

PROTECTION OF PERSONAL INFORMATION (POPIA) POLICY RELATING TO SECURITY AND ACCESS CONTROL

Effective date: 2026/08/12

Version: 0.0

Responsible party: Val de Vie and Paarl Valley Homeowners Associations

Place of business: Val de Vie / Paarl Valley Estates, Paarl, South Africa

1 INTRODUCTION AND PURPOSE

Val de Vie and Pearl Valley ("the Estates") are committed to protecting the privacy of all data subjects (residents, owners, tenants, visitors, contractors, employees, and other persons) while maintaining a safe and secure living environment.

This Policy explains how the Estates collect, use, store, and protect Personal Information in compliance with the **Protection of Personal Information Act 4 of 2013 (POPIA)**, the Constitution of South Africa, and the RCC/NAMA Code of Conduct for Residential Communities. It balances legitimate security needs with privacy rights and addresses concerns about surveillance and monitoring.

The Estates process Personal Information lawfully, minimally, and transparently for security, access control, rule enforcement, and estate administration. Surveillance (e.g., CCTV) is used solely for crime prevention, safety, and protection of common property and not for monitoring of activities outside of the scope as defined in this policy.

This policy must be read together with the Constitution and Estate Code of Conduct of the relevant estates.

2 DEFINITIONS

- **Personal Information (PI):** Any information relating to an identifiable person (e.g., name, ID number, contact details, vehicle registration, biometric data, images/video from CCTV).
- **Special Personal Information (SPI):** Includes biometric data, health information, etc. (processed only with consent or as permitted by law).
- **Management/Processing:** Any operation on Personal Information (collection, storage, use, sharing, deletion).
- **Data subject:** Any natural person entering, occupying, or leaving the Estates whose Personal Information is processed.
- **Responsible party:** The Estate (HOA/Body Corporate) responsible for the management of personal information.
- **Operator:** Third parties (e.g., security company, managing agent) who process information on our behalf.

3 PERSONAL INFORMATION

As a rule, the Estates collect only PI that is adequate, relevant, and not excessive (POPIA Condition 2 – Minimality).

Main categories and purposes are shown below:

Category	Examples	Purpose	Lawful Basis
Resident / Owner / Tenant	Name, ID, contact details, property address, banking info (for levies)	Estate administration, communication, rule collection, rule enforcement	Contract (estate rules/constitution), legitimate interest
Visitors / Contractors	Name, ID/passport, vehicle reg, contact details, purpose of visit	Access control and security	Consent (at gate) or legitimate interest (safety)
Surveillance & Monitoring	CCTV footage, license plate recognition (LPR), access logs, biometric data (if used)	Crime prevention, safety, rule enforcement, incident investigation, CCTV does NOT monitor private homes/gardens.	Legitimate interest (security of residents and common property) – no consent required but full transparency provided
Employees / Staff	Employment details, ID, biometrics (where applicable)	HR and security	Contract and legal obligation
Other	Correspondence, complaints	Dispute resolution	Legitimate interest

Surveillance-specific rules:

- Cameras are positioned only on common property and entrances to ensure strategic coverage of identified high-risk areas and access points.
- Footage is live-monitored only by authorised security personnel and duly authorised estate management.
- Audio is collected only at strategic access points, specifically at a registration point for risk management purposes. Consent is specifically managed in compliance with RICA legislation.
- Relevant signage is clearly displayed at all main gates to inform residents, visitors, and contractors.
- Private areas (e.g., inside homes, gardens, bathrooms) are never monitored and are privacy-masked.

Biometric-specific rules:

- Biometric access control devices are positioned at controlled access points such as main gates and identified access-controlled facilities.

- Biometric data is used solely for the purpose of access control and is accessible only by duly authorised security personnel under controlled conditions.

4 LAWFUL PROCESSING

The Estates comply with all eight conditions of POPIA as outlined below.

1. **Accountability:** Estates ensure compliance with the act, and have appointed an Information Officer.
2. **Processing Limitation:** Estates act to be lawful, reasonable, and minimal, with consent obtained where required.
3. **Purpose Specification:** Information is only collected for specified, explicit purposes that are clearly specified.
4. **Further Processing Limitation:** Further use of information is only applicable when compatible with the original purpose, or when lawfully required.
5. **Information Quality:** All information is kept accurately and up to date, and no changes or alterations are made to original data.
6. **Openness:** Estates fully comply with transparency requirements, and all data subjects are notified via this Policy and relevant signage.
7. **Security Safeguards:** Estates ensure data security as part of the overall Estate security controls - see Section 7 for details.
8. **Data Subject Participation:** Data subjects are not forced or coerced in any way whatsoever - see Section 6 for details.

