



...Treats Rust Rite Everytime...

PROTECTION OF PERSONAL INFORMATION
&
PROMOTION OF ACCESS TO INFORMATION POLICY

Introduction

As a responsible party, Rustrite (Pty) Ltd, (“the Company”) is obliged to comply with the Protection of Personal Information Act (No. 4 of 2013) (“POPI”) as well as the Promotion of Access to Information Act (No. 2 of 2000) (“PAIA”), given that it processes the personal information of its employees, suppliers, applicants/ account holders, clients and other data subjects from time to time.

In addition, the Company acknowledges that there may be requests for information relating to the requesting data subject, the Company and/ or its operations.

Purpose

Pursuant to the above, this Policy is drafted to give effect to a data subjects rights under POPI and to outline the Company’s commitment to protecting data subject privacy as well as ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

POPI requires that the Company inform its data subjects as to how their personal information is collected, processed, secured, disclosed and destroyed. To this end, the Company will ordinarily highlight the purpose of collection of information to the data subject and the time of collection with the purposes of obtaining consent from the data subject. This information can ordinarily be found in the following documents:

1. Contracts of employment;
2. Credit application and surety forms,
3. Correspondence with data subject;
4. Service Level Agreements.

Notwithstanding the above, the purpose of this Policy is to further set out the manner in which the Company deals with such personal information as well as stipulates the general purpose for which general information is used relating to data subjects the Company engages with. Where information is used for reasons outside of those expressed, the data subject will be informed.

The provisions of this policy must be read along with the relevant practices and procedures that are used to operationalise the purpose hereof.

This Policy further outlines the standards expected of employees of the Company in respect of their conduct when collecting, processing and otherwise handling personal information within the business.



...Treats Rust Rite Everytime...

PAIA Manual

A copy of the Section 10 PAIA guide is posted on the website in all official languages (as provided by the Information Regulator) and said Guide is available at each of the Company's offices (see addresses above) for public inspection.

The list of records that are voluntarily disclosable and/ or available without a requester having to request access thereto shall be kept and updated monthly and/ or whenever the contents change. The said list shall be posted on the website, registered with the Information Regulator and kept in hard copy at the offices of the Company from time to time.

A requester who requests access to a record under PAIA statute shall complete the necessary form and follow the protocols required. Refer our website for relevant forms.

Appropriate stakeholders should be made aware of the contents of this Policy when their consent is requested for the processing of their personal information or when there are interactions with data subjects.

Collection of Personal Information

The Company collects stores and processes personal information pertaining to data subjects including its employees, suppliers, applicants/ account holders, sureties, clients and other stakeholders. The type of information collected and processed will depend on the purpose for which it is collected and will be processed for that scope of application only. Whenever appropriate, the Company will inform the data subject of the information required, the purpose thereof, the rights of participation and the other relevant provisions contained at law. Same shall be set out in the agreements or correspondence with such data subject.

The Company will indicate to the data subject the consequence of failing to provide such personal information. 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 or permissions to access information which is required.

Examples of the personal information the company collects includes, but is not limited to information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person –

- a) 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 the person;
- b) information relating to the education or the medical, financial, criminal or employment history of the person;
- c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person
- d) the biometric information of the person;
- e) the personal opinions, views or preferences of the person;



...Treats Rust Rite Everytime...

- f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- g) the views or opinions of another individual about the person; and
- h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

Collection of Employee Information

For the purposes of this Policy, “employees” include potential, past and existing employees of the company.

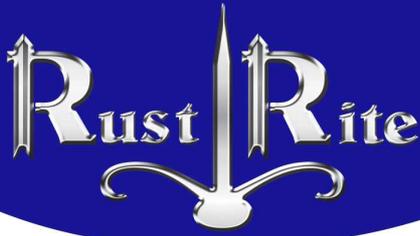
The Company will, when appointing new employees, require information including but not limited to that listed above from the prospective employee in order to process the employee’s information on the company’s system. Such information is reasonably necessary for the Company’s record purposes as well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

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

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:

- a) Submissions to the Department of Employment and Labour
- b) submissions to the Receiver of Revenue
- c) for audit and recordkeeping purposes
- d) in connection with legal proceedings
- e) in connection with and to comply with legal and regulatory requirements
- f) in connection with any administrative functions of the Company
- g) disciplinary action or any other action to address the employee’s conduct or capacity
- h) in respect of any employment benefits that the employee is entitled to
- i) pre-and post-employment checks and screening
- j) any other relevant purpose to which the employee has been notified of



...Treats Rust Rite Everytime...

