

**PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013
(POPI) POLICY**

BRAND NAME MARKETING (PTY) LTD

1. INTRODUCTION

Brand Name Marketing is committed to protect its client's privacy and ensure that the confidentiality of their personal information is used appropriately, transparently, securely and in accordance with the applicable laws.

Information Officers Contact Details:

Brand Name Marketing (Pty) Ltd
Unit 3, Lakeside Park, Lakeside Place,
Capricorn Business Park,
Muizenberg,
Cape Town 7945

Contact details: 021 788 3712

popi@tccc.africa

2. DEFINITIONS

2.1 Consent means the voluntary, specific and informed expression of will;

2.2 Data Subject means the person to whom personal information relates;

2.3 Direct Marketing means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of –

a) Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or

2.4 Operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party;

2.5 POPI means the Protection of Personal Information Act, No. 4 of 2013;

2.6 Personal Information means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person as defined by POPI;

2.7 Processing means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information.

3. SCOPE OF THE POLICY

This policy is applicable to all employees and directors in Brand Name Marketing (Pty) Ltd.

4. POLICY STATEMENT

Brand Name Marketing collects voluntarily personal information of individuals and corporate entities with whom it works in order to operate and carry out its business effectively. We regard the lawful and appropriate processing of all personal information as crucial to successful service delivery and essential to maintaining confidence between Brand Name Marketing and those individuals and entities in which we deal with. Any personal information that you send us will be used for the intended purpose and adhered to the principles of the Protection of Personal Information Act (POPI).

5. PROCESSING OF PERSONAL INFORMATION

5.1 Personal Information will only be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject.

5.2 Purpose of Processing

- Providing products and services to customers
- Marketing and Sales
- Conducting credit reference checks and assessments
- Administration of Agreements
- Employee administration
- In connection with legal proceedings
- Keeping of accounts and records
- Complying with legal and regulatory requirements
- Detecting and prevention of fraud, crime, money laundering and other malpractice
- Profiling data subjects for the purpose of direct marketing

5.3 In the event that Brand Name Marketing (Pty) Ltd appoints or authorizes an operator to process any personal information on its behalf or for any reason, it will implement necessary agreements to ensure that the operator or anyone processing personal information on behalf of Brand Name Marketing (Pty) Ltd or an operator, must –

- Process such information only with the knowledge or authorization of Brand Name Marketing (Pty) Ltd; and
- Treat personal information which comes to his/her/its knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of his/her/its duties.

5.4 Brand Name Marketing will maintain the documentation of all processing operations under its responsibility

5.5 Categories of Data Subject and their Personal Information

We may possess records relating to customers, employees, suppliers, shareholders and service providers:

Entity Type	Personal Information Processed
Customers: Natural Person	Full Name, contact details; physical and or postal address; ID number; tax related information; Banking details; confidential correspondence; Vat number; Financial Information; Spouse information if married COP
Customer – Juristic Person / Entities	Name of legal entity; registration number; physical and or postal address; contact persons; contact details; banking details; financial information; tax related information; Shareholders / Directors information; BBEE information, CIPC supporting documents; Vat number; Trade References
Service Providers	Name of legal entity; registration number; physical and or postal address, contact person; contact details; CIPC supporting documents; Shareholder / Directors information, Banking details, Vat number; BBEE information
Employees	Full Name; ID number; Passport NUMBER; nationality; work permit number; physical and or postal address; contact details; gender; race, language, disability status; politically exposed person details; criminal check; credit check; education information; marital status; employment history; income tax number; banking details

5.6 Retention and Restriction of Records

Brand Name Marketing will not retain any records of personal information any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless –

- The retention of a record is required or authorized by law;
- We reasonably require a record for lawful purposes related to its functions or activities;
- Retention of a record is required by a contract between the parties or entities thereto; or
- The data subject or a competent person where the data subject is a child consented to the retention of a record.

Information collected or processed initially for the purpose of historical, statistical or research value, may be retained for a period longer than contemplated providing Brand Name Marketing has appropriate measures in place to safeguard these records against uses other than it was intended for initially.

