POPIA Policy

Car Vendors (PTY) LTD
118 Adelaide Tambo Drive
Durban North

www.carvendors.co.za

VERSION 1.0.0

15/06/2021

VERSION HISTORY				
VERSION	**APPROVED BY**	**REVISION DATE**	**DESCRIPTION OF CHANGE**	**AUTHOR**
1.0.0	Lee Martin	15 June 2021	Initial Draft	T Nortje

POLICY: PROTECTION OF PERSONAL INFORMATION

1. PURPOSE

The purpose of this policy is to explain the manner in which Car Vendors (PTY) Ltd ('the Company') deals with personal information of Data subjects, and in addition, the purpose for which this information is used.

This policy also serves to protect the Company from compliance risks associated with the protection of personal information which includes:

- Breaches of confidentiality
- Failing to offer choice to Data subjects to choose how and for what purpose their information is used
- Reputational damage.

The policy also demonstrates the Company's commitment to protecting the privacy rights of Data subjects.

2. SCOPE

This document applies to the Company's Directors, all employees, contractors, suppliers, clients, persons acting on behalf of the company and all potential and existing Data subjects.

3. INTRODUCTION

The Protection of Personal Information Act, 4 of 2013 ('POPIA') requires the Company to inform Data subjects as to how their personal information is used, disclosed and destroyed.

The Company is committed to compliance with POPIA and other applicable legislation, protecting the privacy of Data subjects and ensuring that their personal information is used appropriately, transparently and securely.

This policy is made available on the Company's website www.carvendors.co.za/POPIA and should be read in conjunction with the Company's Standard Terms and Conditions.

4. DEFINITIONS

4.1. Personal Information

Personal information means information relating to an identifiable, living, natural person, and where it is applicable, an existing, identifiable juristic person and may include but is not limited to:

- information relating to the race, gender, marital status, national, ethnic or social origin, colour, age, physical or mental health, well-being, disability, language and birth of the person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- the biometric information of the person;
- 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;
- information regarded as confidential business information;
- the views or opinions of another individual about the person; and

- 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.

4.2. **Data subject**

This refers to the natural or juristic person to whom personal information relates, such as employees, clients, delegates, sub-contractors or a company that supplies the Company with goods or services.

4.3. **Processing**

The act or processing information includes any activity or set of operations concerning personal information and includes:

- the collection, receipt, capturing, collation, storage, updating, retrieval, alteration or use;
- dissemination by means of transmission, distribution or making available in any other form; or
- merging, linking, erasure or destruction of information.

5. RIGHTS OF DATA SUBJECTS

The Company will ensure that it makes Data subjects aware of their rights as appropriate and specifically with regards to the following:

5.1. **The right to access personal information**

Data subjects have the right to establish whether the Company holds personal information related to them, including the right to request access to that personal information.

5.2. **The right to have personal information corrected or deleted**

Data subjects also have the right to ask the Company to update, correct or delete their personal information on reasonable grounds.

5.3. **The right to object to the processing of personal information**

Data subjects have the right on reasonable grounds, to object to the processing of their personal information.

The Company will consider such requests and the requirements of POPIA and may cease to process such personal information and may, subject to statutory and contractual record keeping requirements, also destroy the personal information.

5.4. **The right to object to direct marketing**

Data subjects have the right to object to their personal information being used for the purposes of direct marketing by means of unsolicited electronic communications.

5.5. **The right to complain to the Information Regulator**

Data subjects have the right to submit a complaint to the Information Regulator regarding infringements of any of their rights protected under POPIA and to institute civil proceedings against alleged non-compliance with the protection of their personal information.

5.6. **The right to be informed**

Data subjects have the right to be informed that their personal information is being collected by the Company and should also be notified in any situation where the Company reasonably believe that the personal information of data subjects has been accessed by unauthorised person/s.

6. GENERAL GUIDING PRINCIPLES

All employees and persons acting on behalf of the Company will be subject to the following guiding principles:

6.1. **Accountability**

Compliance failure could damage the reputation of the company and its shareholders. The Company could also be exposed to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

The Company will take appropriate steps including disciplinary action against individuals who through intentional or negligent actions and/or omissions fail to comply with this policy.

6.2. **Processing limitation**

The Company collects personal information directly from Data subjects only as it pertains to business requirements. The type of information will depend on the need for which it is collected and will be processed for that purpose only. We will inform Data subjects as to what information is mandatory or deemed optional, as far as possible.

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

- Trade-in valuations;
- Vehicle Test drives and Demo's;
- Fine Management;
- Credit Scoring;
- Retrieving Bank Settlements;
- OEM Recall campaigns;
- Recordkeeping and payment of employees;
- Administration of employment benefits;
- Recording and payment of suppliers;
- Confirming, verifying and updating client information;
- For registration purposes with statutory bodies (CIPC, SARS) and institutions (banks);
- Contractual obligations;
- In connection with legal proceedings;
- In connection with and to comply with legal and regulatory requirements or when allowed by law;
- Marketing activities.

According to Section 10 of POPIA, personal information may only be processed if the purpose for which it is processed, is adequate, relevant and not excessive. Certain conditions must be met for the Company to process personal information as in Section 11 of POPIA. These are listed below:

- Data subjects consent to the processing – consent is obtained during early stages of the relationship.
- Processing is necessary – personal information is required to facilitate the provision of services to the Data subject or for the conclusion of a contract to which the Data subject is a party.
- The Company is under obligation by law.
- The legitimate interest of the Data subject is protected – it is in their best interest to provide the personal information.
- Processing is in the best interest of the Company – in order to provide our services to the Data subject.

