

Stephen Jordaan/Bulls Eye Accounting and tax solutions

MANUAL
in terms of Section 51 of The Promotion of Access to information Act
2/2000 (the "ACT")

DATE OF COMPILATION: 26 June 2021
DATE OF REVISION: 26 June 2021

**PROMOTION OF ACCESS TO INFORMATION ACT,
ACT 2 OF 2000 (“The Act”)**

1. Introduction
2. Definitions
3. Scope of the policy
4. Policy statement
5. Processing of personal information
6. Access to personal information
7. Implementation guidelines
8. Processing conditions
9. Direct Marketing
10. Statutory retention periods

**PROMOTION OF ACCESS TO INFORMATION ACT,
ACT 2 OF 2000 (“The Act”)**

1 Introduction

This Data Protection and Information Sharing Policy describes the way that Stephen Jordaan/Bulls Eye Accounting and tax solutions will meet its legal obligations and requirements concerning confidentiality and information security standards

The requirements within the Policy are primarily based upon the Protection of Personal Information Act, No 4 of 2013, as that is the key piece of legislation covering security and confidentiality of personal information.

Contact Details

Information Officer S Jordaan

Postal Address 15b Fuchsia Street Durbanville

Telephone Number 074 5847533

Email address info@bulls-eye.co.za

2 Definitions

Consent : means the voluntary, specific and informed expression of will

Data Subject means the natural or juristic person to whom the Personal Information relates

Direct Marketing means approaching a Data Subject personally for the purpose of selling them a product or service, of requesting a donation

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

Personal Information means information relating to an unidentifiable, living, natural person, or an identifiable, existing juristic person, as defined in POPI

Processing means an operation or activity, whether or not by automatic means, concerning Personal Information

3 Scope of the policy

The Policy applies to all employees

4 Policy Statements

The organization collects and uses Personal Information of the individuals and corporate entities with whom it provides services to in order to operate and carry out its business effectively

5 Processing of personal information

Purpose of Processing

Providing products and services to customers

Marketing and sales

In connection with legal proceedings

Keeping of accounts and records

Complying with legal and regulatory requirements

Categories of Data Subjects and their Personal Information

Customers: Natural Persons

Names; contact details; physical and postal addresses; date of birth; ID number; tax related information; nationality; gender; confidential correspondence

Customer – Juristic Persons / Entities

Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related information; authorized signatories; beneficiaries; ultimate beneficial owners; shareholding information; BBBEE information

Categories of Recipients for Processing the Personal Information

The organization may share the Personal Information with its agents, affiliates, and associated companies who may use this information to send the Data Subject information on products and services. The organization may supply the Personal Information to any party to whom the Group may have assigned or transferred any of its rights or obligations under any agreement, and/or to service providers who render the following services:

- Capturing and organizing of data;
- Storing of data;
- Sending of emails and other correspondence to customers;
- Conducting due diligence checks;
- Administration of the Medical Aid and Pension Schemes.

Actual or Planned Transborder Flows of Personal Information

Personal Information may be transmitted transborder to the organizations authorized dealers and its suppliers in other countries, and Personal Information may be stored in data servers hosted outside South Africa, which may not have adequate data protection laws. The Group will endeavor to ensure that its dealers and suppliers will make all reasonable efforts to secure said data and Personal Information

Retention of Personal Information Records

The organization may retain Personal Information records indefinitely, unless the Data Subject objects thereto. If the Data Subject objects to indefinite retention of its Personal Information the organization shall retain the Personal Information records to the extent permitted or required by law.

