POPI Act Compliance Manual

K2014228501 (SA) (Pty) Ltd

(Registration Number: 2014/228501/07)

Published in terms of the Promotion of Access to Information Act 2 of 2000 (PAIA) as amended to the Protection of Personal Information Act 4 of 2013 (POPI Act)

Table of contents

1. Introduction

What is the POPI Act?

Protection of Personal Information Act.

To promote the protection of personal information processed by public and private bodies; to introduce certain conditions so as to establish minimum requirements for the processing of personal information; to provide for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of this Act and the Promotion of Access to Information Act, 2000; to provide for the issuing of codes of conduct; to provide for the rights of persons regarding unsolicited electronic communications and automated decision making; to regulate the flow of personal information across the borders of the Republic; and to provide for matters connected therewith.

Reference: Government Gazette, 26 November 2013, Act nr4 of 2013, Protection of Personal Information Act, 2013

2. Purpose of the Manual

This manual provides and outline the type of records and personal information the business holds, how it is protected and where it is stored. The POPI act gives effect to everyone's constitutional right of access to information held by the private and public sectors.

Requests to view this manual can be made to the Information Officer and the Finance Director. The contact details of these individuals are available:

Information Officer	René Blom rene@drawbridge.co.za 084 670 3334
Group Financial Manager	Estelle Steyn estelle@claremont.co.za 083 786 2751

Information & Deputy Officers:

The Information Officer for the group is René Blom and a Deputy Officer was nominated within each of the dealerships.

The role of the Information Officer is to supply and enforce the relevant POPI guidelines to the dealerships with the assistance of the Deputy Officers.

The Deputy Officer is the Finance Manager of the relevant Dealerships. The Deputy Officers needs to ensure that the rules and structures set out by the Information Officer, in line with the current POPI Act 4 of 2013, is implemented, monitored and adhered to within each dealership.

The Deputy Officers are:

Haval Malmesbury	Heila Vos heila@havalmalmesbury.co.za 066 265 2003 022 482 3831
Haval Vredenburg	Heila Vos heila@havalmalmesbury.co.za 066 265 2003 027 713 1277

Company Details:

K2014228501 (SA) (Pty) Ltd conducts business in the automotive industry by selling and buying cars and conducting repairs and services on cars.

Within the group there are two dealerships in total:

- Haval Malmesbury
  36 Bokomo Street
  Malmesbury, 7300
  022 482 3831

- Haval Vredenburg
  18 Saldanha road
  Vredenburg
  027 713 1277

Availability of the manual

The manual is available for viewing in terms of the section 4 of the regulations of the POPI Act. This manual will also be made available on the company's website for viewing by all clientele and personnel.

The file itself is kept at the head office in Claremont, Cape Town and copies of the manual can be obtained by the Information Officer or Deputy Officer at each dealership.

3. Protection of information

In order to run the business, the K2014228501 (SA) Group requires personal information of its employees and clients. Often this information may need to be supplied in electronic format and/or a hard copy. An appropriate level of security will be adhered to in relation to the storage of such information and used when communication needs to be done with said information.

Within the motor industry, clients supply their private information to apply for finance to purchase a vehicle or sell a vehicle on a daily basis. The purpose of this Compliance Manual is to outline the methods and processes put into place to ensure the information supplied by the clients, businesses and employees are protected, safe and destroyed accordingly after said expiration date.

The business agrees to:

- Notify the relevant individual when information is collected by the company;
- What the purpose and intent is of obtaining said information;
- What the information will be used for;
- Obtain consent from the individual with whom the company is in business with;
- To share the information collected with third party's such as an insurance company only when the individual/client/data subject has agreed to the share of information;.
- Request the correction, removal and option to amend the information provided.

The information supplied by the client/employee will be treated as confidential and the information will be only be used for the purpose for which it was intended too.

3.1 Employee information

Employment contracts
The employee contracts and information provided are in hard copy format. These documents are then scanned and saved in a secure location, online. The hard copies are kept in a file room, with minimal and monitored access, behind a lock and key.

Applications – CV's submissions
CV's received from applicants are received directly from applicants and agencies, who have received consent to have the CV's shared. These CV's are kept on a server and shared with relevant managers in a secure format such as a zipped folder.

Payslips (VIP)
All payslips are printed by the Financial Manager and shared with the relevant employees in person. All outdated and old payslips that an employee may request can be generated through the VIP System and will be sent through on email to the employee, encrypted and password-pdf protected.

