, and capable of speedy and efficient retrieval.

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 reason, and such retention is required for operational reasons.

13.Roles and Responsibilities

13.1 Chief Executive Officer

The CEO will actively promote good governance and practices for the Protection of Personal Information and ensure that the Protection of Personal Information is effectively implemented across Thorburn.

13.2 Chief Information Officer

The CIO is responsible to ensure that all appropriate safeguards (technical, physical and organisational) are deployed and effectively monitored on an on-going basis across Thorburn.

13.3 Personal Information Officer

The PIO is primarily responsible for Thorburn's compliance with POPIA. This comprises:

- ensuring that Thorburn has a POPI compliance programme in place and that all employees, Operators, Third Parties/Service Providers, Contractors and Agents acting on behalf of Thorburn are aware of this Policy and their obligations in relation to the POPI compliance programme
- ensuring the POPI compliance framework is developed, implemented, monitored and maintained
- ensuring compliance with all legislation
- the co-ordination / facilitation of all POPI related breaches and incidents which may occur across Thorburn
- have oversight of designated Personal Information Champions
- dealing with requests made in relation to POPIA
- working with the Regulator on investigations
- ensuring Impact Assessments are done to guarantee that adequate measures and standards exist to comply with the conditions for the lawful processing
- ensuring a manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of PAIA
- ensuring that internal measures are developed together with adequate systems to process requests for information or access thereto
- ensuring that internal awareness sessions are conducted on POPIA, Regulations, Code of Conduct and information obtained from the Regulator
- The information officer shall upon request by any person, provide copies of the manual to that person upon the payment of a fee to be determined by the Regulator.

13.4 Tsebo Group IT Manager

Is responsible for:

- ensuring all systems, services, software and equipment meet acceptable security standards and are protected from internal and external security breaches
- Checking and scanning security hardware and software regularly to ensure they are functioning properly
- Researching third-party services, such as cloud services that the company may consider using to backup, store or process data

13.5 Tsebo Group Legal Officer

Group Legal is responsible for the provision of legal advice and support and to assist in the consistent definition of required POPI related clauses and / or terms and conditions for all written agreements.

13.6 Group Internal Audit

GIA is responsible for conducting independent audits and/or reviews to assess the level of adherence to controls implemented in order to operationalise the POPI requirements within business.

13.7 Group Compliance Officer

The Compliance function is responsible for ensuring a level of compliance to applicable legislation across Thorburn.

The GCO is also responsible for:

- Assisting and providing the required support in the investigations of privacy related breaches, queries, and complaints.
- ensuring that the appropriate processes are put in place in order to demonstrate compliance to this Policy.
- the on-going awareness and implementation of this Policy as well as all other associated policies and / or procedures.

13.8 Chief Sales & Marketing Officer

The Chief Sales and Marketing Officer is responsible for approving POPI statements attached to emails and other marketing copy. Addressing data protection queries from clients and media outlets as well as coordinating with the PIO and GCO to ensure all marketing initiatives adhere to this Policy.

13.9 CEO and Functional Heads of Department

The CEO and Functional Heads of Department are responsible for ensuring their employees and where applicable all Operators, Third Parties/Service Providers, contractors and agents acting on behalf of the Thorburn understand the role of the Protection of Personal Information conditions in their day-to-day work, through induction, training and performance monitoring, and for monitoring compliance within their own areas of responsibility.

13.10 Personal Information Champions

The CEO and Functional Heads of Department must ensure that Personal Information Champions are designated for their Departments and provided with the appropriate training and support. Personal Information Champions are required to:

- advise employees and where applicable Operators, Third Parties/Service Providers, contractors and agents acting on behalf of Thorburn within their areas of responsibility on the implementation of and compliance with POPIA, this Policy and any associated documents and procedures
- ensure appropriate technical and organisational measures are taken within their divisions/departments to ensure against unauthorised or unlawful processing, accidental loss or destruction of Personal Information
- support Thorburn's notification of the Regulator by maintaining Collection Matrix, the PI Inventory, Retention Schedules as well as databases and relevant procedures and the purposes of processing
- promptly passing onto the Personal Information Officer all data subject access requests from third partied for Personal Information
- keep the Personal Information Officer informed of any changes in the collection, use, and security of Personal Information (Impact Assessments) within their areas of responsibility
- Report any loss of personal information to the CEO / Functional Heads of Department and Data Information Officer
- Ensure proper completion of the Consent Management Documents with their respective division/department

13.11 All Employees

All employees of Thorburn are responsible for understanding the POPI obligations in terms of related policies and procedures as well as:

- checking that any processing activities engaged in comply with this Policy
- ensuring that PI is not used in any unlawful way
- ensuring that PI is not stored incorrectly, are not careless with it or cause a breach of legislation and our policies
- reporting losses or unauthorised disclosures of Personal Information to the Personal Information Officer
- ensuring that any transfer of Personal Information to Third Parties is authorised, lawful and that appropriate and safe transport mechanisms are employed in respect of the Personal Information so transferred such as encryption

- ensuring that only authorised downloading of electronic Personal Information onto portable devices, copying of hard copy Personal Information or the removal of manual from our premises occurs
- ensure that a written operator agreement is in place with a Third Party/Service Provider/Operator/ Agent or any other stakeholder prior to requesting the aforementioned to process Personal Information on behalf of Thorburn
- raising any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this Policy or our legal obligations without delay
- not attempt to gain access to information that is not necessary to hold, know or process
- ensuring that the Personal Information they provide about themselves is up to date; and
- Complying with this Policy at all times.

13.12 Third Parties/Service Providers/Operators

All Third Parties, Service Providers, Operators, Contractors, Agents and any other stakeholders acting on behalf of Thorburn have a responsibility to act only on Thorburn's instructions and to ensure that their processing of Personal Information provided to them by the us is carried out strictly in compliance with this Policy, Operator Agreements in place, and in accordance with POPIA and the general processing principles under POPIA.

14.Right to Access Personal Information

Thorburn recognises the rights of data subjects to know whether or not we hold information on them as well as the right to access all the Personal Information that we may hold about them and our responsibility to enable data subjects to access their PI. To this end, our PAIA Manual explains how:

- Access requests must be submitted and acknowledged by Thorburn through the PIO 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, Deletion and Objection to processing of Personal Information

A data subject may, in the prescribed manner, request Thorburn to:

- correct or delete Personal Information about them in our possession or under our 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 we are no longer authorised to retain;
- may object, at any time, to the processing of their Personal Information.

16. Questions or concerns about this Policy

If you have any questions or comments about this Policy, please contact POPI@Thorburn.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 PIO and must be processed in consultation with the 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 Thorburn will define, document, communicate and assign accountability for all POPI governance.

19. Other Policies and Documents

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

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