5 PROCESSING, CONSENT AND NOTIFICATION

- **Management:** Personal Information management (including processing) is undertaken for the administration, control, safety and security of the Estates.
- **Residents/owners:** Acknowledge, by being bound by the relevant Constitution and Estate Code of Conduct by virtue of their ownership/residence, that they are accordingly bound by this policy.
- **Visitors:** Explicit consent is obtained by means of gate registers or digital systems, as well as Privacy Notices.
- **Withdrawal:** Data subjects may withdraw consent, where it was specifically required, at any time (subject to legal/security obligations) with the understanding that withdrawal may affect access (e.g., visitor entry).

6 RIGHTS AS A DATA SUBJECT

Data subjects have the right to:

- Access information by following a duly defined PAIA request process.
- Correct or delete inaccurate/outdated information as per change process.
- Object to processing of data, specifically including direct marketing.
- Lodge a complaint with the Information Officer or the Information Regulator.
- Be notified of security breaches through a defined standard operating procedure.

Requests must be submitted in writing/email to the Information Officer (see contact below). The Estates shall respond within 30 days (or as per PAIA process timelines).

7 SECURITY SAFEGUARDS

The Estates implement reasonable technical and organisational measures (per Annexure A of the RCC Code and Cyber Essentials principles):

- All data, except CCTV footage, are subject to encryption, access controls (role-based), firewalls, and controls against cyber-attacks.
- The Personal Information management system is subjected to regular risk assessments and reviews.
- All Operator Agreements are documented and implemented with duly conducted training with security providers that meet POPIA standards.
- All Estate CCTV footage is stored securely on servers that are access controlled and cyber-secured.
- Live access to CCTV is limited to authorised personnel and duly authorised management only.
- CCTV, while mainly used for security and safety reasons, may be used by authorised personnel to investigate incidents affecting property protection and breach of estate rules.
- In compliance with POPIA, information is retained only for as long as reasonably necessary.
- Access to information is controlled with consideration of legal obligations, operational requirements, and pending investigations.
- Data is destroyed securely (shredding/deletion) once no longer needed.

Data type	Period
CCTV / surveillance footage (general)	30 days with rolling overwrite.
CCTV footage linked to an incident	Until investigation / claim / matter is closed.
Visitor / access-control logs (name, vehicle reg, entry/exit time, host, gate)	90 days, or up to 6 months if risk-justified.
Access-control system logs (biometric, card, LPR, turnstile events)	90 days, or up to 12 months for higher-risk sites.
Contractor access / registration data	Duration of the specific job/visit + 90 days.
Incident / occurrence / occurrence-book reports	5 years.
CCTV / system audit logs (who viewed or exported footage)	12 months.

8 SHARING OF PERSONAL INFORMATION

The Estates share only when necessary (e.g., with security Operator, SAPS for incidents, auditors, legal advisors). All third parties have POPIA-compliant agreements. No selling of data shall be allowed under any circumstances.

9 DATA BREACHES

We will notify the Information Regulator and affected data subjects as soon as reasonably possible if a breach occurs (per s22 POPIA).

10 INFORMATION OFFICER

Val de Vie

Name: Eugene Botha, Estate COO **Contact:** Eugene.Botha@vdyvhoa.co.za or 021-8636100. HOA offices, The Yard, Val de Vie estate, Paarl, 7646. Email all POPIA requests/complaints to: Eugene.Botha@vdyvhoa.co.za

Pearl Valley

Name: Greg van Heerden, Estate Manager **Contact:** Greg.vanHeerden@pvhoa.co.za or 021-0014419. HOA offices, 682 Appaloosa street, The Acres, Pearl Valley estate, Paarl, 7646. Email all POPIA requests/complaints to: Greg.vanHeerden@pvhoa.co.za

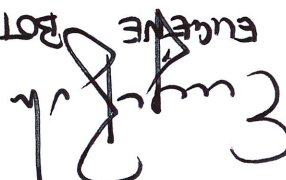
11 COMPLAINTS

First to the Information Officer following standard operating procedure. If unresolved, to the Information Regulator (info regulator.org.za).

12 REVIEW AND UPDATES

This Policy is reviewed annually or when law changes. Updates will be published and notified.


E. BOTHA

Greg van Heerden

EUGENE BOTHA

Greg van Heerden

M. Hudson
13 Aug. 2006