Code of Conduct & Training
All employees have undergone training and all new employees will receive the relevant POPI training on their first day when they commence employment.

Furthermore, as part of the employment contract a POPI Declaration is signed that ensures the employee is fully aware of the Act, and confirm that he/she agrees with the Act and the regulations outlined by the Act. This way the employee is also fully aware of the company expectancy with reference to the guidelines set out by the POPI Act and what the outcome would be, should an employee be found guilty of not adhering to the POPI Act.

Reference of this contract is in the POPI File held by the Information Officer.

3.1.1 The collection and processing of employee's personal information

The Employee acknowledges that the employment relationship requires the Employer to collect, organize, process and store certain personal information of the Employee.

The personal information is necessary:

a) for purposes of screening, appointments, training and development, performance management, administration, employment relationship issues, termination of employment and any other employment-related purposes; and

b) to enable the Employer to comply with its obligations under South African laws and regulations.

c) The Employee acknowledges and agrees that the Employer may:

i. process such personal information for the above-mentioned purposes.

ii. share relevant personal information with third parties (including his/her medical aid/ pension fund administrators, government departments, bargaining council) where this is necessary or legally required.

d) For purposes of this agreement, the term “Personal Information” includes Special Personal Information such as the employee’s race, health, biometric information and /or trade union status.

e) The Employee may review and update his personal Information from time to time by contacting the Financial Manager directly.

3.1.2 Personal information of other employees, suppliers or customers

The Employee may, in the performance of his employment duties, gain access to the personal information of other employees, third party suppliers and/or customers.

The Employee accordingly undertakes and agrees that he will:

a) treat such personal information as strictly confidential;

b) process the personal information only for purposes of carrying out his duties to the Employer;

c) fully comply with the Employer's policies in respect of processing of personal information;

d) immediately report to the Employer any breach of the above obligations, either by himself or a fellow Employee.

e) A failure to comply with the above obligations may result in disciplinary steps, including possible dismissal.

3.2 Client Information

Car Sales

When a Sales Executive engages with a client regarding a prospective sale, the client will sign a document to confirm that his name, address, e-mail address and details of his existing vehicle and all finance agreements will be processed.

When a client purchases a car from the Dealership, various documents need to be completed. One of such documents is the Offer to Purchase (OTP) document. On this document, clients will need to give their consent that they agree to have a third party such as an insurance company reach out to the client with quotes. This forms part of the Limitations section of the 8 Conditions of the POPI Act. The same document would be signed when a vehicle is traded in as part of the purchase sale.

The OTP contains the following section relating to Data Protection:

*I wish to receive promotional communication (**Yes/No**)*

*I wish to receive beneficial information (**Yes/No**)*

I may:

a) Refuse to accept;
b) Inform you in writing to discontinue; or
c) Register a pre-emptive block with the Registry for Direct Marketing against any direct marketing communication from you.

I am required by law to provide you with all the documentation in terms of the Financial Intelligence Centre Act, No. 38 of 2001, and should I fail to provide the required documentation, this offer cannot proceed.

I have authorized you to submit my particulars to the eNatis system for registration of the vehicle on the national database of roadworthy vehicles and licensed drivers.

The Sales Executive is responsible to obtain verbal consent from the client if they are willing to agree to have their photo, name and surname shared on social media.

It then is the responsibility of the Marketing Manager and design team to edit the photo to remove the registration number, if visible in the photograph, before sharing it on social media. Social Media platforms include: Facebook & Instagram.

Servicing a car, Direct purchases (Parts & Accessories)

When a car is booked in for a service, the client will sign a separate document to provide consent that he may be contacted throughout the day to share information regarding his vehicle.

The Job Cards used in the workshop department, the quotes and invoices presented to clients all reflect a disclaimer that advises the client that the company is POPI compliant. The disclaimer also obtains the client/data subject's consent to proceed with reaching out to other businesses with the intent and purpose of assisting the client whilst they are in business with the company. The disclaimer that will appear on the job cards, quote and invoices are as follows:

"Protection of Personal Information Act Disclaimer: We respect your privacy and are committed to protect and responsibly manage your personal information with you. We collect and process your personal information to enable us to provide the services or advice you may require. To comply with the new Protection of Personal Information (POPI) Act, we require your authorisation and consent to process your personal information. By signing this document you agree to give us consent to collect the minimum required information from you in return we will process your personal information only for the purposes for which it was collected or agreed with you to provide and render the relevant services to you. By signing this document, you also provide us with consent to reach out to you in the near future with any marketing related material used for our business. You have the right to at any time ask us to update, correct or have your details removed from our records. You always have the right to object to the processing of your personal information. You have the right to complain to the Information Regulator, whose contact details are: Tel: 012 406 4818/ Email: inforeg@justice.gov.za"

3.3 Online systems and storage

Firewalls

Firewalls are in place to protect the systems used on each device within the dealership. The firewalls alert the head of IT of all issues that may occur that could be harmful to the systems used by the business. This serves as an early warning system. The Firewalls are tested by an external company from time to time to ensure the security infrastructure is sufficient and secure.

VPN

Employees who work remotely from home will require the access of the VPN login which will require their password login, this is a safe and secure format to access information whilst being offsite and out of office.

MFiles

This is the company Document Management System (DMS). It handles the scanning of original documents into a digital format which is stored on the company server. All documents are searchable and retrievable. There are limited users that have access to the Mfiles' platform and use rights are restricted. Documents are kept for up to 10 years, all older documents that are no longer required are physically shredded.

Clear data

This company leaves a secure storge box at the dealerships and clears the box 1-2 times a month, depending on the agreement in place with the specific dealership. Documents that have been completed by clients are scanned prior to being disposed of in the box. Clear Data collects the box and empties it into a shredder.

Outdated hardware

Every three years the laptops and desktops are upgraded to ensure the devices used within the company comply to current security programs and systems. The outdated devices are wiped, and the hard drives are cleared. Desktops and Laptops that have been cleared of all information are either used in the company's training room to educate employees and assist with training programs or they are donated to the less fortunate. On each donation a pre-assessment is done by the IT department to confirm that there aren't any data available on the device anymore that could implicate anyone. Be it an employee or client.

Zip folders

All employees are meant to share client or employee confidential information on email by means of attaching a zipped, password encrypted document. This way the information can be shared internally and externally with another company on a safer platform. An SOP (Standard Operating Procedure) document was shared with all employees and forms part of the day-to-day manner of conducting business.

3.4 WhatsApp Communication

3.4.1 Sharing internal information on WhatsApp

Within the dealerships there are various WhatsApp groups the employees work on to share internal communication.

The following disclaimer was shared, giving the employee the choice to leave the group, or stay out of free will.

DISCLAIMER:
Claremont Holdings Pty Ltd, K2014228501 SA Pty Ltd, Rouxrand Properties Pty Ltd, Bluedust Motor Holdings Pty Ltd, Weskus Motors (EDMS) BPK

With the compliance due date, for the Protection of Personal Information Act, 4 of 2013 ("POPIA"), being 1 July 2021, the deadline introduces a few changes that we are required to implement within our organisation.

Going forward, the company WhatsApp Administrators require your consent to be part of this WhatsApp group.

As such, you are herewith notified that you are entitled to refuse such consent and you may exercise such a right by leaving this group.

Should you elect to remain in this group, it will be accepted that you have consented to being a part of this group and to your personal information (being your mobile phone number and name) being noticeable to any person in this group. In this regard, we request all members, of this group, not to make use of such personal information for whatsoever reason, without obtaining the consent of the relevant person.

Due to the nature of our communications, staff are often shared within this group for the purposes of keeping relevant parties up to date. Please may we ask that you adhere to avoid any further sharing or redistribution of

images or information containing other staff or colleagues without obtaining the relevant consents.

3.4.2 Sharing Client Information on WhatsApp

All employees have been informed during a training session that they are encouraged not to store client information from WhatsApp on their phones. But rather to transfer the data to their work Computer/Laptop to continue working from the devices on the client information. Considering the information is part of the business information and then also covered by the relevant security systems in place provided by the company to protect the information shared. Whilst the Act does not currently fully indicate its compliance/non-compliance with the use of WhatsApp, our employees are encouraged to treat all client information obtained by clients, with their consent with a mindful manner; focusing on protecting information that is meant to be private.

4. List of records the Company would hold

4.1 Records which are freely available (section 51(1)(c) of PAIA)

4.1.1 The following records are automatically available to the public and need not be requested in accordance with the procedure outlined in this Manual:

- brochures;
- information available on the company's website.