6.3. **Further processing limitation**

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose. Where the secondary purpose is not compatible with the original purpose, the Company will first obtain additional consent from the Data subject.

6.4. **Information quality**

The Company will take reasonable steps to ensure that all personal information is complete, accurate and not misleading. Where personal information is collected from third parties, the Company will take reasonable steps to ensure that the information is correct by verifying the accuracy of the information directly with the Data subject or by way of independent sources.

6.5. **Security safeguards**

Section 19 of POPIA requires the adequate protection of personal information that is held by the Company. The Company will continuously review security controls and processes to prevent unauthorised access and use of personal information.

The following procedures are in place to ensure that personal information are secure:

- The Company's Information Officer is the Managing Director whose details are available below and who is responsible for compliance with the conditions and provisions of POPIA;
    - Leanne Martin
    - popia@carvendors.co.za
- The Company's Information Officer may delegate certain responsibilities to other employees;
- This policy is available from the Company's website;
- Employees will be trained on this policy and POPIA;
- Each new employee will be required to sign an employment contract that contains relevant consent and confidentiality clauses for the use and storage of personal information, 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 and confidentiality clauses for the use and storage of personal information and new and updated policies for the handling of personal data in terms of POPIA;
- The Company's servers are protected by firewalls.

7. **SPECIFIC DUTIES AND RESPONSIBILITIES**

7.1. **Board of Directors**

The Company's Board of Directors is ultimately accountable for ensuring that the Company meets its obligations under POPIA. The Board of Directors may however delegate some of its responsibilities to management or other capable individuals.

7.2. **The Company's Information Officer or the person(s) delegated by the officer is responsible for the following:**

- Taking steps to ensure the Company's reasonable compliance to POPIA;
- Keeping the Board of Directors informed of the Company's information protection responsibilities, for instance in the case of a security breach;
- Reviewing the Company's information protection procedures and policies;
- Ensuring that the Company makes it convenient for Data subjects to communicate with the Company regarding their personal information;
- Approve any contracts entered into which may have an impact on personal information held by the Company;

- Oversee the amendment of employment contracts and other service level agreements;
- Encourage compliance with the lawful processing of personal information;
- Ensure that employees and persons acting on behalf of the Company are aware of the risks associated with the processing of personal information;
- Ensure that employees are trained in the processing of personal information;
- Address POPIA related questions;
- Address POPIA related requests and complaints made by Data subjects;
- Act as contact point for the Information Regulator on issues pertaining to the processing of personal information; and
- Approving and maintaining the protection of personal information statements and disclaimers that are displayed on the Company's website, including those attached to communications such as emails and electronic newsletters.

7.3. **The Company's Executive Manager in charge of Information Technology or the person(s) delegated by said manager is responsible for:**

- Ensuring that the Company's IT infrastructure and any other devices used for processing personal information meet acceptable security standards;
- Ensuring that servers containing personal information are sited in a secure location;
- Ensuring that all electronically stored information is backed-up and tested on a regular basis;
- Ensuring that all back-ups are protected from unauthorised access, accidental deletion and malicious hacking attempts;
- Ensuring that information being transferred electronically is encrypted;
- Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software;
- Performing regular IT audits to ensure that the security of the Company's hardware and software systems are functioning properly;
- Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by unauthorised persons; and
- Performing a proper due diligence review prior to contracting with third party providers to process personal information on the Company's behalf.

7.4. **Employees and other persons acting on behalf of the Company are responsible for:**

- Keeping all personal information that they come into contact with secure by taking precautions and complying with this policy;
- Ensuring that personal information is kept in as few places as is necessary;
- Ensuring that personal information is encrypted prior to sharing the information electronically;
- Ensuring that all devices such as computers, flash drives, etc. are password protected and never left unattended (refer to the Company's Electronic Communications policy);
- Ensure that computer screens and other devices are switched off when not in use;
- Ensure that removable storage devices such as external drives that contain personal information are locked away securely when not being used;

- Ensure that where personal information is stored on paper, that such hard copies are kept in a secure place where unauthorised persons are not able to access it;
- Ensure that where personal information has been printed out, that the printouts are not left unattended where unauthorised individuals could see them;
- Take reasonable steps to ensure that personal information is stored only for as long as it is needed or required.

Employees and other persons acting on behalf of the company will under no circumstances:

- Process personal information where it is not a requirement to perform their work-related duties;
- Save copies of personal information directly to their own private computers or mobile devices; and
- Share personal information informally.

When an employee, or a person acting on behalf of the Company, becomes aware or suspicious of any security breach of personal information, he or she must immediately report this to the Information Officer.

8. **DISCIPLINARY ACTION**

The Company may recommend appropriate legal or disciplinary action to be taken against any employee found to be implicated in any non-compliant activity outlined within this policy.

Any gross negligence or intentional mismanagement of personal information will be considered a serious form of misconduct under the Company's Disciplinary code and may lead to dismissal.

Examples of actions that may be taken subsequent to an investigation include:

- A recommendation to commence with disciplinary action
- A referral to law enforcement agencies for criminal investigation
- Recovery of funds in order to limit any damages caused.