Brand Name Marketing will destroy or delete a record of personal information or de-identify it as soon as reasonably practicably after it is no longer authorized to retain such record.

The de-identifying or deletion of a record of personal information will be done in a manner that prevents its reconstruction in an intelligible/understandable form.

In the event where records of personal information are used of a data subject to make a decision about the data subject – It must;

- Retain the record for such period as may be required or prescribed by law or a code of conduct; or
- If there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

Brand Name Marketing will restrict the processing of personal information if;

- Its accuracy is contested by the data subject, for a period enabling the company to verify the accuracy of the information;
- We no longer require the personal information for achieving the purpose for which it was collected or subsequently processed, but it has to be maintained for purposes of proof;
- The processing is unlawful and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or
- The data subject request to transmit the personal data into another automated processing system.

Personal information that has been restricted will only be processed for purposes of proof, or with the data subject's consent, or with the consent of a competent person where the data subject is a child, or for the protection of the rights of another natural or legal person or if such processing is in the public interest.

Where personal information is restricted, Brand Name Marketing will inform the data subject before lifting the restriction.

5.7 Information Security Measures

Brand Name Marketing will secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonably, technical and organizational measures, which include:

- Company Firewalls
- Email Firewall
- Virus protection software and update protocols
- Secure setup of hardware and software making up the IT infrastructure
- Outsourced Service Providers who process Personal Information on behalf of the company are contracted to implement security controls

- Departmental access
- Microsoft multi factor authentication

5.8 Security Compromises

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorized person, Brand Name Marketing will notify-

- The information Regulator; and
- The data subject, unless the identify of such data subject cannot be established.

The notification of a breach will be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the company's information system.

The company will only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

The notification to a data subject will be in writing and communicated to the data subject.

The notification will provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise.

6. ACCESS TO PERSONAL INFORMATION

All individuals within the company will be restricted to personal information in accordance with the functions they fulfill. Any request to access or view further personal information should be addressed with the Information Officer.

7. REQUEST FOR DISCLOSURE

Brand Name Marketing will respond when the data subject request notification of purpose of use, disclosure, correction, addition or deletion of details, and suspension of use or elimination relating to personal information held by the company.

8. MONITORING AND ENFORCEMENT

Each employee of the company will be responsible for administering and overseeing the implementation of this policy and, as applicable, support guidelines, standard operating procedures, notices, consents and appropriate related documents and processes. Managers and responsible employees will be trained according to their functions in legal requirements, policies and guidelines that govern the protection of personal information in the company. The company will conduct periodic reviews and audits, where appropriate, to demonstrate compliance with privacy law and its policies, this Act and any applicable regulations. Employees who violate the guidelines and standard operating procedures of this policy may be subject to disciplinary action being taken against him/her.

9. IMPLEMENTATION GUIDELINES

This policy has been put in place throughout the company, training on the Policy and POPI will take place with all affected employees.

All new employees will be made aware at induction of their responsibilities under the terms of this Policy and POPI.

Any modification or updates in respect of this policy and legislation or guidelines will be brought to the attention of all employees.

10. CONDITIONS OF LAWFUL PROCESSING OF PERSONAL INFORMATION

The Information Officer will ensure that Brand Name Marketing adheres to the following conditions for the lawful processing of personal information.

10.1 Accountability

Brand Name Marketing will remain liable for compliance with these conditions, even if it has outsourced its processing activities.

When collecting and during the processing phase of personal information, we will ensure that the purpose and means are relevant and comply with the requirements of this Act.

10.2 Processing Limitations

The processing of personal information is only lawful if, given the purpose of processing, the information is adequate, relevant and not excessive.

Grounds for lawful processing exists when;

- The data subject or a competent person where the data subject is a child consents to the processing;
- The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party;
- The processing complies with an obligation imposed by law on the company
- The processing protects a legitimate interest of the data subject;
- The processing is necessary for the proper performance of a public law duty by the company or
- The processing is necessary for pursuing the legitimate interest of the company or of a third party to whom the information is supplied.