- k) any compliance requirements at law.

Should information be processed for any other reason that is not in the legitimate interests of the employee or Company, the Company will inform the employee accordingly.

The Company acknowledges that personal information may only be processed if certain conditions are met which, depending on the merits include -

- a) The employee consents to the processing
- b) The processing is necessary to attend to justifiable rights and obligations, for example contractual fulfilment
- c) The processing complies with an obligation imposed by law on the company
- d) Processing protects a legitimate interest of the employee
- e) Processing is necessary for pursuing the legitimate interests of the company or of a third party to whom information is supplied.

Collection of Client, Applicant/ Account Holder and/ or Supplier Information

For purposes of this Policy, clients and applicants/ account holders, include potential, past and existing clients or applicants / account holders.

The Company collects and processes personal information, such as that mentioned hereunder for the purposes of executing the obligations in terms of the agreement with the client, supplier or applicant/ account holder. 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:

- a) identity number, name, surname, address, postal code
- b) business, residential and/or postal address
- c) Contact information
- d) Banking details and financial details (including expenses and liabilities)
- e) Company registration number
- f) BBBEE status
- g) Auditor information
- h) Full name of the legal entity
- i) Tax and/or VAT number



...Treats Rust Rite Everytime...

- j) Details of the person responsible for the client's account
- k) Details relating to judgments against the data subject

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.

The Company's suppliers who fall within the definition of "operators" will be required to enter into a written agreement guaranteeing their commitment to the Protection of Personal Information.

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

Use of Client and Supplier Information

Personal information will only be used for the purpose for which it was collected, as agreed and as required in law. This may include, but not be limited to:

- a) Providing products and/ or services to clients
- b) In connection with sending accounts and communication in respect of services rendered
- c) Assessing credit worthiness
- d) Confirming, verifying and updating client details
- e) Conducting market or customer satisfaction research
- f) For audit and record keeping purposes
- g) In connection with legal proceedings
- h) In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.
- i) Referral to other service providers
- j) Verification of information provided by data subject
- k) Suretyship agreements and obligations

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

- a) Client consents to the processing



...Treats Rust Rite Everytime...

- b) The processing is necessary to attend to rights and obligations that are justifiable, including fulfilling contractual provisions
- c) The processing complies with an obligation imposed by law on the company
- d) Processing protects a legitimate interest of the party
- e) Processing is necessary for pursuing the legitimate interests of the company or of a third party to whom information is supplied.

Disclosure of Personal Information

Subject to legislative provisions providing the contrary, and agreements with the data subject concerned, the company may share data subject's personal information with third parties as well as obtain information from such third parties for reasons set out above or to execute the obligations in the agreement.

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

Safeguarding Personal Information and Consent

It is a requirement of POPI to adequately protect the personal information the Company holds and to avoid unauthorised access and use of personal information.

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

The Company has appointed an Information Officer who is responsible for the encouragement of compliance with the conditions of the lawful processing of personal information and other provisions of POPI and PAIA.

Information Officer Details:

FULL NAME	GREGORY MEAKER
DESIGNATION	DIRECTOR
EMAIL	popi@rustrite.co.za
CONTACT NUMBERS	+27 21 903 0215
FAX NUMBER	+27 21 903 0217
POSTAL ADDRESS	PO Box 131, Kuils River, 7579
PHYSICAL ADDRESS	24 Fabriek Street, Kuils River, 7580

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 POPI.



...Treats Rust Rite Everytime...

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.

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.

In the event any data subject to which the Company interacts with is aware of a data breach or suspected data breach, they are required to immediately notify the Information Officer of the Company.

The Company shall activate its Incident Response Plan which includes the notification of the affected parties, and the Information Regulator should it have reason to believe that personal 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 to identify all affected data subjects, it may be necessary to consider website publication and whatever further direction the Information Regulator prescribes.

Notification will be provided in writing by means of either:

- ✓ email
- ✓ registered mail
- ✓ place on our website.

Data subjects are requested to ensure their email and address are regularly updated so that notification can be sent to the latest address.

The notification shall provide the following information where possible:

- a) description of the possible consequences of the breach,
- b) measures taken to address the breach,
- c) recommendations to be taken by the data subject to mitigate adverse effects,
- d) the identity of the party responsible for the breach.

In addition to the above, the Company shall notify the 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 Regulator.

All incidents of breach or suspected breach will be recorded in a register kept by the Information Officer.

The following provisions will apply in this regard –



...Treats Rust Rite Everytime...

