

# INFINITY BRANDS (PTY) LTD

**REGISTRATION NUMBER: 2014/117386/07**

---

## PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013

### COMPLIANCE PLAN

#### 1. INTRODUCTION

The Personal Protection of Information Act 4 of 2013 (“**POPIA**”) took effect on 1 July 2020. Responsible parties were granted a grace period until 30 June 2021 to ensure compliance with POPIA.

Infinity Brands (Pty) Ltd (“**Infinity Brands**”), functions as an operator as defined in Section 1 of POPIA (“**Operator**”), rendering data processing services to third-party contractors (“**Responsible Party**” or “**Responsible Parties**”). It also collects and processes personal information as a Responsible Party.

Infinity Brands is cognisant of the nature of the civil liability created in terms of section 99(1) of POPIA and that the restricted nature of the defences in terms of section 99(2) creates significant risk for entities which may not be adequately addressed by the steps typically taken by entities to limit such risk.

Infinity Brands understands the importance of protecting the Personal Information which it has been entrusted with for processing purposes, and for ensuring that a high level of compliance with POPIA is achieved.

As a result of the aforementioned, Infinity Brands designed this compliance plan carefully, to ensure compliance with POPIA.

From the outset, Infinity Brands has evaluated and shall continually evaluate whether it processes information lawfully. This is achieved by complying with the eight requisites in POPIA, namely:

- **Accountability**: Infinity Brands ensures that the conditions are complied with at the time of determination of the purpose of the Personal Information, the motivation for which the Personal Information is processed, and the manner in which the Personal Information is processed. In doing so, Infinity Brands has appointed **Luke Harrison (“Harrison”)** to be the Compliance Officer.

- **Processing limitation:** The processing of personal information is limited to lawful processing in a reasonable manner that does not infringe the privacy of any subject. In this regard, Infinity Brands, at all times evaluates whether it is processing information which directly relates to the purpose and scope for which it was collected or received from the Responsible Party. Moreover, Harrison ensures that the Responsible Party has obtained the necessary consent from the data subject and information obtained from that data subject, even if such information relates to other data subjects. Data is processed in accordance with an agreement concluded between the Responsible Parties and Infinity Brands, where possible. Likewise, Infinity Brands also processes information about third parties, as required for the purpose of its own business activities.
  
- **Purpose specification:** When receiving Personal Information, Infinity Brands ensures that the information required is specific, defined, and for a lawful purpose, in relation to the function and business nature of Infinity Brands. As an Operator, Infinity Brands, when receiving information and documents, ensures that the Responsible Party has informed the data subject of the purpose of the required documents and information obtained. Infinity Brands have also clearly specified the purpose of the data collection in its privacy policy, which is accessible in electronic format on its website: <https://infinitybrands.co.za>.
  
- **Further processing limitation:** Infinity Brands, as an Operator, is contracted from time to time by Responsible Parties to process the required information and to perform the services as agreed upon in the service level contract. In addition to processing personal information on behalf of a Responsible Party, Infinity Brands similarly processes personal information collected from data subjects, for its own purposes as specified in this Compliance Plan. Infinity Brands equips its clients with the necessary information to make fact-based decisions in its entity, and to optimise its services and products. Infinity Brands ensures that the personal information processed is at all material times a requisite to render the services contemplated in the service level agreement, and processes the information in accordance with the lawful instructions obtained by the Responsible Party, for the following purposes:
  - a) To enable Infinity Brands to deliver bespoke and curated long-term brand strategies to its various franchisees (Responsible Parties);
  - b) To optimise, guide and operate specifically designed franchise support systems;

- c) To optimise the manner of marketing actioned by Infinity Brands, whether that be via a platform, website or social media format of Infinity Brands, and ultimately, strengthen customer relationships between clients, Infinity Brands and franchisees;
- d) To assist Franchisees in measuring the effectiveness and distribution of its products and services, and to understand the manner in which the data subject, who uses either the franchisees or Infinity Brands' services, interacts with its services, products and platforms;
- e) To conduct and support research and innovation on competitive products and services, to enhance the marketing and distribution strategy of each franchise;
- f) To innovate and optimise Infinity Brands' website to ensure that the site is more user-friendly, and suits the needs of the clients of Infinity Brands as well as the clients of the franchisees (Responsible Parties).
- g) To use operational data to benchmark franchise performance, setting standards and goals for the franchise networks owned, operated and managed by Infinity Brands;
- h) To empower its franchisees (Responsible Parties) to execute informed data-driven decisions, which enhances efficiency, reduce unnecessary expenses and improve customer satisfaction.