Special Personal Information includes;

- Religious, philosophical, or political beliefs;
- Race or ethnic origin;
- Health and sex life
- Biometric information (including blood type, fingerprints, DNA, retinal scanning, voice recognition, photographs);
- Criminal Behavior;

- Information concerning a child

This above information may only be processed by the company under the following circumstances:

- The Data Subject has consented to such processing;
- The Special Personal Information was deliberately made public by the Data Subject;
- Processing is necessary for the establishment of a right or defense in law;
- Processing is for historical, statistical, or research reasons
- If processing of race or ethnic origin is in order to comply with affirmative action laws

The data subject or competent person may withdraw his, her or its consent, at any time provided that: the lawfulness of the processing of personal information in terms of paragraph 10.2 will not be affected.

Collection directly from data subject

As far as possible, Brand Name Marketing will collect personal information directly from the data subject, except under the following circumstances:

- The information is contained in or delivered from a public record or has deliberately been made public by the data subject;
- The data subject or a competent person where the data subject is a child has consented to the collection of the information from another source;
- Collection of the information from another source would not prejudice a legitimate interest of the data subject;
- Collection of information from another source is necessary to maintain, comply with or exercise any law or legal right;
- Collection from the data subject would prejudice the lawful purpose of collection;
- Collection from the data subject is not reasonably practicable in the circumstances of the particular case.

10.3 Purpose Specification

The company shall only process personal information for the specific purposes as set out and defined in Paragraph 5.1

10.4 Further Processing Limitation

New processing activity must be compatible with original purpose of processing. Further processing will be regarded as compatible with the purpose of collecting it;

- Data Subject has consented to the further processing;
- Personal information is contained in a public record;
- Personal Information has been deliberately made public by the data subject;
- Further processing is necessary to maintain, comply with or exercise any law or legal right;
- Further processing is necessary to prevent or mitigate a threat to public health or safety, or the life or health of the Data Subject or a third party.

10.5 Information Quality

The company shall take reasonable steps to ensure that personal information is complete, accurate, not misleading and updated. The company shall periodically review data subject records to ensure that the personal information is still valid and correct.

Employees should as far as reasonably practicable follow the following guidance when collecting personal information

- Personal Information should be dated when received;
- A change should be kept to where the personal information was obtained;
- Changed to information records should be dated;
- Irrelevant or unneeded personal information should be deleted or destroyed;
- Personal information should be stored securely, either on a secure electronic database or in a secure physical filing system.

10.6 Openness

The company shall take reasonable steps to ensure that the Data Subject is made aware of;

- What Personal Information is collected, and the source of the information
- The purpose of collection and processing;
- Where the supply of personal information is voluntary or mandatory, and the consequences of a failure to provide such information;
- Whether collection is in terms of any law requiring such collection;
- Whether the personal information shall be shared with any third party.

10.7 Security Safeguards

Brand Name Marketing shall ensure the integrity and confidentiality of all personal information in its possession, by taking reasonable steps to;

- Identify all reasonably foreseeable risks to information security;
- Establish and maintain appropriate safeguard against such risk;

Written records

- Personal information records should be kept in locked cabinets, or safes;
- When in use personal information records should not be left unattended in areas where non-staff members may access them;
- The company 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;
- Personal information which is no longer required should be disposed of by shredding.

Any loss or theft of, or unauthorized access to, personal information must be immediately reported to the information officer.

Electronic Records

- All electronically held Personal Information must be saved in a secure database;
- As far as reasonably practicable, no personal information should be saved on individual computers, laptops or hand-held devices;
- All computers, laptops and hand-held devices should be access protected with a password, fingerprint or retina scan, with the password being of reasonable complexity and changed frequently;
- The company shall implement and maintain a “clean screen policy” where all employees shall be required to lock their computers or laptops when leaving their desks for any length of time and to log off at the end of the days;
- Electronic personal information which is no longer required must be deleted from the individual laptop or computer and the relevant database. The employee must ensure that the information has been completely deleted and is not recoverable.

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 shall take all necessary steps to remotely delete the information, if possible.

10.8 Data Subject Participation

Data Subject have the right to request access to, amendment, or deletion of their personal information.

