POPIA INFORMATION DOCUMENT

Protection of Personal Information Act 4 of 2013

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

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 clear and 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 for all personal information we hold. Our appointed Information Officer can be contacted at accounts@deviceregister.co.za.

2. OUR CORE PRIVACY PRINCIPLE

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

Where a Subscriber optionally submits a client identity number for the purpose of cross-insurer fraud matching, this number is immediately and irreversibly converted to a one-way SHA-256 cryptographic hash before any data leaves the entry point. The original identity number is never transmitted to, stored on, or accessible by Device Register servers under any circumstances. See Section 6 below for the full technical explanation.

3. WHAT INFORMATION WE COLLECT FROM INSURERS AND WHY

From Registered Insurers (the Platform's direct customers):

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 and trading entity in SA	Legitimate interest / legal compliance

Email Address	Login, 2FA, 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, invoices, financial records	Legal obligation
Session & Login Data	Security, fraud prevention, access control	Legitimate interest

From Device Records registered on the Platform:

Device records contain only technical and policy reference information. None of this constitutes personal information about any individual:

- Policy Number, a reference identifier used internally by the Insurer
- Device Category and Type (e.g. Mobile Device, Laptop, Appliance)
- Device Brand and Model
- Serial Number, a hardware identifier unique to the physical device
- IMEI Number, a network identifier for mobile devices
- MAC Address, a network hardware identifier
- Device Status (registered, stolen, claimed, repaired)
- Date of Registration
- Client ID Hash (optional), a one-way SHA-256 cryptographic fingerprint. The original identity number is never stored. See Section 6.

4. WHAT WE EXPLICITLY DO NOT COLLECT

Device Register does not store identity numbers. All identity-based matching uses irreversible SHA-256 hashes only. The actual ID number cannot be recovered by anyone.

- **Client / Policyholder identity numbers in any readable, decryptable, or reversible form**
- Client contact information (phone numbers, email addresses, physical addresses)
- Client banking or financial information of any kind
- Client biometric data
- Any information that would allow Device Register to identify the end consumer behind a policy
- Sensitive personal information as defined in Section 26 of POPIA

5. HOW WE PROTECT INFORMATION

- SSL Encryption: All data in transit is encrypted using industry-standard HTTPS/TLS.
- Password Hashing: All passwords stored using bcrypt, plain text passwords are never stored.
- Identity Hashing: All client identity numbers converted to irreversible SHA-256 hashes, original numbers are never stored.
- Two-Factor Authentication: Every login requires a one-time PIN sent to the registered email address.
- Session Management: Sessions automatically expire after a period of inactivity.
- Login Lockout: Accounts are locked after 3 failed login attempts for 15 minutes.
- 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, cross-insurer data is not visible except through controlled fraud flag notifications.

6. CLIENT IDENTITY HASHING — FULL TECHNICAL EXPLANATION

What is SHA-256 Hashing?

SHA-256 (Secure Hash Algorithm 256-bit) is a one-way cryptographic function used universally by banks, governments, and technology companies. It converts any input (such as an identity number) into a fixed-length 64-character string of letters and numbers called a hash. The same identity number will always produce exactly the same hash, but it is mathematically impossible to reverse the process to recover the original identity number from the hash.

How Device Register Uses SHA-256

When a Subscriber optionally enters a client identity number on the Platform, the following occurs:

- Step 1: The identity number is converted to its SHA-256 hash immediately at the point of entry.
- Step 2: Only the hash is transmitted to Device Register's servers.
- Step 3: Only the hash is stored in the Device Register database.
- Step 4: When another Subscriber enters the same identity number, their hash is compared against stored hashes. A match indicates the same individual, without either insurer or Device Register ever seeing the actual identity number.
- Step 5: The original identity number is permanently gone. It is not stored anywhere. It cannot be recovered.

Device Register therefore does not "process" identity numbers as defined under POPIA, because the original identity number never reaches or is stored on Device Register infrastructure. The SHA-256 hash is not personal information because it cannot be linked back to any individual without the original identity number.

7. CLIENT BLACKLIST REGISTRY

The Platform provides an industry-wide Client Blacklist Registry that enables Subscribers to flag clients who have submitted fraudulent insurance claims. This serves the public interest of fraud prevention and operates as follows:

- Entries are submitted voluntarily by Subscribers based on their own reasonable belief of fraudulent conduct.
- Entries visible to all active Subscribers contain client name, policy number, device serial number, reason for flagging, and the submitting insurer's company name.
- Entries do not contain identity numbers in any readable form.
- Where an ID hash accompanies a blacklist entry, only the hash is stored, the identity number is never retained.
- The lawful basis for processing blacklist data is legitimate interest in fraud prevention, which is explicitly recognised under POPIA.
- All Subscribers consent to participation in the Blacklist Registry as a condition of Platform use, confirmed in the POPIA Consent and Acknowledgement Form.
- The Company reserves the right to remove any blacklist entry that is found to be false, malicious, or unsubstantiated.

8. DATA RETENTION

Device records are retained permanently, even after an Insurer's subscription expires. This is a deliberate design decision in the public interest of fraud prevention, a device that was registered as stolen should remain traceable indefinitely. Insurer account data is retained for as long as legally required for financial and compliance purposes.

9. 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

10. 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

This document is issued by Device Register (Pty) Ltd in accordance with POPIA Section 18 notification requirements.