Save for processing the personal information collected from the data subject, as indicated and for the purposes as set out above, Infinity Brands does not share the personal information with any other entity and/or individual, save for the Responsible Party which has collected such Personal Information.

- **Information quality**: Infinity Brands collects the Personal Information of Data Subjects. As such, Infinity Brands ensures that the personal information so collected, is complete insofar as possible, accurate and continually updated where necessary. Pursuant thereto, Infinity Brands requests Data Subjects on an annual basis to update the collected Personal Information and to inform Infinity Brands of any changes in personal information. Infinity Brands has also informed its clients that it can amend, vary and change the client's personal information, by completing and submitting the necessary forms in its PAIA Manual. Its Data Quality Management Strategy employs the following key characteristics:

- a) **Data Standards:** Infinity Brands has established data quality standards and guidelines to ensure consistency in its data entry, storage and usage.
  - b) **Data Cleansing:** Infinity Brands implements data cleansing processes to identify and correct any inaccuracies, duplicates and inconsistencies in the personal information within its control.
  - c) **Data Monitoring:** Infinity Brands utilises certain features to monitor the quality of its personal information continuously, and to detect any and all anomalies.
- 
- **Openness:** Infinity Brands, as an Operator, requires that all Responsible Parties obtain the data subject's consent prior to the collection and processing of any Personal Information. Similarly, Infinity Brands as a Responsible Party, ensures that all data subjects from which it collects personal information is aware that the information is collected, the nature thereof, the source thereof as well as the purpose for which the information is requested and what law and/or reason if any, prescribes the disclosure of such personal information.
  - **Security Safeguards:** Infinity Brands has established a detailed proprietary data strategy to ensure that the personal information which it collects and receives, are at all times kept secure and free from public interference. As such, the primary objectives of this data strategy includes:
    - a) **Access Controls:** Infinity Brands has implemented role-based access controls to ensure that only authorised personnel can access specific personal information. The user roles of all employees of Infinity Brands have been clearly defined, and permission to personal information has been granted based on the role responsibility and its concomitant data requirements.
    - b) **Encryption:** Infinity Brands employs the safety features offered by encryption, to protect the personal information at rest and during transit, by utilising industry-standard encryption protocols.
    - c) **Data Masking:** Infinity Brands applies data-masking techniques to obscure sensitive information in non-production environments such as testing and development.
    - d) **Incident Response:** Infinity Brands has carefully curated an incident response plan to address all potential data breaches and security incidents. This plan outlines the measures to be taken in the event of either a potential data breach or security incident,

including actions such as notifications, mitigation strategies as well as disaster and recovery actions.

- e) **Virtual Private Networks (VPNs):** Infinity Brands utilises VPNs to ensure secure remote access to its data platforms and systems, which encrypts Internet traffic between remote users and Infinity Brand's corporate network, ensuring that any personal information transmitted over public networks remains secure.
- f) **Password Management Tool:** Infinity Brands has implanted a password management tool to assist in managing and securing passwords across its organisation.
- g) **Firewalls:** Infinity Brands has implemented firewalls at both its network and application levels to protect its internal system from any unauthorised access and cyber threats.
- h) **Endpoint Security:** Infinity Brands utilises endpoint security solutions to ensure that all laptops, desktops, and mobile devices of employees remain protected against any security breaches or cyber threats.
- i) **Regular Security Audits:** Infinity Brands conducts regular security audits to identify vulnerabilities in its data strategy plan, and to ensure compliance with security policies.
- j) **Employee Training and Awareness:** Infinity Brands offers frequent training events to its employees to ensure that all employees are properly educated about data security practices.
- k) **Data Retention and Disposal:** Infinity Brands has implemented proper data retention and disposal practices, which clearly specify the duration for which personal information must be retained based on regulatory requirements and business needs. After the retention period, personal information is securely disposed of to prevent unauthorised access. All electronically stored personal information of data subjects is deleted from its system, and any hard copies are destroyed.