All such requests must be submitted in writing to the information officer. Unless there are grounds for refusal. The company shall disclose the requested personal information:

- On receipt of adequate proof of identity from the data subject, or requester;
- Within a reasonable time
- On receipt of the prescribe fee, if any;
- In a reasonable format

The company shall not disclose any personal information to any party unless the identity of the requester has been verified.

11. DIRECT MARKETING

All direct marketing communications shall contain the company’s details and an address or method for the customers to opt-out for receiving further marketing communication.

Existing Customers

Direct marketing by electronic means to existing customers is only permitted;

- If the customer's details were obtained in the context of a sale or service; and
- For the purpose of marketing the same or similar products;

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

11.1 Consent

The company may send electronic direct marketing communication to data subject who have consented to receiving it. The company may approach the data subject for consent only once.

11.2 Record keeping

The company shall keep records of;

- Date of consent
- Wording of the consent
- Who obtained the consent
- Proof of opportunity to opt-out on each marketing contact
- Records of opt-outs

12. DESTRUCTION

Documents may be destroyed after the termination of the retention period specified herein, or as determined by the company from time to time.

The company may suspend destruction of any record or document due to pending or reasonably foreseeable litigation, audits, government investigations or similar proceedings. Employees will be notified of applicable documents where the destruction has been suspended to which they have access to.

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

The documents must be made available for collection by an approved document disposal company.

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.

The documents and information listed below may not contain all the records and documents processed and in the possession of the company and should merely be used as a guideline.

The information officer should be consulted where there is uncertainty regarding the retention of destruction of a document and/or information.

COMPANIES ACT

Nr.	Type of document	Minimum retention required
1	Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Act;	7 Years
2	Notice and minutes of all shareholders meeting, including resolution adopted and documents made available to holders of securities	
3	Copies of reports presented at the annual general meeting of the company	
4	Record of directors and past directors, after the director has retired from the company	
5	Written communication to holders of securities and	
6	Minutes and resolutions of directors meeting, audit committee and directors' committees	
7	Registration certificate	Indefinitely
8	Memorandum of Incorporation and alteration and amendments	
9	Rules	
10	Securities register and uncertified securities register	
11	Register of company secretary and auditors and	
12	Regulated companies (companies to which chapter 5, part B, C and Takeover Regulations apply)- Register of disclosure of person who holds beneficial interest equal to or in excess of 5 % of the securities of that class issued	

CONSUMER PROTECTION ACT

Nr.	Type of document	Minimum retention required
1	Full names, physical address, postal address and contact details	3 Years
2	ID number and registration number	
3	Contact details of public officer in case of a juristic person	
4	Service rendered	
5	Cost to be recovered from the consumer	
6	Frequency of accounting to the consumer	
7	Amounts, sums, values, charges, fees, remuneration specified in monetary terms	
8	Conducting a promotional competition refer to Section 36(11)(b) and Regulation 11 of Promotional Competitions	

ACCOUNTING

Nr.	Type of document	Minimum retention required
1	Annual Financial Statements including, annual accounts, director's and auditors	15 Years
2	Book of accounting recording information required by the Companies Act No.71 of 2008	
3	Branch Register	5 Years
4	Certificate of change of name	Indefinite
5	Certificate of incorporation	
6	Certificate of commence business	
7	Director's attendance register	15 Years
8	Index of members	
9	Memorandum and articles of association	Indefinite
10	Minute book, CM25 and CM26, as well as	

	resolutions passed at the general/class meetings	
11	Microfilm image of any original record reproduced directly by the camera	Indefinite
12	Proxy forms	3 Years
13	Proxy forms used at court convened meetings	
14	Register of allotments – after a person ceased to be a member	15 Years
15	Register of directors and certain officers	
16	Register of director's shareholding	
17	Register of Members	
18	Register of mortgage and debentures and fixed assets	

