TERMS AND CONDITIONS OF SERVICE

Device Register (Pty) Ltd

Legal Entity:	Device Register (Pty) Ltd
Website:	deviceregister.co.za
Email:	info@deviceregister.co.za
Effective Date:	23 March 2026
Version:	1.1
Jurisdiction:	Republic of South Africa

These Terms and Conditions govern access to and use of the Device Register platform. By registering an account, making a payment, or accessing any feature of the platform, you acknowledge that you have read, understood, and agree to be bound by these Terms.

TABLE OF CONTENTS

1. DEFINITIONS AND INTERPRETATION

In these Terms and Conditions, unless the context requires otherwise, the following definitions shall apply:

- "Platform" means the Device Register web-based software-as-a-service application accessible at deviceregister.co.za, including all features, tools, dashboards, APIs, and related services.
- "Company" means Device Register (Pty) Ltd, the owner and operator of the Platform.
- "User" or "Subscriber" means any approved insurance company, broker, intermediary, corporate entity, or individual who has registered an account on the Platform.
- "Branch User" means a secondary user account created under a primary Subscriber account on the Small Branch or Corporate Entity plan.
- "Device" means any electronic, electrical, or mechanical item registered on the Platform by a Subscriber.
- "Registry" means the centralised database of all device records stored on the Platform.
- "Subscription" means the recurring access plan purchased by a Subscriber, as detailed in Clause 6.
- "POPIA" means the Protection of Personal Information Act 4 of 2013 (South Africa).
- "PayFast" means the third-party payment gateway used to process subscription payments.
- "Content" means all data, information, records, serial numbers, IMEIs, MAC addresses, client details, and other material uploaded or entered by Subscribers.
- "ID Hash" means a one-way SHA-256 cryptographic fingerprint derived from a client identity number. The original identity number cannot be recovered from the ID Hash under any circumstances.
- "Client Blacklist Registry" means the industry-wide database of clients flagged for fraudulent claim activity by registered Subscribers, accessible to all active Subscribers on the Platform.

References to the singular include the plural and vice versa. Headings are for convenience only and do not affect interpretation.

2. ACCEPTANCE OF TERMS

By completing the registration process, making payment, or accessing any part of the Platform, the User unconditionally accepts these Terms and Conditions in full. If you do not agree to these Terms, you must not register an account, make payment, or use the Platform in any manner. These Terms constitute the entire agreement between the Company and the User regarding the use of the Platform and supersede all prior agreements, representations, or understandings. The Company reserves the right to amend these Terms at any time. Continued use of the Platform following notification of amendments constitutes acceptance of the revised Terms. Users will be notified of material changes via email.

> *NOTE: These Terms are governed by and construed in accordance with the laws of the Republic of South Africa.*

3. PLATFORM ACCESS AND ACCOUNT REGISTRATION

3.1 Eligibility

Access to the Platform is restricted exclusively to approved South African insurance companies, registered brokers, intermediaries, corporate entities, and individuals operating within the South African insurance industry. The Company reserves the right to approve or reject any application at its sole discretion.

3.2 Account Registration

To access the Platform, Users must complete the registration process and provide accurate, complete, and current information. Users are responsible for maintaining the accuracy of their account information at all times.

3.3 Account Security

Users are responsible for maintaining the confidentiality of their login credentials. Each account is for the exclusive use of the registered entity and may not be shared with unauthorised third parties. Users must notify the Company immediately upon becoming aware of any unauthorised access.

3.4 Two-Factor Authentication

The Platform requires two-factor authentication (2FA) via one-time password (OTP) for every login session. Users must maintain access to their registered email address to complete authentication.

3.5 Session Management

Sessions automatically expire after a period of inactivity. The Platform enforces single-session access — concurrent logins from multiple devices are not permitted.

4. ACCEPTABLE USE POLICY

4.1 Permitted Use

The Platform may only be used for its intended purpose — the lawful registration, tracking, and management of insured devices within the South African insurance industry.

4.2 Prohibited Conduct

Users must not, under any circumstances:

- Register devices that do not belong to their client portfolio or that they are not authorised to register.
- Submit false, misleading, inaccurate, or fraudulent device information.
- Attempt to circumvent, disable, or interfere with any security features of the Platform.
- Use automated tools, bots, scrapers, or scripts to access or extract data from the Platform without prior written consent.
- Share login credentials with unauthorised individuals or organisations.
- Use the Platform for any unlawful purpose or in violation of any applicable laws or regulations.
- Attempt to reverse-engineer, decompile, or disassemble any part of the Platform.
- Upload or transmit any malicious code, viruses, or harmful data.
- Impersonate any person, entity, or organisation.
- Submit false, malicious, or unsubstantiated blacklist entries against clients or policyholders.

4.3 Consequences of Breach

Any breach of this Acceptable Use Policy may result in immediate suspension or termination of the User's account without notice or refund. The Company reserves the right to report criminal conduct to the relevant authorities.

5. DEVICE REGISTRATION AND DATA ACCURACY

5.1 User Responsibility

Users bear sole responsibility for the accuracy, completeness, and lawfulness of all device data submitted to the Platform. The Company does not independently verify the accuracy of device records entered by Users.

5.2 Data Standards

All device registrations must include valid serial numbers. Where applicable, IMEI numbers and MAC addresses must be accurate and correspond to the device being registered. Policy numbers must be current and verifiable.

5.3 Duplicate Detection

The Platform automatically cross-references all new registrations against existing records to detect duplicate serial numbers and IMEI numbers across all Subscribers. Where duplicates are detected, fraud flags are raised and the relevant parties are notified.