General Description of Information Security Measures

The organization employs up to date technology to ensure the confidentiality, integrity and availability of the Personal Information under its care. Measures include:

Firewalls
Virus protection software and update protocols
Limited access to premises

6 Access to personal information

All individuals and entities may request access, amendment, or deletion of their own Personal Information held by the organization. Any requests should be directed, on the prescribed form, to the Information Officer

Remedies available if request for access to Personal Information is refused

Internal Remedies

The organization does not have internal appeal procedures. As such, the decision made by the Information Officer pertaining to a request is final, and requestors will have to exercise such external remedies at their disposal if a request is refused, and the requestor is not satisfied with the response provided by the information officer

External Remedies

A requestor that is dissatisfied with the information officer's refusal to disclose information, May within 30 days of notification of the decision, apply to a court for relief. Likewise, a third party dissatisfied with the information officer's decision to grant a request for information, may within 30 days of notification of the decision, apply to a court for relief. For purposes of the Act, courts that have jurisdiction over these applications are the Constitutional Court, the High Court or another court of similar status.

Grounds for Refusal

Protecting personal information that the organization holds about a third person (who is a natural person) including a deceased person, from unreasonable disclosure;

If disclosure of the record would result in a breach of a duty of confidence owed to a third party in terms of an agreement

If disclosure of the record would endanger the life or physical safety of an individual;

If disclosure of the record would prejudice or impair the security of property or means of transport;

If disclosure of the record would prejudice or impair the protection of a person in accordance with a witness protection scheme;

If disclosure of the record would prejudice or impair the protection of the safety of the public;

The record is a computer programme

Records that cannot be found or do not exist

If the organization has searched for a record and it is believed that the record does not exist or cannot be found, the requester will be notified by way of an affidavit or affirmation. This will include the steps that were taken to try to locate the record.

7 Training & Dissemination of Information

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

Modifications and updates to data protection and information sharing policies, legislation, or guidelines will be brought to the attention of all staff

Employee Contracts

Each new employee will sign an Employment Contract containing the relevant consent clauses for the use and storage of employee information, and a confidentiality undertaking as part and will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information, however it is stored. Failure to comply will result in the instigation of a disciplinary procedure

8 PROCESSING CONDITIONS

The organization shall ensure that all processing conditions, as set out in POPI, are complied with when determining the purpose and means of processing Personal Information and during the processing itself.

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

The organization may only process Personal Information if one of the following grounds of lawful processing exists:

The Data Subject consents to the processing

Processing is necessary for the conclusion or performance of a contract with the Data Subject;

Processing complies with a legal responsibility imposed on the Group;

Processing protects a legitimate interest of the Data Subject

Special Personal Information includes:

Religious, philosophical, or political beliefs;
Race or ethnic origin;
Trade union membership;
Health or sex life;
Biometric information (including blood type, fingerprints, DNA, retinal scanning, voice recognition, photographs);
Criminal behavior;
Information concerning a child.

The Group may only process Special Personal Information 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

All Data Subjects have the right to refuse or withdraw their consent to the processing of their Personal Information, and a Data Subject may object, at any time, to the processing of their Personal Information on any of the above grounds, unless legislation provides for such processing. If the Data subject withdraws consent or objects to processing then the organization shall forthwith refrain from processing the Personal Information.

Collection directly from the Data Subject

Personal Information must be collected directly from the Data Subject, unless:
Personal Information is contained in a public record;
Personal Information has been deliberately made public by the Data Subject;
Personal Information is collected from another source with the Data Subject's consent;
Collection of Personal Information from another source would not prejudice the Data Subject;
Collection of Personal 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.

Purpose Specification

The Group shall only process Personal Information for the specific purposes as set out and defined above at paragraph 5.

Further Processing

New processing activity must be compatible with original purpose of processing. Further processing will be regarded as compatible with the purpose of collection if:
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

Information Quality

The organization shall take reasonable steps to ensure that Personal Information is complete, accurate, not misleading and updated. The organization 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 record should be kept of 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.

Openness

The organization 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

Data Subject Participation

Data Subject has 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 as set out in paragraph 6. Above, the organization 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 prescribed fee, if any;
In a reasonable format

The organization shall not disclose any Personal Information to any party unless the identity of the requester has been verified.

