DEVICE REGISTER

Reg: 2026/247894/07 | deviceregister.co.za

POPIA Information Document

Protection of Personal Information Act 4 of 2013

Device Register (Pty) Ltd | Reg: 2026/247894/07 | March 2026 | Version 1.1 | Confidential

Purpose of This Document

This document is provided for the benefit of investors, auditors, regulatory bodies, and strategic partners seeking to understand how Device Register (Pty) Ltd processes personal information in compliance with the Protection of Personal Information Act 4 of 2013 (POPIA). It provides a transparent account of what information is collected, why it is collected, how it is protected, and what rights individuals and entities have in respect of their data.

1. Who We Are

Device Register (Pty) Ltd (Reg: 2026/247894/07) is a South African SaaS company operating a centralised device fraud prevention registry for the insurance industry. We are the Responsible Party in terms of POPIA. Our Information Officer can be contacted at **accounts@deviceregister.co.za**.

2. Our Core Privacy Principle

Core Principle

Device Register does NOT collect, record, store, or process any personal information belonging to the end clients or policyholders of registered Insurers beyond the minimum identifiers required for fraud prevention. We collect only the minimum necessary information from the Insurer entity itself for the purpose of operating the Platform.

3. What Information We Collect From Insurers and Why

From Registered Insurers:

Information Collected	Purpose	Legal Basis
First Name & Last Name	Account identification and correspondence	Contractual necessity
Company Name	Business identity verification	Contractual necessity
Company Registration No.	Verify legitimately registered entity in SA	Legitimate interest / legal compliance
Email Address	Login, invoices, notifications	Contractual necessity
Contact Number	Account support and verification	Contractual necessity
Province & Address	Geographic record for billing purposes	Contractual necessity
Payment Records	Subscription billing, financial records	Legal obligation

Session & Login Data	Security, fraud prevention, access control	Legitimate interest

From Device Records:

Device records contain technical and policy reference information. None of the standard device fields constitute personal information. Where Vehicle Claims are processed, additional fields are collected as described in Section 3A.

- Policy Number — reference identifier used internally by the Insurer
- Device Category and Type (e.g. Mobile Device, Laptop, Appliance)
- Device Brand and Model
- Serial Number — hardware identifier
- IMEI Number — network identifier for mobile devices
- MAC Address — network hardware identifier
- Device Status (registered, stolen, claimed, repaired)
- Date of Registration

3A. Vehicle Claims — Why We Collect ID Numbers and Cell Numbers

When processing vehicle insurance claims, certain additional personal identifiers are collected from the Insurer on behalf of the policyholder. This section explains what is collected, why it is necessary, and how it is technically protected.

Fields Collected for Vehicle Claims:

- Insured ID Number — required to uniquely identify the policyholder for fraud prevention and claim validation
- Insured Cell Number — required for claim communication, regulatory compliance, and fraud detection
- Insured Email Address — required for claim correspondence
- Driver ID Number — required to validate the authorised driver for the claim
- Vehicle Registration Number — required to identify the insured vehicle

Why These Fields Are Necessary:

South African insurance claims regulations and SAPS stolen vehicle reporting require identification of the policyholder and driver. Without ID numbers, fraudulent claims involving multiple identities cannot be detected. Without cell numbers, claim notifications required by the Short-Term Insurance Act cannot be sent.

How We Protect This Data — Client-Side Encryption Before Transmission

ID numbers, cell numbers, email addresses, and vehicle registration numbers **NEVER reach the server in plain text**. Encryption is performed entirely in the browser before data is transmitted. By the time any data leaves the user's device, it is already **AES-256-CBC encrypted**. The server receives and stores only encrypted ciphertext — the server itself never sees the original value. Keys are derived from installation-specific WordPress security salts and are never stored alongside the data. Even if the database were accessed without authorisation, all sensitive fields would be unreadable ciphertext.

Technical Encryption Process:

- Step 1: User enters ID number or cell number into the form on their device.
- Step 2: JavaScript encrypts the value using AES-256-CBC before form submission.
- Step 3: The encrypted ciphertext (not the plain text) is transmitted to the server.
- Step 4: The server stores only the encrypted ciphertext in the database.

- Step 5: When an authorised user views the record, the ciphertext is decrypted for display.
- Step 6: The plain text value is never logged, cached, or stored anywhere on the server.

NOTE: Even in the event of a database breach, ID numbers, cell numbers, and vehicle registrations would be unreadable ciphertext. Encryption keys are derived from installation-specific WordPress security salts and are never stored alongside the data.

4. What We Explicitly Do NOT Collect

Client / Policyholder names (other than on vehicle claims where provided by the Insurer)

Client banking or financial information of any kind

Client biometric data

Any information that would allow Device Register to identify the end consumer from device records alone

Sensitive personal information as defined in Section 26 of POPIA beyond what is necessary for claims processing

5. How We Protect Information

- SSL/TLS Encryption: All data in transit is encrypted using HTTPS/TLS.
- AES-256-CBC Client-Side Encryption: ID numbers, cell numbers, email addresses and vehicle registrations are encrypted before transmission — see Section 3A.
- Password Hashing: All passwords stored using bcrypt — plain text passwords are never stored.
- 4-Digit PIN Authentication: Mobile app access uses a device-stored PIN never transmitted to the server.
- Session Management: Web sessions expire after 30 minutes of inactivity.
- Mobile App Tokens: App authentication tokens expire after 30 days, stored as one-way SHA-256 hashes.
- SQL Injection Protection: All database queries use parameterised prepared statements.
- Audit Logging: Every data change is logged with timestamp and user reference.
- Access Control: Each Insurer can only access their own device records.

6. Data Retention

Device records are retained permanently, even after subscription expiry — a deliberate decision in the public interest of fraud prevention. Vehicle claim records are retained permanently as required by the Short-Term Insurance Act. Insurer account data is retained for a minimum of 5 years following account cancellation.

7. Data Subject Rights

Right to access personal information held about them

Right to request correction of inaccurate information

Right to request deletion of information (subject to legal retention obligations)

Right to object to processing in certain circumstances

Right to lodge a complaint with the Information Regulator of South Africa

To exercise any of these rights, contact: **accounts@deviceregister.co.za**

8. Information Regulator Contact Details

The Information Regulator (South Africa)

Website: **www.inforegulator.org.za** | Email: **inforeg@justice.gov.za**

JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001

NOTE: This document is issued by Device Register (Pty) Ltd in accordance with POPIA Section 18 notification requirements. Version 1.1 — March 2026. Updated to reflect vehicle claims data processing and client-side AES-256 encryption implementation.