

PROTECTION OF PERSONAL INFORMATION ACT (POPIA)

ROKWIL GROUP (PTY) LTD

Rokwil (Pty) Ltd

Reg No
2017/649536/07

VAT No

Director
R Stainton

CONTENTS

1. Introduction
2. Rights of Data Subjects
 - 2.1 The Right to Access Personal Information
 - 2.2 The Right to Have Personal Information Corrected or Deleted
 - 2.3 The Right to Object to the Processing of Personal Information
 - 2.4 The Right to Object to Direct Marketing
 - 2.5 The Right to Complain to the Information Regulator/Officer
 - 2.6 The Right to be Informed
3. General Guiding Principles
 - 3.1 Accountability
 - 3.2 Processing Limitation
 - 3.3 Specific Purpose
 - 3.4 Limitation on Further Processing
 - 3.5 Information Quality
 - 3.6 Transparency/Openness
 - 3.7 Security Safeguards
 - 3.8 Participation of Individuals
4. Collection and Use of Personal Information
 - 4.1 Collection of Employee Information
 - 4.2 Use of Employee Information
 - 4.3 Collection of Client Information
 - 4.4 Use of Client Information
5. Disclosure of Personal Information
6. Safeguarding Personal Information and Consent
7. Security Breaches
8. Access and Correction of Personal Information
9. Retention of Records
10. POPI Complaints Procedure
11. Disciplinary Action
12. Policy Amendments

1. INTRODUCTION

The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 (POPIA).

POPIA aims to promote the protection of privacy through eight guiding principles that are intended to be applied to the processing of personal information in a sensitive manner.

The Company acknowledges that it is obliged to comply with the Protection of Personal Information Act No 4 of 2013 (POPIA), in light of the fact that it processes the personal information of its employees and clients from time to time.

The Company guarantees its commitment to protecting the privacy of its clients and employees, and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

This Policy sets out the manner in which the Company deals with such personal information as well as stipulates the general purpose for which such information is used.

Employees and clients should be made aware of the contents of this Policy when their consent is requested for the processing of their personal information.

This Policy shall apply to any other parties' personal information which the Company collects and processes.

2. RIGHTS OF DATA SUBJECTS

Where appropriate, the Company will ensure that its clients and employees are made aware of their rights as data subjects, namely

2.1 The Right to Access Personal Information

The Company recognises that a data subject has the right to establish whether the Company holds personal information related to him/her, including the right to request access to that personal information.

2.2 The Right to have Personal Information Corrected or Deleted

The data subject has the right to request, where necessary, that his/her personal information must be corrected or deleted where the Company is no longer authorised to retain the personal information.

2.3 The Right to Object to the Processing of Personal Information

The data subject has the right, on reasonable grounds, to object to the processing of his/her personal information. In such circumstances, the Company will give due consideration to the request and the requirements of POPIA. The Company may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record-keeping requirements, also approve the destruction of the personal information.

2.4 The Right to Object to Direct Marketing

The data subject has the right to object to the processing of his/her personal information for purposes of direct marketing by means of unsolicited electronic communications.

2.5 The Right to Complain to the Information Regulator

The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his/her personal information.

2.6 The Right to be Informed

The data subject has the right to be notified that his/her personal information is being collected by the Company. He/she also has the right to be notified in any situation where the Company has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

3. GENERAL GUIDING PRINCIPLES

All employees and persons acting on behalf of the Company will at all times be subject to, and act in accordance with, the following guiding principles:

3.1 Accountability

Failing to comply with POPIA could potentially damage Rokwil's reputation or expose the Company to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

The Company will endeavour to ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with. However, the Company will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

3.2 Processing Limitation

The Company will ensure that personal information under its control is processed:

- In a fair, lawful and non-excessive manner; and
- only with the informed consent of the data subject; and
- only for a specifically-defined purpose.

The Company will inform the data subject of the reasons for collecting his/her personal information and obtain written consent prior to processing personal information.

The Company will under no circumstances distribute or share personal information between separate legal entities, associated organisations (such as subsidiary companies) or with any

individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other aspects of the Company's business and be provided with the reasons for doing so.

3.3 Specific Purpose

All of the Company's sites and offices must be informed by the principle of transparency. Rokwil will process personal information only for specific, explicitly defined and legitimate reasons. The Company will inform data subjects of these reasons prior to collecting or recording the data subject's personal information.

3.4 Limitation on Further Processing

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose. Therefore, where the Company seeks to process personal information it holds for a purpose other than the original purpose for which it was first collected, and where this secondary purpose is not compatible with the original purpose, the Company will first obtain additional consent from the data subject.

3.5 Information Quality

The Company will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading.

