

PROTECTION OF PERSONAL INFORMATION & PROMOTION OF ACCESS TO INFORMATION POLICY

1. Introduction

- 1.1 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, customers and other data subjects from time to time as well as that there may be lawful requesters of information relating to the company and its operations.
- 1.2 The company is committed to protecting data subject privacy as well as ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.
- 1.3 POPI requires the company to inform its data subjects as to how their personal information is collected, processed, secured, disclosed and destroyed.
- 1.4 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.
- 1.5 The Information Officer shall ensure that a PAIA guide is posted on the website and that the said Guide is available at each of its offices for public inspection. A requester who requests access to a record under PAIA statute shall complete the necessary form and follow the protocols required.
- 1.6 The provisions of this policy must be read along with the relevant practices and procedures that are used to operationalise the purpose hereof.

2. Definition of Personal Information (PI)

- 2.1 “Personal information” means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—
 - (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;
 - (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.

3. Collection of personal information

- 3.1 The company collects stores and processes personal information pertaining to data subjects including its employees, suppliers, customers 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.
- 3.2 The company may 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 able to render services to a customer in the absence of certain information which is required.
- 3.3 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;
 - 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.

4. Collection of customer and/or supplier information

- 4.1 For purposes of this Policy, customers/suppliers include potential, past and existing customers.
- 4.2 The company collects and processes its customer/supplier 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 customer/supplier include, but is not limited to:
- ✓ The customer's identity number, name, surname, address, postal code
 - ✓ The customer'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 customer/supplier account
- 4.3 The company also collects and processes customer/supplier personal information for sales and marketing purposes and to ensure that our products and services remain relevant to our customer/supplier.
- 4.4 The customer/supplier personal information will only be used for the purpose for which it was collected and as agreed, if any such agreement is required at law. This may include, but not be limited to:
- ✓ Providing products and/ or services to customers
 - ✓ In connection with sending accounts and communication in respect of services rendered
 - ✓ Processing sales/purchases of products
 - ✓ Receiving or making payments
 - ✓ Referral to other service providers
 - ✓ Confirming, verifying and updating customer/supplier details
 - ✓ Conducting market or customer/supplier 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.
- 4.5 The company acknowledges that personal information of customer/supplier' may only be processed if any of the conditions set out hereunder are met:
- ✓ Customer consents to the processing
 - ✓ The processing is necessary to attend to rights and obligations that are justifiable, including fulfilling contractual provisions
 - ✓ The processing complies with an obligation imposed by law on the company
 - ✓ Processing protects a legitimate interest of the party
 - ✓ 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**
- 5.1 Subject to legislative provisions providing the contrary, 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.
- 5.2 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.
- 6. Safeguarding personal information and consent**
- 6.1 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.
- 6.2 The company shall review its technical and operational security controls and processes to protect personal information.
- 6.3 The Company shall appoint 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.

- 6.4 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.
- 6.5 Consent to process customer/supplier information is obtained from data subjects (or a person who has been given authorisation from the customer to provide the customer's personal information) during the introductory, appointment and needs analysis stage of the relationship.

7. Security breaches

- 7.1 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.
- 7.2 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 it may be necessary to consider website publication and whatever else the Information Regulator prescribes.
- 7.3 Notification will be provided in writing by means of either:
- ✓ email
 - ✓ registered mail
 - ✓ place on our website.
- 7.4 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.
- 7.5 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.
- 7.6 The following provisions will apply in this regard –
- ✓ The Information Officer will be responsible for overseeing the investigation;
 - ✓ The Information Officer will be responsible for reporting to the Information Regulator within 2 working days of a breach/ compromise to personal information;
 - ✓ The Information Officer will be responsible for reporting to the Data Subject(s) within 2 working days of a breach/ compromise to personal information;
 - ✓ The timeframes above are guidelines and depending on the merits of the situation may require earlier or later reporting.

8. Access and correction of personal information

- 8.1 Data subjects have the right to request access to any personal information that the company holds about them.
- 8.2 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 (details available on the company website: <http://www.rancetimber.co.za/>).
- 8.3 Where any person 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 customer confirms his/her objection.

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

9. Retention of records

9.1 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.

10. Amendments to this policy

10.1 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 company stakeholders where it affects them.