Protection Of Personal Information Policy

Applicable to Thorburn, its joint ventures , suppliers, directors, and all employees

Thorburn Security Solutions Website Privacy Policy

Message from Chef Executive Officer

The advent of the fourth industrial revolution has resulted in technologies, which is referred to as the essential 8, infiltrating the daily work and social lives of our employees, customers, and suppliers. The essential 8 are Artificial Intelligence, Machine Learning, Robotics, Augmented Reality, 3D printing, Blockchain, drones and the Internet of Things. At Thorburn Security Solutions we have already employed some of these technologies in our service offerings like the Internet of Things, Robotics and Augmented Reality. Furthermore, the connected economy in which we operate allows our employees, customers, and suppliers to be 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 access logs, surveillance footage, biometric verification for security services). All these technologies results in data being processed. 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.

Thorburn Security Solutions considers it 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 data protection and security in all we do, irrespective whether the information belongs to the customer, the supplier, or the employee. Our Data Protection Policy enables 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, irrespective of seniority or rank are obliged to adhere to this Policy.

As the Chief Executive Officer, it is my duty to ensure that the rules and principles of data protection at Thorburn Security Solutions are followed across the Group.

_____

Stephan Botha

Chief Executive Officer

Author:	Group Compliance Officer	Issue Date:	29 April 2021
Approver:	Group Legal Officer, CEO	Reviewed Date:	17 September 2025
Doc No:	POPI/GOV/01/TSG	Issue No:	3

1. Introduction

The Thorburn Security Solutions (Pty) Ltd (Thorburn Security Solutions) 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 Security Solutions 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 Security Solutions'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 data protection we must define, document, communicate our policies, statement, notices and other management processes to regulate our compliance and assign accountability for the management thereof as follows:

2.1 Data Protection Policy

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

2.2 Protection of Personal Information (POPI) Website Statement

The Thorburn Security Solutions POPI Website Statement must be made available to all stakeholders via our website, outlining how we manage and process 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 Data Protection 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 Data Protection Incident Response Plan

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

2.6 Data Protection Impact Assessments

Impact Assessments have been conducted across the group to establish the PI Impact within the various divisions and departments. Going forward, Impact Assessments must be completed in order 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 Data Protection Awareness

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

2.9 Data Protection 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 Data Protection Information Officer and participate in Data Protection Awareness Campaigns and initiatives.

3. Consent

Thorburn Security Solutions 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 Security Solutions 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 Security Solutions and its Third Parties and 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 Security Solutions 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 Security Solutions websites, such as the date and time of your visit, the information you searched to find the Thorburn Security Solutions websites, or your activity on the Thorburn Security Solutions 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 outside the Thorburn Security Solutions (Pty) Ltd structure who work with or on behalf of Thorburn Security Solutions 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. Privacy Notices

Thorburn Security Solutions is committed to transparency and compliance with Section 18 of the Protection of Personal Information Act (POPIA).

Accordingly, Thorburn Security Solutions shall issue and maintain specific Privacy Notices tailored to the categories of data subjects with whom it engages, including:

- Employees (current and prospective)
- Clients and customers
- Suppliers and service providers
- Website users
- Job applicants

These notices will be issued at or before the time of collection of personal information and will include, at a minimum, the following details:

- The information being collected and the source;
- The purpose of collection;
- Whether provision of information is mandatory or voluntary;
- The consequences of failing to provide the information;
- Any law authorising or requiring the collection;
- Intended recipients of the information;
- Whether the data will be transferred across borders and to whom;
- Data subject rights and the complaint process.

All privacy notices shall be reviewed annually and made available via internal channels (e.g., intranet, HR systems) and external platforms (e.g., corporate website, onboarding packs, contracts).

6. 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 Security Solutions will only process your PI 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 Security Solutions 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 protection 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 which 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.

7. Information quality

Thorburn Security Solutions is dedicated to keep PI that is processed accurately and, where necessary, up to date. Thorburn Security Solutions 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 Security Solutions is correct. Thorburn Security Solutions 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 or restrict to our use of your PI; and
- ask us to delete your PI from our database.

8. Disclosure to Third Parties/Service Providers/Operators

In order to ensure consistency in our employment activities and/or 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 Security Solutions (Pty) Ltd structure but work with or on behalf of Thorburn Security Solutions 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 Security Solutions or related third parties; or
- You agree that we may disclose your information.

Disclosure will always be subject to an agreement between Thorburn Security Solutions 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 Security Solutions will conduct a due diligence questionnaire to assess the control environment of said Third Party to identify any possible risks posed by inadequate controls.

9. Operator Management and Oversight

In accordance with Sections 20 and 21 of POPIA, all third-party service providers ("Operators") that process personal information on behalf of Thorburn Security Solutions are required to:

- Enter into a written Operator Agreement that imposes obligations regarding the security and confidentiality of personal information;
- Complete a Third-Party Due Diligence Questionnaire;
- Undergo risk classification in accordance with Thorburn Security Solutions's Information Risk Framework; and
- Implement appropriate technical and organisational measures to secure personal information.

A central Operator Register will be maintained by the Group Compliance Office, listing all approved Operators, associated risks, signed agreements, and dates of review.

Thorburn Security Solutions reserves the right to audit Operators or require evidence of their compliance with applicable data protection laws and standards.

10.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 Security Solutions 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.

Personal information may only be transferred outside the borders of South Africa where:

- The recipient jurisdiction provides adequate protection as contemplated in Section 72 of POPIA; or
- The data subject has provided informed consent; or
- The transfer is necessary for the performance of a contract, or in the data subject's interest; or
- The transfer is authorised by law.

