DATA PROTECTION POLICY

1. Introduction

The Baby Cart (“**Provider**”) provides a platform where users of its website can offer, sell and buy the products listed on the website and can bid on and purchase the products on offer through seller auctions listed on the website. For the purposes of carrying out its business and related objectives, the Provider will from time to time, process personal data of individuals and legal entities including public and private entities, such as personal data pertaining to the users of its website, employees and staff, prospective employees and job applicants, service providers and contractors, vendors, and other third parties (“**Personal Data**”).

This Policy seeks to ensure that the Provider:

a) Complies with the South African and international legal standards and best practice for the processing of Personal Data which includes the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, disseminating and destruction of Personal Data.

b) Protects the rights of the users of its website, employees and staff, prospective employees and job applicants, service providers and contractors, vendors, and other third parties ("**Data Subjects"**) in respect of Personal Data processed.

c) Transparently renders how it processes Personal Data of individuals.

d) Mitigates the risks of data breaches.

2. Purpose and Objectives

2.1. The Provider processes Personal Data belonging to Data Subjects on an ongoing basis to carry out and pursue its business and related operational interests. This may include:

a) Recruitment and employment purposes.

b) Concluding contracts and business transactions.

c) For risk assessments, insurance and underwriting purposes.

d) Assessing and processing queries, enquiries, complaints, and / or claims.

e) Conducting criminal reference checks and/or conducting credit reference searches or verification.

f) Confirming, verifying and updating persons details.

g) For purposes of personnel and other claims history.

h) For the detection and prevention of fraud, crime, money laundering or other malpractice.

i) Conducting market or customer satisfaction research.

j) Promotional, marketing and direct marketing purposes.

k) Financial, audit and record keeping purposes.

l) In connection with legal proceedings.

m) Providing services to users of its website to carry out the services requested and to maintain and constantly improve the relationship.

n) Communicating with employees, third parties, customers, suppliers and/or governmental officials and regulatory agencies.

o) In connection with and to comply with legal and regulatory requirements or when it is otherwise required or allowed by law.

2.2. The objective and purpose of this policy is therefore to set out the Provider's policy on the processing of Personal Data and to provide guidelines on how Personal Data is to be processed and safeguarded.

3. Scope

3.1. This policy will apply to the processing by the Provider of all and any Data Subjects' Personal Data.

3.2. This policy, without exception, will apply to:

3.2.1. The Provider and its subsidiary companies, including all employees thereof, including permanent, fixed term, and temporary staff, directors and executives, secondees.

3.2.2. Any entity or person who processes Personal Data on behalf of the Provider, whether residing or operating in South Africa, or overseas, who will hereinafter be referred to as an "operator", provided they have been made aware of this policy.

4. Data Protection principles and conditions

4.1. Personal Data shall always be:

4.1.1. Obtained and processed fairly and lawfully.

4.1.2. Obtained only for specific lawful purposes.

4.1.3. Adequate, relevant and not excessive.

4.1.4. Accurate, and kept up to date.

4.1.5. Held for no longer than necessary for the purpose it was obtained for.

4.1.6. Processed in accordance with the rights of Data Subjects.

4.1.7. Be protected in appropriate ways, methodologies and procedures and according to suitable methods, both organisationally and technologically.

4.1.8. Not be disclosed, transferred or exported illegally, or in breach of any agreement with a Data Subject.

4.2. All employees and where applicable, operators and persons acting on behalf of the Provider, shall continually be responsible for ensuring the safeguarding, protection and avoidance of any unauthorised disclosure or breach of Personal Data in the execution of employment duties and services to the Provider, or otherwise in the course of rendering services or being associated with the Provider.

4.3. Where it is necessary to store Personal Data on portable devices such as laptops, USB flash drives, portable hard drives, CDs, DVDs, employees and where applicable, operators and persons acting on behalf of the Provider without exception must before storing said Personal Data ensure that the Personal Data is encrypted and is kept secure, and that appropriate measures and safeguards are in place to prevent unauthorised access, disclosure and loss of such Personal Data.

4.4. Where paper or hard copies of Personal Data are removed from the Provider's premises, employees, operators and/or persons acting on behalf of the Provider must ensure that only relevant Personal Data is taken. In addition, such Personal Data must be kept safe and secure and appropriate measures and safeguards are taken to prevent any unauthorised access, disclosure and loss of such Personal Data.

4.5. Paper or hard copies of Personal Data and portable electronic devices housing Personal Data should be stored in locked units, which should not be left on desks overnight or in view of other employees or third parties.

4.6. Personal Data which is no longer required should be destroyed or securely archived and retained.

4.7. Personal Data shall be deemed confidential information and shall not be disclosed unlawfully to any third party.

4.8. Personal Data loss must be reported to the relevant manager of the department from where the information emanates and to the Chief Financial, Risk or Compliance Officer.

4.9. Negligent loss or unauthorised disclosure of Personal Data, or failure to report such events, may be treated as a disciplinary matter.

4.10. The Provider will continuously review the security controls and processes to ensure that all Personal Data is secure.