Security Safeguards

The organization 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 safeguards against such risks;

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 organization 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 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 organization 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 day;
Electronically Personal Information which is no longer required must be deleted from the individual laptop or computer and the relevant database.
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

9 DIRECT MARKETING

All Direct Marketing communications shall contain the organization details, and an address or method for the customer to opt-out of 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.

Consent

The Group may send electronic Direct Marketing communication to Data Subjects who have consented to receiving it. The Group may approach a Data Subject for consent only once

Record Keeping

The Group shall keep record of

Date of consent

Wording of the consent

Who obtained the consent

Proof of opportunity to opt-out on each marketing contact

Record of opt-outs

10 DESTRUCTION OF DOCUMENTS

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

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

11 STATUTORY RETENTION PERIODS

Companies Act

7 Years

Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Act;
Notice and minutes of all shareholders meeting, including resolutions adopted and documents made available to holders of securities
Copies of reports presented at the annual general meeting of the company
Copies of annual financial statements required by the Act
Copies of accounting records as required by the Act;
Record of directors and past directors, after the director has retired from the company;
Written communication to holders of securities and
Minutes and resolutions of directors' meetings, audit committee and directors' committees.

Indefinitely

Registration certificate;
Memorandum of Incorporation and alterations and amendments;
Rules;
Securities register and uncertified securities register;
Register of company secretary and auditors and
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

3 Years

Full names, physical address, postal address and contact details;
ID number and registration number;
Contact details of public officer in case of a juristic person;
Service rendered;
Cost to be recovered from the consumer;
Frequency of accounting to the consumer;
Amounts, sums, values, charges, fees, remuneration specified in monetary terms;
Conducting a promotional competition refer to Section 36(11)(b) and Regulation 11 of Promotional Competitions;

Financial intelligence centre Act

5 Years

Whenever a reportable transaction is concluded with a customer, the institution must keep record of the identity of the customer;
If the customer is acting on behalf of another person, the identity of the person on whose behalf the customer is acting and the customer's authority to act on behalf of that other person;
If another person is acting on behalf of the customer, the identity of that person and that other person's authority to act on behalf of the customer;
The manner in which the identity of the persons referred to above was established;
The nature of that business relationship or transaction;
In the case of a transaction, the amount involved and the parties to that transaction;
All accounts that are involved in the transactions concluded by that accountable institution in the course of that business relationship and that single transaction;
The name of the person who obtained the identity of the person transacting on behalf of the accountable institution;
Any document or copy of a document obtained by the accountable institution

Compensation for occupational injuries and diseases act

4 years
Register, record or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees.

3 years
Health and safety committee recommendations 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;
Records of incidents reported at work.

Basic conditions of employment act

3 years
Section 29(4):
Written particulars of an employee after termination of employment;
Section 31: -Employee's name and occupation;
Time worked by each employee;
Remuneration paid to each employee;
Date of birth of any employee under the age of 18 years.

Employment equity Act

3 years
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

Labour relations act

3 years
Records to be retained by the employer are the collective agreements and arbitration awards.

Indefinite

An employer must retain prescribed details of any strike, lock-out or protest action involving its employees;
Records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions

Unemployment insurance act

5 years
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

Tax administration act

5 years

Section 29 documents which:

Enable 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

Income tax act

5 years

Amount of remuneration paid or due by him 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;

Employer Reconciliation returns.

Value Added tax act

5 years

Where a vendor's basis of accounting is changed the vendor shall prepare lists of debtors and creditors showing the amounts owing to the creditors at the end of the tax period immediately preceding the changeover period;

Importation of goods, bill of entry, other documents prescribed by the Custom and Excise Act and proof that the VAT charge has been paid to SARS;

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 lists and paid cheques;

Documentary proof substantiating the zero rating of supplies;

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 principal to be ascertained.

Note : clients are to keep their own copies of any of the above documents for inspection purposes