DATA PRIVACY POLICY

Vula Vula Research Services (Pty) Ltd ("the Company")

DEFINITIONS

Data Subject means the person to which Personal Information relates;

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 the person's—

a) 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;
b) education or the medical, financial, criminal or employment history;
c) identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier, or other particular assignment;
d) biometric information;
e) personal opinions, views, or preferences;
f) implicitly or explicitly private or confidential correspondence or further correspondence that would reveal the contents of the original correspondence;
g) name 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.

POPIA means the Protection of Personal Information Act 4 of 2013, as amended from time to time, including any regulations and/ or code of conduct made under POPIA.

Processing means any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information, including-

a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use;
b) dissemination by means of transmission, distribution or making available in any other form; or
c) merging, linking, as well as restriction, degradation, erasure, or destruction of information.

1. INTRODUCTION

1.1. The Company is committed to protecting the privacy and security of all Personal Information in the possession or control of the Company or its employees in accordance with POPIA and other applicable laws.

1.2. This document outlines the Data Privacy policy of the Company.

2. SCOPE

2.1. This Policy applies to all employees, directors, subcontractors, agents, and appointees (collectively referred to as Employees). The provisions of the Policy are applicable to both on and off-site Processing of Personal Information.

3. RESPONSIBILITY

3.1. Information Officer

3.2. IT

3.3. All employees (including sub-contractors, temporary staff, associates, partners and suppliers)

4. PRIVACY

4.1. All Employees are required to treat Personal Information as strictly private and confidential.

4.2. All Employees must identify risks to the Personal Information in their possession and take reasonable steps to protect against the risks, such as locking Personal Information away when not in use and encrypting digital files containing Personal Information.

4.3. No employee may:

- 4.3.1. access Personal Information without authorisation;
- 4.3.2. Process Personal Information outside of the scope of their employment duties;
- 4.3.3. Process Personal Information without consent from the Data Subject;
- 4.3.4. Process Personal Information for any unlawful or unauthorised purpose;
- 4.3.5. share or transmit Personal Information to any third party without authorisation;
- 4.3.6. share Personal Information over email unless the Personal Information is encrypted and secure; or
- 4.3.7. transport or transmit Personal Information without implementing appropriate measures to protect Personal Information from unlawful or unauthorised access while being transported or transmitted.

4.4. Every Employee is required to implement a clean-desk policy. No document containing Personal Information may be left unattended. All Personal Information must be locked away and secured at all times.

4.5. On termination of an Employee's relationship with the Company, the Employee must return all Personal Information under their possession or control to the Company. No Personal Information may be retained the Employee following termination of their relationship with the Company.

5. PURPOSE

5.1. In order for the Company to pursue its business objectives and strategies and to comply with the law, the Company and its employees must collect and Process Personal Information.

5.2. Personal Information may be collected for the following purposes:

5.2.1. To meet client contractual requirements;

5.2.2. Conducting credit reference, criminal, or employment history checks and other similar assessments;

5.2.3. Detecting and prevention of fraud, crime, money laundering and other malpractice.

5.2.4. Administration of agreements, including those with employees and supplier;

5.2.5. Asset funding purposes.

5.2.6. Conducting market or customer satisfaction research.

5.2.7. Marketing and sales.

5.2.8. In connection with legal proceedings.

5.2.9. Staff administration, including medical records and assessments.

5.2.10. Keeping of accounts and records.

5.2.11. Complying with legal and regulatory requirements.

5.2.12. Managing human resource development.

5.2.13. To ensure physical security (i.e., CCTV).

5.3. Personal Information may only be collected where permitted by law and for a specified, explicit, and legitimate purpose. Personal Information may not be processed in a way that is incompatible with that purpose.

5.4. If Personal Information must be Processed for a purpose not listed above, written authorisation must be sought from the Employee's Line Manager.

6. RELEVANCE

6.1. Personal Information collected must be relevant and not excessive in relation to the purpose and must only be retained for as long as necessary.

7. CONSENT REQUIREMENT

7.1. Consent must be acquired from all Data Subjects to Process their Personal Information for any purpose, including those identified above.

7.2. Consent forms are available on the company drive.

7.3. Records of consents acquired must be kept by the Employee along with the Personal Information collected. This record should specify:

7.3.1. Date of the consent;

7.3.2. Wording of the consent;

7.3.3. Who obtained the consent;

7.3.4. Proof of opportunity to opt-out on each marketing contact; and

7.3.5. If the Data Subject opted out of marketing.

7.4. If consent is refused by a Data Subject, the Company and its Employees may not engage with the Data Subject or enter into any agreement or relationship with them.

8. ENSURING INFORMATION QUALITY

8.1. Employees are required to, as far as reasonably practicable, ensure the following when collecting Personal Information:

8.1.1. should be dated when received;

8.1.2. a record should be kept of where the Personal Information was obtained;

8.1.3. changes to Personal Information records should be dated;

8.1.4. irrelevant or unnecessary Personal Information should be deleted or destroyed; and

8.1.5. Personal Information should be stored securely, either on a secure electronic database or in a secure physical filing system.

8.2. Records containing Personal Information must be kept accurate and updated when needed and identified errors must be corrected.

9. SECURING PERSONAL INFORMATION

9.1. The Company is legally obliged to provide reasonable, adequate protection for Personal Information and to prevent unauthorised access to and use of Personal Information.

9.2. The Company implements the following measures to protect Personal Information:

9.2.1. Firewalls;

9.2.2. Virus protection software and update protocols;

9.2.3. Logical and physical access control;

9.2.4. Secure setup of hardware and software in the IT infrastructure; and

9.2.5. Various internal policies implementing POPIA.

9.3. If an Employee suspects that Personal Information has been accessed or Processed unlawfully or by an unauthorised person, the Employee must notify the Information Officer and refer to the POPIA: Breach policy.

10. TRAINING

10.1. The Company will provide all Employees with appropriate Privacy Awareness Training and Material.

10.2. Employees are required to familiarise themselves with, and implement, all processes and policies put in place to protect Personal Information.

10.3. Employees must ensure that they participate in any training provided by the Company.

11. DESTROYING PERSONAL INFORMATION

11.1. Personal Information must be destroyed at the request of the Data Subject or if there is no consent, legal justification, or legitimate purpose to have and Process it.

11.2. Where applicable, the Company will notify the relevant client of the Data Subject's exercising of their rights in terms of POPIA.

11.3. Personal Information must be destroyed when there is no longer a purpose for retaining the Personal Information. Destruction of documents and electronic records containing personal Information must be done on a regular basis.

11.4. Files must be checked in order to make sure that they may be destroyed in terms of the Company's Records Management Policy and also to ascertain if there are important original documents in the file.

11.5. Original documents must be returned to the holder thereof, failing which, they should be retained by the Company pending such return.

11.6. Deletion of electronic records must be done in consultation with the IT Department, to ensure that deleted Personal Information is incapable of being reconstructed and/or recovered.

12. REVIEW

12.1. This policy must be reviewed annually or when necessary.