Should it come to the attention of Infinity Brands that there has been a security breach and/or that its information was accessed by an unauthorised person, Infinity Brands undertakes to notify the Regulator and the Responsible Party as a matter of priority.

- **Data Subject's Participation:** Infinity Brands is cognisant of the fact that data subjects have the right to know the nature and extent of any personal information which Infinity Brands has, pertaining to such data subject and he/she may request the records or description of the information held by means of Infinity Brands PAIA manual, which will be made available on request, and which is placed at reception.

- **Nature of the Personal Information collected:** Infinity Brands has completed a detailed schedule of the personal information which it collects, has in its possession, and obtains from Responsible Parties. The schedule is attached to this Compliance Plan, and reviewed on a six month interval.

Further steps by Infinity Brands to ensure compliance with POPIA:

STEPS:	DESCRIPTION:	COMPLETED:
	Appointment of Information Officer	<p>Luke Harrison</p> <p><a href="mailto:cdo@infinitybrands.co.za">cdo@infinitybrands.co.za</a></p> <p>Appointment date: 06 December 2024</p>
	Appointment of Deputy Information Officer	<p>Nkululeko Alfred Nxumalo</p> <p><a href="mailto:it@infinitybrands.co.za">it@infinitybrands.co.za</a></p> <p>Appointment Date: 06 December 2024</p>
	Review of information on data subjects	Completed annually or regularly with due regard to ongoing instructions.
	Disclosure of Information	<p>Preceded by a request by the data subject for consent to divulge any personal information.</p> <p>Preceded further by a request made in terms of the Promotion of Access to Information Act (PAIA) manual.</p>
	Adequate policies in place	<p>Information is at all times processed with due regard to the 8 items listed in this compliance plan. This compliance plan was drafted as a reminder of and to record the process and policies in place in relation to the protection of personal information of data subjects.</p> <p>Information is processed by agreement between Infinity Brands and the third-party processor, for a specific purpose and in line with the business activities of Infinity Brands.</p>

	Training	<p>The Information Officer, Luke Harrison, underwent training and continues to undergo training in relation to POPIA which training is facilitated by professionals at Burger Huyser Attorneys Incorporated, for purposes of ensuring that he understands the protocols to be implemented as well as the reasons for the protocols and factors that must be considered at all times.</p>
--	----------	--

	<p>Appropriate Measures</p>	<p>Infinity Brands implements appropriate, reasonable technical and organisational measures to secure the integrity and confidentiality of any personal information in its possession or control.</p> <p>In doing so, Infinity Brands makes use of a Centralised Data Repository where all personal information is stored. Access to this data lake and data warehouse are limited, and determined by the roles which employees of Infinity Brands must execute.</p> <p>Any personal information is safeguarded by way of:</p> <ol style="list-style-type: none"> <li>1. <b><u>Individual passwords and login details</u></b>, which are retained privately and not shared. Infinity Brands also uses a <b><u>Password Management Tool</u></b>, which stores passwords in an encrypted vault.</li> <li>2. <b><u>Limited to no access</u></b> for certain individuals to ensure only authorised individuals have access to the data subjects' personal information;</li> <li>3. Infinity Brands utilises <b><u>encryption</u></b> and <b><u>data masking techniques</u></b> to ensure that personal information remains protected.</li> <li>4. A proper and detailed <b><u>Incident Response Plan</u></b> has been drawn up.</li> <li>5. Infinity Brands have implement <b><u>VPNs</u></b>, <b><u>Firewalls</u></b> and <b><u>Endpoint Security Solutions</u></b> to prevent any unauthorised access or cyber-attacks.</li> <li>6. Infinity Brands <b><u>regularly audits</u></b> the accuracy and completeness of both the</li> </ol>
--	-----------------------------	---



Infinity Brands is aware of the consequences of non-compliance with POPIA, specifically:

CRIMINAL	CIVIL
POPIA imposes various criminal offences for non-compliance. Non-compliance with POPIA can result in imprisonment not exceeding 10 years and/or a fine not exceeding R10 million.	In terms of section 99 of POPIA, a data subject or, at the request of the data subject, the Regulator, may institute a civil action for damages in a court having jurisdiction against a responsible party for breach of POPIA.