The more important it is that the personal information be accurate (eg beneficiary details of a life insurance policy), the greater the effort the Company will put into ensuring its accuracy. Where personal information is collected or received from third parties, the organisation will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources.

3.6 Transparency/Openness

The Company will take reasonable steps to ensure that data subjects are notified that their personal information is being collected, including the purpose for which it is being collected and processed.

The Company can be contacted via email on info@rokwil.com should a client or employee wish to enquire whether Rokwil holds related personal information, request access to related personal information, request the Company updates or corrects personal information or make a complaint concerning the processing of personal information.

3.7 Security Safeguards

The Company will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.

Security measures will also be applied in relation to particularly sensitive information. The more sensitive the information, such as medical information or credit card details, the greater the security in place.

The Company will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the Company's IT network. All paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.

All new employees are required to sign employment contracts containing terms for the use and storage of employee information. Confidentiality clauses have also been included to reduce the risk of unauthorised disclosures of personal information for which the Company is responsible.

All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment contract containing the relevant consent and confidentiality clauses.

3.8 Participation of Individuals

A data subject may request the correction or deletion of his/her personal information held by the Company. The Company will ensure that it provides a facility for data subjects who want to request the correction or deletion of their personal information.

Details of the procedure to follow when requesting the correction or deletion of personal information can be found in the Company's Promotion of Access to Information Act (PAIA) Section 51 Manual which is available on the website www.rokwil.com.

4. COLLECTION AND USE OF PERSONAL INFORMATION

The Company collects and processes various information pertaining to its employees and clients. The type of information will depend on the need for which it is collected and will be processed for that process only. Whenever possible, the Company will inform the client or employee of the information required and which information is deemed optional.

The Company must indicate to the employee or client the consequence of failing to provide such personal information and also indicate any prejudice which may be incurred due to non-disclosure. For example, the Company may not be able to employ an individual without certain personal information relating to that individual or the Company may not be in a position to render services to a client in the absence of certain information which is required.

Examples of the personal information the Company collects includes, but is not limited to:

- Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of an employee
- Information relating to the education or the medical, financial, criminal or employment history (this includes disciplinary action) of an employee
- Banking and account information

- Contact information
- Any identifying number, symbol, email address, telephone number, location information, online identifier or other particular assignment to the employee or client
- The biometric information of the employee and client
- The personal opinions, views or preferences of an employee (also performance appraisals or correspondence) and the views or opinions of another individual about the person

4.1 Collection of Employee Information

For the purposes of this Policy, employees include potential, past and existing employees of the Company.

The Company will, when appointing new employees, require information, including, but not limited to that listed above, from the prospective employee in order to process the employee's information on the Company's system. Such information is reasonably necessary for the Company's record purposes as well as to ascertain if the prospective employee meets the requirements, for the position which he is being appointed, and is suitable for appointment.

The Company will use and process such employee information, as set out below, for including, but not limited to, its employment records and to make lawful decisions in respect of that employee and its business.

4.2 Use of Employee Information

Employees' personal information will only be used for the purpose for which it was collected and intended. This would include, but is not limited to:

- submissions to the Department of Labour
- submissions to the Receiver of Revenue
- for audit and recordkeeping purposes
- in connection with legal proceedings
- in connection with and to comply with legal and regulatory requirements
- in connection with any administrative functions of the Company
- disciplinary action or any other action to address the employee's conduct or capacity
- in respect of any employment benefits that the employee is entitled to
- pre- and post-employment checks and screening
- any other relevant purpose to which the employee has been notified of

Should information be processed for any other reason, the Company will inform the employee/s accordingly.

The Company acknowledges that personal information may only be processed if certain conditions are met:

- The employee consents to the processing
- The processing is necessary
- The processing complies with an obligation imposed by law on the Company
- Processing protects a legitimate interest of the employee

Processing is necessary for pursuing the legitimate interests of the Company or of a third party to whom information is supplied

4.3 Collection of Client Information

For purposes of this Policy, clients include potential, past and existing clients.

The Company collects and processes its clients' personal information, such as that mentioned hereunder. The type of information will depend on the need for which it is collected and will be processed for that purpose only. Further examples of personal information collected from clients include, but is not limited to:

- The client's identity number, name, surname, address, postal code
- The client's residential and postal address
- Contact information
- Banking details
- Company registration number
- Full name of the legal entity
- Tax and/or VAT number
- Details of the person responsible for the client's account

The Company also collects and processes clients' personal information for marketing purposes in order to ensure that our products and services remain relevant to our clients and potential clients.