4.2 Records held by the Company in terms of other legislation (section 51(1)(d) of PAIA)

4.2.1 The company retains a number of records in accordance with legislation which applies to it, including but not limited to:

- Basic Conditions of Employment Act No 75 of 1997;
- Companies Act No 71 of 2008;
- Compensation for Occupational Injuries and Diseases Act No 130 of 1993;
- Consumer Protection Act No 68 of 2008;
- Copyright Act No 98 of 1978;
- Electronic Communications and Transactions Act No 25 of 2002;
- Employment Equity Act No 55 of 1998;
- Financial Intelligence Centre Act No 38 of 2001;

- Income Tax Act No 58 of 1962;
- Labour Relations Act No 66 of 1995;
- Medical Schemes Act No 131 of 1998;
- National Credit Act No 34 of 2005;
- Occupational Health and Safety Act No 85 of 1993;
- Pension Funds Act No 24 of 1956;
- Protection of Personal Information Act No 4 of 2013;
- Regulation of Interception of Communications and Provision of Communication-Related Information Act No 70 of 2002;
- Skills Development Act No 97 of 1998;
- Skills Development Levies Act No 9 of 1999;
- Unemployment Insurance Act No 63 of 2001;
- B-BBEE Act No 53 of 2003; and
- Value Added Tax Act No 89 of 1991.

4.2.2 Where any information contained in any records retained by the company in terms of the above legislation is of a public nature, such records may be available for inspection without a person having to request access thereto in terms of PAIA.

4.3 Records held by the company (section 51(1)(e) of PAIA)

The records held by the company include but are not necessarily limited to:

Subjects on which the company holds records	**Categories of records held on each subject**
Service Records	Client Correspondence and Job Cards.
Corporate Governance	Codes of Conduct, Policies, Compliance Records.
Finance & Administration	Financial statements and reports, Purchase orders, Remittances, Tax records, Invoices.
Human Capital/Resources	Employee personal information, UIF returns, PAYE, Retirement and Provident Fund information, Medical Aid Records, Offer Letters, Code of Conducts, Leave records and Policies, Training records, Shareholder agreements, meeting minutes.

Marketing	Marketing and brand information, adverts and designs, photographs, data base, brochures and publications.
Operations	General correspondence, Quotes, Invoices, Purchase Orders, Receipts, Order Books, Vehicle registration documents, Trade Terms and Conditions, Contracts.

5. Process for requests to Information

5.1 Any requests for access to records of the company are subject to PAIA and, in respect of personal information, POPI.

5.2 In terms of PAIA, a request for access is to be made on the prescribed form accessible at https://www.justice.gov.za/forms/paia/J752_paia_Form%20C.pdf. The request is to be made to the Information Officer addressed to the contact details set out above (section 53(1) of PAIA).

5.3 The requester must provide sufficient detail on the form to enable the Information Officer to identify the record and the requester. The requester should also indicate which form of access is required and specify a postal address, fax number in the Republic of South Africa or email address. The requester should also indicate if, in addition to a written reply, any other manner is to be used to inform the requester and state the necessary particulars to be so informed (section 53(2)(a) and (b) and (c) and (e) of PAIA).

5.4 The requester must identify the right that is sought to be exercised or protected and provide an explanation of why the requested record is required for the exercise or protection of that right (section 53(2)(d) of PAIA).

5.5 In circumstances where the request for access is being made on behalf of another person, the requestor is obliged to prove the capacity in which the request is being made, with any submissions in support thereof being subject to the satisfaction of the company (section 53(2)(f) of PAIA). Section 71 of PAIA makes provision for a request for information or records about a third party. In considering such a request, the company will adhere to the provisions of sections 71 to 74 of PAIA. The requestor is to note the provisions of Chapter 5 of Part 3 of PAIA in terms of which the company is obliged, in certain circumstances, to advise third parties of requests lodged in respect of information applicable to or concerning such third parties. In addition, the provisions of Chapter 2 of Part 4 of PAIA entitle third parties to dispute the decisions of the company by referring the matter to the High Court.

5.6 The Information Officer will decide on whether or not to grant the request as soon as is reasonably possible (but in any event within thirty days of the request having been submitted) and notify the requester accordingly.

5.7 The Information Officer may decide to extend the period of thirty days for another period of not more than thirty days if:

5.7.1 the request is for a large number of records;

5.7.2 the search for the records is to be conducted at premises not situated in the same town or city as the head office of the company;

5.7.3 consultation among divisions or departments; as the case may be, of the company is required;

5.7.4 the requester consents to such an extension in writing; or

5.7.5 the parties agree in any other manner to such an extension.