- a) The Information Officer will be responsible for overseeing the investigation;
- b) The Information Officer will be responsible for reporting to the Information Regulator within 2 working days of a breach/ compromise to personal information;
- c) The Information Officer will be responsible for reporting to the Data Subject(s) within 2 working days of a breach/ compromise to personal information;
- d) The timeframes above are guidelines and depending on the merits of the situation may require earlier or later reporting.

Access and Correction of Personal Information

Data subjects have the right to request access to any personal information that the Company holds about them.

Data subjects 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 above) or to the Company's head office (see details below) or submitted via the website "Information Officer Portal".

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 data subject must provide reasons for the objection to the processing of his/her personal information.

The Information Officer shall record data subject requests on a register.

HEAD OFFICE DETAILS

CONTACT PERSON	CLAUDINE BOTHA
TELEPHONE NUMBER	+27 21 903 3131
EMAIL ADDRESS	pa@dekro.co.za
FAX NUMBER	+27 21 903 0217
POSTAL ADDRESS	PO BOX 131, KUILS RIVER, 7579
PHYSICAL ADDRESS	24 FABRIEK STREET, KUILS RIVER, 7580



...Treats Rust Rite Everytime...

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 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 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 No. 75 of 1997, as amended requires the Company to retain records relating to its staff for a period of no less than 3 years.

In addition, the below guidelines shall apply to information relating to the following legislation:

- ✓ The Close Corporations Act, No 69 of 1984, generally 15 years
- ✓ The Consumer Protection Act, No 68 of 2008, generally 3 years
- ✓ The National Credit Act, No 34 of 2005 ("NCA"), generally 5 years
- ✓ The Electronic Communication and Transaction Act, No 25 of 2002, 1 year
- ✓ The Financial Advisory and Intermediary Services Act, No 37 of 2002, generally 5 years
- ✓ The Compensation for Occupational Injuries and Diseases Act, No 130 of 1993, generally 4 years
- ✓ The Occupational Health and Safety Act, No 85 of 1993, up to 40 years
- ✓ The Insolvency Act, No 24 of 1936, up to 5 years
- ✓ The Employment Equity Act, No 55 of 1998, generally 5 years
- ✓ The Labour Relations Act, No 66 of 1995, generally 3 years
- ✓ The Unemployment Insurance Act, No 63 of 2002, generally 5 years
- ✓ The Income Tax Act, No 58 of 1962, is the Act that governs all the laws relating to income taxes and donations and the Value Added Tax Act, No 89 of 1991, provides for the taxation of the supply of goods and services as well as the importation of goods. The Tax Administration Act, No 28 of 2011, has been effective from 1 October 2012, generally 5 years

Amendments to this Policy

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.

Standards of Conduct required of Employees

In addition to the provisions contained within this POPI policy, the employment contract, the disciplinary code, as well as any other applicable document / policy relating to employees conduct, the following standards of conduct and practice, and their



...Treats Rust Rite Everytime...

accompanying underlying principles, must be complied with at all times and a breach thereof may result in serious disciplinary action and even dismissal for a first offence.

Physical Records and Assets

All physical records containing personal information (PI) as well as any hardware, devices or similar equipment must always be protected from unauthorised access and/ or damage and/ or loss and/ or other prejudice. Reasonable measures must be implemented at the discretion of the employee, in addition to those advised by the employer, to appropriately safeguard information from unauthorized access or use.

Systems and Platforms

Compliance with security requirements in respect of, for example, the following areas is crucial –

- a) Changing, storage and sharing of usernames and passwords
- b) Data back-ups and protection
- c) Limitations on the use of personal devices such as external hard drives or similar storage options, mobile phones and the like

Internal and External Posting of Personal Information of Company Data Subjects

A prohibition on the sharing and/ or posting of PI on any platforms outside of those that are Company approved under specific conditions as well as a total ban on posting and/ or transmitting PI outside of the Company on social media and/ or any other similar platform.

Conditions to be observed when collecting or Processing PI

The following principles must be complied with when dealing with PI and if there is any doubt, the written authority of the Information Officer must be obtained by the employee prior to the said processing –

1. Accountability

The employee must ensure that the conditions and all the measures that give effect to such conditions are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

2. Processing limitation

Personal information must be processed

- a) lawfully; and
- b) in a reasonable manner that does not infringe the privacy of the data subject.