PERSONNEL RECORDS

Nr.	Type of document	Minimum Retention Required
1	Basic Conditions of Employment Act: Section 29 (4): Written particulars of an employee after termination of employment; Section 31: Employee's name and occupation Time worked by employee Remuneration to be paid to each employee Date of birth of any employee under 18 years of age	3 Years
2	Employment Equity Act: Records in respect of the company's workforce, employment equity plan and other records relevant to compliance with the Act; Section 21 report which is sent to the Director General	3 Years
3	Labour Relations Act: Records to be retained by the employer are the collective agreements and arbitration awards	3 Years

	<p>An employer must retain prescribe details of any strike, lock-out or protest action involving its employees;</p> <p>Records of each employee specifying the nature of any disciplinary transgressions, the action taken by the employer and the reasons for the actions</p>	Indefinite
4	<p>Unemployment Insurance Act: Employers must retain personal records of each of their current employees in terms of their names, identification number, monthly remuneration and address where the employee is employed</p>	5 Years

TAX

Nr.	Type of document	Minimum Retention Required
1	<p>Tax administration Act Section 29 documents which: Enables a person to observe the requirements of the act; Are specifically required under a Tax Act by the Commissioner by the public notice; Will enable SARS to be satisfied that the person has observed these requirements</p>	5 Years
2	<p>Income Tax Act Amount of remuneration paid or due by him/her to the employee; The amount of employee's tax deducted or withheld from the remuneration paid or due; The income tax reference number of that employee; Any further prescribed information</p>	5 Years

	Employer reconciliation return	
3	<p>Value Address Tax Act</p> <p>Where a vendor's basis of accounting is changed the vendor shall prepare a list of debtors and creditors showing the amounts owing to the creditors at the end of the tax changeover period;</p> <p>Importation of goods, bill of entry, other documents prescribed by the Custom and Excise Act and proof that the VAT charged has been paid to SARS;</p> <p>Vendors are obliged to retain records of all goods and services, rate of tax applicable to the supply, list of suppliers or agents, invoices and tax invoices, credit and debit notes, bank statements, deposit slips, stock list and paid cheques;</p> <p>Documentary proof substantiating the zero rating of suppliers;</p> <p>Where a tax invoice, credit or debit note, has been issued in relation to a supply by an agent or a bill of entry as described in the Customs and Excise Act, the agent shall maintain sufficient records to enable the name, address and VAT registration number of the principle to be ascertained.</p>	

HEALTH AND SAFETY

Nr.	Type of document	Minimum Retention Required
1	Register, records or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribe particulars of all the employees compensated for	4 Years

	disablement caused by occupational injuries or disease sustained or contracted by employees in the course of their employment, or for death sustained by these injuries at their place of work.	
2	A health and safety committee shall keep record of each recommendation made to an employer in terms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation.	3 Years
3	Records of incidents reported at work	3 Years
4	Records of assessment and air monitoring, and the asbestos inventory	Minimum of 40 Years
5	Medical surveillance records	40 Years
6	Records of risk assessments and air monitoring results	40 Years
7	Record of assessment and air monitoring	30 Years
8	All records of assessment and noise monitoring	40 Years

CREDIT AGREEMENT

Nr.	Type of document	Minimum Retention Required
1	Enquiries	2 Years
2	Payment profile	5 Years
3	Adverse information	1 Years
4	Civil court judgements	The earlier of 5 years or until the judgement is rescinded by a court or abandoned
5	Administration orders	The earlier of 10 years or until the judgement is rescinded by a court
6	Sequestrations	The earlier of 10 years or until the judgement is rescinded by a court
7	Liquidations	Unlimited
8	Rehabilitation order	5 Years

ELECTRONIC COMMUNICATION

Nr.	Type of document	Minimum Retention Required
1	Personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates processes or stores the information	As long as the information is used and at least 1 year thereafter
2	A record of any third party to whom the information was disclosed	As long as the information is used and at least 1 year thereafter
3	All personal data that has become obsolete	

MISCELLANEOUS

Nr.	Type of document	Minimum Retention Required
1	Employment record – all non-hired applicants (including all applications and resumes – whether solicited or unsolicited, results of post-offer, pre-employment, physicals, results of background investigations, if any, related correspondence	3 Years