4.4 Use of Client Information

The client's personal information will only be used for the purpose for which it was collected and as agreed. This may include, but not be limited to:

- Providing products or services to clients
- In connection with sending accounts and communication to a client in respect of services rendered
- Referral to other service providers
- Confirming, verifying and updating client details
- Conducting market or customer satisfaction research
- For audit and record keeping purposes
- In connection with legal proceedings
- In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law

The Company acknowledges that personal information may only be processed if any of the conditions set out hereunder are met:

- Client consents to the processing
- The processing is necessary
- The processing complies with an obligation imposed by law on the Company
- Processing protects a legitimate interest of the client

- Processing is necessary for pursuing the legitimate interests of the Company or of a third party to whom information is supplied

5. DISCLOSURE OF PERSONAL INFORMATION

The Company may share employees' and clients' personal information with third parties as well as obtain information from such third parties for reasons set out above.

The Company may also disclose employees' or clients' information where there is a duty or a right to disclose in terms of applicable legislation, the law or where it may be necessary to protect the Company's rights.

6. SAFEGUARDING PERSONAL INFORMATION AND CONSENT

It is a requirement of POPIA to adequately protect the personal information the Company holds and to avoid unauthorised access and use of personal information. The Company will, therefore, ensure that informed consent is obtained from the employee or client where necessary.

The Company shall review its security controls and processes on a regular basis to ensure that personal information is secure.

The Company's Information Officer is responsible for the encouragement of compliance with the conditions of the lawful processing of personal information and other provisions of POPI.

Information Officer Details

Name: Rod Stainton
Telephone number: 031 003 0896
Address: 8 Bishops Court, Warrior Road, Hillcrest, 3630
Email address: info@rokwil.com

Each new employee will be required to sign an employment contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPIA.

Every employee currently employed within the Company will be required to sign an addendum to their employment contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI.

The Company's suppliers, insurers and other third-party service providers will be required to sign a service level agreement guaranteeing their commitment to the Protection of Personal Information; this is, however, an ongoing process that will be evaluated as required.

Consent to process client information is obtained from clients (or a person who has been given authorisation from the client to provide the client's personal information) during the introductory, appointment and needs analysis stage of the relationship.

7. SECURITY BREACHES

Should the Company detect a security breach on any of its systems that contain personal information, the Company shall take the required steps to assess the nature and extent of the breach in order to ascertain if any information has been compromised.

The Company shall notify the affected parties should it have reason to believe that their information has been compromised. Such notification shall only be made where the Company can identify the data subject to which the information relates. Where it is not possible it may be necessary to consider website publication and whatever else the Information Regulator prescribes.

Notification will be provided in writing by means of either:

- email
- registered mail
- place on our website

The notification shall provide the following information where possible:

- description of possible consequences of the breach
- measures taken to address the breach
- recommendations to be taken by the data subject to mitigate adverse effects
- the identity of the party responsible for the breach

In addition to the above, the Company shall notify the Information Regulator of any breach and/or compromise to personal information in its possession and work closely with and comply with any recommendations issued by the Information Regulator.

8. ACCESS AND CORRECTION OF PERSONAL INFORMATION

Employees and clients have the right to request access to any personal information that the Company holds about them.

Employees and clients have the right to request the Company to update, correct or delete their personal information on reasonable grounds. Such requests must be made to the Company's Information Officer (see details in point 6 above) or to the Company's head office at 8 Bishops Court, Warrior Road, Hillcrest.

Where an employee or client objects to the processing of their personal information, the Company may no longer process said personal information. The consequences of the failure to give consent to process the personal information must be set out before the employee or client confirms his/her objection.

The client or employee must provide reasons for the objection to the processing of his/her personal information.

9. RETENTION OF RECORDS

The Company shall ensure the safeguarding and protection of all personal information or data. The Company is obligated to retain certain information as prescribed by law. This includes but is not limited to the following:

With regard to the Companies Act, No. 71 of 2008 and the Companies Amendment Act No 3 of 2011, hard copies of the documents mentioned below must be retained for **seven** 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 meetings, 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 and copies of accounting records as required by the Act.

The Basic Conditions of Employment Act No. 75 of 1997, as amended requires the Company to retain records relating to its staff for a period of no less than **three** years.

10. POPI COMPLAINTS PROCEDURE

A complaint form (Annexure 1) may be completed and emailed to the Information Officer at info@rokwil.com.

11. DISCIPLINARY ACTION

Where a POPI complaint or infringement has been finalised, the Company may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.

In the case of ignorance or minor negligence, the Company will undertake to provide further awareness training to the employee.

Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which the Company may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

12. POLICY AMENDMENTS

Amendments to this Policy will take place from time to time subject to the discretion of the Company and pursuant to any changes in the law. Such changes will be brought to the attention of employee's clients where it affects them.