This includes considerations of minimality and adequacy given the purpose for which it is intended. In addition -

- a) The data subject or a competent person (data subject is a child) consents to the processing; or/ and
- b) The purpose is to carry out actions for the conclusion or performance of a contract; or/ and
- c) Processing complies with an obligation imposed by law on the responsible party; or/ and
- d) Processing protects a legitimate interest of the data subject; or/ and
- e) Processing is necessary for the proper performance of a public law duty by a public body; or/ and
- f) Processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied; or/ and
- g) Collection must be directly from the data subject, except as otherwise provided for unless the information is contained in or derived from a public record or has deliberately been made public by the data subject.

3. Purpose Specification

PI is collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.

4. Further Processing Limitation

Further processing of personal information must be compatible with the purpose for which it was collected and consider -

- a) the consequences of the intended further processing for the data subject
- b) the manner in which the information has been collected; and
- c) any contractual rights and obligations between the parties.

5. Security Safeguards

Employees must secure the integrity and confidentiality of personal information in their possession or under their control by taking appropriate, reasonable technical and organisational measures to prevent—

- a) loss of, damage to or unauthorised destruction of personal information; and
- b) unlawful access to or processing of personal information.

Employees must take reasonable measures to—

- a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under their control;
- b) establish and maintain appropriate safeguards against the risks identified;
- c) regularly verify that the safeguards are effectively implemented; and
- d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

Employees must have due regard to **generally accepted information security practices and procedures** which may apply to the situation generally or be required in terms of specific industry or professional rules and regulations.

Additional security safeguards guidelines to be observed –

- ✓ Only share PI on a need-to-know basis,
- ✓ Security systems including anti-virus and malware detections (and install updates immediately)
- ✓ Secure and back-up files
- ✓ Encryption
- ✓ Password security, protection and authentication
- ✓ Use multifactor identification,
- ✓ BYOD protocols agreed before allowing use
- ✓ Keep mobile devices safe
- ✓ Accessing suspect links, pop-ups and unknown mails prohibited
- ✓ Only use secure Wi-Fi
- ✓ Firewall protection at work and at home
- ✓ Report any security concerns and warnings
- ✓ Limit employee and user access in general
- ✓ Monitor 3rd parties
- ✓ Provide education and training
- ✓ Be cautious with unvetted USB's



...Treats Rust Rite Everytime...

- ✓ Install security software updates
- ✓ Be aware of social engineering.

6. Website Privacy Policy

Log Files

www.rustrite.co.za follows a standard procedure of using log files. These files log visitors when they visit websites. All hosting companies do this as a part of hosting services' analytics. The information collected by log files include internet protocol (IP) addresses, browser type, Internet Service Provider (ISP), date and time stamp, referring/exit pages and possibly the number of clicks. These are not linked to any information that is personally identifiable. The purpose of the information is for analysing trends, administering the site, tracking users' movement on the website and gathering demographic information.

Cookies and Web Beacons

Like any other website, www.rustrite.co.za uses "cookies". These cookies are used to store information including visitors preferences and the pages on the website that the visitor accessed or visited. The information is used to optimize the users experience by customizing our web page content based on visitors browser type and/or other information.

Third Party Privacy Policies

www.rustrite.co.za's Privacy Policy does not apply to other advertisers or websites. Thus, we are advising you to consult the respective Privacy Policies of these third-party ad servers for more detailed information. It may include their practices and instructions about how to opt-out of certain options.

Children's Information

Another part of our priority is adding protection for children while using the internet. We encourage parents and guardians to observe, participate in, and/or monitor and guide their online activity. www.rustrite.co.za does not knowingly collect any Personal Identifiable Information from children under the age of 13. If you think that your child provided this kind of information on our website, we strongly encourage you to contact us immediately and we will do our best efforts to promptly remove such information from our records.

Online Privacy Policy Only

Our Privacy Policy applies only to our online activities and is valid for visitors to our website with regards to the information that they shared and/or collect on www.rustrite.co.za

This policy is not applicable to any information collected offline or vial channels other than this website.

Consent

By using our website, you hereby consent to our Privacy Policy and agree to its terms.

Breaches of this Policy

Failure to adhere to the principles and rules in this policy shall result in disciplinary action, which may include dismissal where appropriate.



Tel: +27 (0) 21 - 903 0215/6 • Fax: +27 (0) 21 - 903 0217 • Email: info@rustrite.co.za

24 Fabriek Street, Kuils River, 7580 • PO Box 131, Kuils River, 7579

...Treats Rust Rite Everytime...

For any further information on the policy, you are directed to contact the IO.

Implementation Date	17 JUNE 2021
Authorized by	GREGORY ALAN MEAKER
<i>This document and its procedures may be amended from time to time at the discretion of management subject to prevailing laws and best practice.</i>	