Where required, Thorburn Security Solutions shall enter into cross-border data transfer agreements incorporating POPIA-compliant clauses or Binding Corporate Rules (BCRs).

A Cross-Border Transfer Register shall be maintained by the Information Officer, listing:

- The country of transfer;
- Legal basis for the transfer;
- Technical and contractual safeguards in place;
- Identity of the recipient.

Thorburn Security Solutions will ensure that PI transferred outside South Africa is subject to no lesser level of protection than afforded under POPIA.

11.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 Security Solutions 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.

12.Disposal and Destruction

Personal Information which is no longer required should 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 Security Solutions will safely and securely destroy or delete your PI in a manner that prevents reconstruction of your PI in an intelligible form.

13.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 Security Solutions must before processing PI 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 PI.

PI must not be disclosed unlawfully to any Third Parties, Service Providers or Operators. Transfers of PI to Third Parties, must be authorised in writing by the Functional Head/Divisional CEO and such information must be protected by adequate contractual provisions or data sharing/processor agreements.

All losses of PI must be reported to the relevant Functional Head, Divisional CEO of the department or division where the information emanates, the relevant Data Protection Champion and the Data Protection Information Officer.

Negligent loss or unauthorised disclosure of PI, 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 PI may be stored or processed have been implemented.

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

14.Information Retrieval and Management

Records in all formats containing PI must be collected, processed safely and securely stored, deleted and/or disposed of in accordance with Thorburn Security Solutions'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 PI 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.

15. Roles and Responsibilities

15.1 Chief Executive Officer ("CEO")

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 Security Solutions (Pty) Ltd.

15.2 Chief Information Officer ("CIO")

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 the Group.

15.3 Data Protection Information Officer ("DPIO")

The DPIO is primarily responsible for Thorburn Security Solutions's compliance with POPIA. This comprises:

- ensuring that Thorburn Security Solutions has a POPI compliance programme in place and that all employees, Operators, Third Parties/Service Providers, contractors and agents acting on behalf of Thorburn Security Solutions 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 lawful processing;
- the co-ordination / facilitation of all POPI related breaches and incidents which occur across Thorburn Security Solutions;
- have oversight of designated Data Protection 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; and
- The DPIO 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.

15.4 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; and
- Researching third-party services, such as cloud services that the company may consider using to backup, store or process data.

15.5 Group Legal Officer ("GLO")

GLO 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.

15.6 Group Internal Audit ("GIA")

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.

15.7 Group Compliance Officer ("GCO")

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

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.

15.8 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 CIO and GCO to ensure all marketing initiatives adhere to this Policy.

15.9 Divisional CEOs and Functional Heads of Department

Divisional CEOs 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 Group understand the role of the Data Protection conditions in their day-to-day work, through induction, training and performance monitoring, and for monitoring compliance within their own areas of responsibility.

15.10 Data Protection Champions

Divisional CEOs and Functional Heads of Department must ensure that Data Protection Champions are designated for their Divisions or Departments and provided with the appropriate training and support. Data Protection Champions are required to:

- advise employees and where applicable Operators, Third Parties/Service Providers, contractors and agents acting on behalf of the Group 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 Security Solutions's notification of the Regulator by maintaining a Collection Matrix, the PI Inventory, Retention Schedules as well as databases and relevant procedures and the purposes of processing;
- promptly passing on to the DPIO all data subject access requests from third parties;
- keep the DPIO informed of any changes in the collection, use, and security of PI (Impact Assessments) within their areas of responsibility;
- Report any loss of personal information to the Divisional CEOs / Functional Heads of Department and DPIO; and
- Ensure proper completion of the Consent Management Documents with their respective division/department.

15.11 All Employees

All employees of Thorburn Security Solutions 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 PI to the DPIO;
- ensuring that any transfer of PI to Third Parties is authorised, lawful and that appropriate and safe transport mechanisms are employed in respect of the PI so transferred such as encryption;
- ensuring that only authorised downloading of electronic PI onto portable devices, copying of hard copy PI or the removal of manuals 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 PI on behalf of Thorburn Security Solutions;
- 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 PI they provide about themselves is up to date; and
- Complying with this Policy at all times.

15.12 Third Parties/Service Providers/Operators

All Third Parties, Service Providers, Operators, Contractors, Agents and any other stakeholders acting on behalf of Thorburn Security Solutions have a responsibility to act only on Thorburn Security Solutions's instructions and to ensure that their processing of PI provided to them by Thorburn Security Solutions 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.

16 . Consent and Preference Management

Thorburn Security Solutions shall obtain voluntary, informed, and specific consent for any processing activity not justified by another lawful ground. This includes:

- Direct marketing;
- Processing of Special Personal Information;
- Cross-border data transfers not covered by contractual or statutory bases.

All consent collected shall be documented, time-stamped, and subject to regular review.

A Preference Management System shall be implemented to allow data subjects to:

- Withdraw consent at any time;
- Update communication preferences;
- Object to processing activities, particularly for direct marketing purposes.

17. Right to Access Personal Information

Thorburn Security Solutions recognises the rights of data subjects 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 Security Solutions through the CIO 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.

18. Correction of Personal Information

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

- correct or delete PI 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 PI about them that we are no longer authorised to retain.

19. Questions or concerns about this Policy

If you have any questions or concerns about this Policy, please contact POPI@tsebo.com .

20. 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 CIO and must be processed in consultation with the Group Audit and Risk Executive, Group Legal Officer and Group Compliance Officer.

21. 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 Security Solutions will define, document, communicate and assign accountability for all POPI governance.

22. Other Policies and Documents

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

Group IT Information Security Policy;

Group Cyber Security Policy;

Group Protection of Personal Protection Website Statement;

Group Protection of Employee Personal Information Notice;

as well as other related procedures.