5.8 Should the company require an extension of time, the requester shall be informed in the manner stipulated in the prescribed form of the reasons for the extension.

5.9 If the Information Officer fails to respond (or extend the period within which the respond) within thirty days after a request has been received, it will, in terms of PAIA, be deemed to have refused the request (section 58 read together with section 56(1) of PAIA).

5.10 Where access is granted:

5.10.1 the Information Officer will advise the requester of:

a) the access fee to be paid for the information (in accordance with paragraph 6 of this Manual below) prior to CMS South Africa being able to process the request and grant the access (section 54(1) of PAIA);
b) the format in which access will be given;
c) the fact that the requester may lodge an appeal with a court of competent jurisdiction against the access fee charged or the format in which access is to be granted (section 56(2) of PAIA); and

5.10.2 access to the record requested will be given as soon as reasonably possible.

5.11 The following access and reproduction fees apply:

5.11.1 the request fee payable by a requester, other than a personal requester (being a requester who seeks access to a record containing personal

information about that requester) is R50,00. The requester may lodge an application to the court against the tender or payment of the request fee (section 54(3)(b) of PAIA); and

5.11.2 where the Information Officer is of the opinion that the number of hours required to search, reproduce and/or prepare the information requested will exceed 6 hours, it may require that a deposit be paid, calculated in accordance with PAIA.

5.11.3 Access and Reproduction fees respectively:

For every photocopy of an A4 size page or part thereof	R1,10
For every printed copy of an A4 size page or part thereof	R0,75
For a copy of a compact disc	R70,00
For a transcript of visual images for an A4 size page or part thereof	R40,00
For a copy of visual images	R60,00
For a transcript of an audio record, for an A4 size page or part thereof	R20,00
For a copy of an audio record	R30,00

5.12 If the request for access is refused, the Information Officer shall advise the requester in writing of the refusal, including adequate reasons for the refusal and that the requester may lodge an appeal with a court of competent jurisdiction against the refusal of the request (section 56(3) of PAIA).

5.13 Upon the refusal by the Information Officer, any deposit paid by the requester will be refunded.

5.14 The requester may lodge an appeal with a court of competent jurisdiction against any process set out in this paragraph 5.

6. Records not found

6.1 If a record cannot be found or if the records do not exist, the Information Officer shall notify the requester (providing full details of steps taken to find the record or determine its existence) that it is not possible to give access to the requested record.

6.2 If the record in question should later be found, the requester shall be given access to the record unless access is refused by the company.

7. Refusal of access

7.1 The company may refuse to grant access on certain grounds, including the following (Part 3, Chapter 4 of the PAIA):

7.1.1 that the record constitutes privileged information for the purposes of legal proceedings or is subject to professional privilege;

7.1.2 to protect the commercial information or the confidential information of a third party or the company;

7.1.3 that it is necessary to protect the safety of individuals or property;

7.1.4 that it is necessary to protect the research information of a third party or the company; or

7.1.5 that granting access would result in the unreasonable disclosure of personal information about a third party.

8. Plan of action when information is leaked

All employees have undergone training and have signed a contractual agreement of their adherence to the POPI Act and regulations the company needs to adhere to as a Business.

The employees have also undergone training and are fully aware of the processes in place in relation to the POPI Act.

The relevant software and firewall programs have also been put into place to protect the files and all systems.

Should a client advise that they feel that the company has leaked information or shared their information without their consent to others the following process will be followed:

- Any potential breach must be reported to the line manager and Information Officer

- Investigation
  - An investigation will first be done to determine what information was shared.
  - Where the information could've leaked or been shared from or where it could've been accessed from.
- Reporting
  - The details of the investigation will then be reported and logged with the Deputy Officer, Information Officer and Senior Management team of the business.
- Rectify
  - The necessary steps will then be taken to determine how the share of information can be avoided with reference to how the leak occurred.
  - The persons affected will be provided with the feedback from the investigation.
  - The relevant action to repair the relationship with said affected person will be done.

9. Updating of the manual

The company will, if necessary, update and publish this Manual annually.

DATED AND SIGNED AT CLAREMONT ON THIS 28TH DAY OF JUNE 2024.

RENé BLOM

INFORMATION OFFICER