5.4 Live Pre-Registration Check

The Platform performs a real-time check against the national registry and Client Blacklist Registry before a device registration is submitted. Where a potential match is identified, the Subscriber is notified and must consciously acknowledge the warning before proceeding.

5.5 Permanence of Records

Once a device is registered on the Platform, its record is retained permanently in the Registry even if the Subscriber's account is cancelled or suspended. This is a deliberate design principle to preserve the integrity of the national device registry and support fraud prevention across the industry.

5.6 Audit Trail

All changes to device records are logged with a timestamp, the identity of the User making the change, the previous value, and the new value. This audit trail is tamper-evident and may be used in dispute resolution or legal proceedings.

5.7 Stolen Device Reporting

Users must promptly update device status to "Reported Stolen" upon receiving a theft claim. Failure to do so may result in fraudulent re-registration of the device by another party. The Company accepts no liability for losses arising from failure to update device status.

> *NOTE: The accuracy and completeness of device records is the sole responsibility of the Subscriber. The Company provides the infrastructure but does not warrant the accuracy of user-submitted data.*

6. SUBSCRIPTION AND PAYMENT TERMS

6.1 Subscription Plans

Access to the Platform is provided on a subscription basis. The following plans are currently available:

- Individual Branch: pricing as published on the Device Register platform at time of subscription (1 user login).
- Small Branch: pricing as published on the Device Register platform at time of subscription (up to 5 user logins).
- Corporate Entity: pricing as published on the Device Register platform at time of subscription (up to 10 user logins).

Pricing is subject to change. Subscribers will be notified of price changes at least 30 days in advance.

6.2 Payment Processing

All payments are processed securely via PayFast. The Company does not store payment card details. PayFast's terms and conditions apply to all payment transactions.

6.3 Subscription Activation

Subscriptions are activated automatically upon confirmed payment via PayFast's Instant Transaction Notification (ITN) system. Access is granted immediately upon activation.

6.4 Recurring Billing

Subscriptions are not automatically renewed. Users are responsible for renewing their subscription before the expiry date. Renewal reminders are sent at 7 days and 3 days before expiry.

6.5 Subscription Expiry

Upon expiry of a subscription, the User's access to the Platform will be restricted. Existing device records remain in the Registry. The User may renew their subscription at any time to restore full access.

6.6 Branch User Billing

Branch users registered under a Small Branch or Corporate Entity plan do not pay separately. Their access is included in the primary Subscriber's plan and is tied to the primary account's subscription status.

6.7 Annual Plans

Annual plans are billed upfront for the full year at a discounted rate. Annual subscriptions are not eligible for pro-rata refunds.

> *NOTE: All prices are quoted in South African Rand (ZAR) and are inclusive of VAT where applicable.*

7. CANCELLATION AND REFUND POLICY

7.1 Cancellation by Subscriber

Subscribers may cancel their account at any time via the "Cancel Account" function in their Profile & Billing page, or by contacting accounts@deviceregister.co.za. Cancellation takes effect immediately upon confirmation.

7.2 Effect of Cancellation

Upon cancellation, the Subscriber's access to the Platform is revoked immediately. All device records registered by the Subscriber remain permanently in the Registry and are not deleted.

7.3 Refund Policy

The Company operates a strict no-refund policy on all subscription payments. Partial refunds for unused subscription periods will not be issued under any circumstances.

7.4 Exceptions

In exceptional circumstances, at the sole discretion of the Company, a credit or partial refund may be considered. Such requests must be submitted in writing to accounts@deviceregister.co.za within 7 days of the relevant payment date.

7.5 Cancellation by the Company

The Company reserves the right to cancel any account for breach of these Terms, non-payment, fraudulent activity, or any other reason deemed appropriate, without prior notice and without liability to refund any amounts paid.

7.6 Branch User Cancellation

The primary Subscriber may cancel Branch User accounts at any time. Upon cancellation, all devices registered under that Branch User are reassigned to the primary Subscriber's account.

> *NOTE: Cancellation requests must be submitted via the Platform or in writing to accounts@deviceregister.co.za. Verbal cancellations will not be accepted.*

8. FRAUD DETECTION AND REPORTING OBLIGATIONS

8.1 Platform Fraud Detection

The Platform incorporates automated fraud detection mechanisms including cross-insurer duplicate serial number and IMEI checking, stolen device flagging, fraud scoring, real-time alert notifications, live pre-registration checks, and the Client Blacklist Registry. These mechanisms are provided as a tool to assist Subscribers and do not constitute a guarantee that all fraud will be detected.

8.2 Subscriber Reporting Obligations

Subscribers have a responsibility to:

- Promptly report stolen or recovered devices by updating the device status on the Platform.
- Investigate and respond to fraud flags raised by the Platform.
- Report confirmed fraud incidents to the South African Police Service (SAPS) and relevant regulatory authorities.
- Notify the Company of any suspected system abuse or fraudulent registrations by other parties.
- Only submit blacklist entries where there is a genuine and reasonable basis for believing fraudulent claim activity has occurred.

8.3 False Reporting

The submission of false, misleading, or malicious fraud reports or blacklist entries is strictly prohibited. Users found to have submitted false fraud reports or blacklist entries may have their accounts suspended and may face legal action.

8.4 Limitation

The fraud detection features are provided on a best-efforts basis. The Company does not warrant that all fraudulent activity will be detected and accepts no liability for undetected fraud.

> *NOTE: Fraud detection is a shared responsibility. The effectiveness of fraud prevention is enhanced when all Subscribers maintain accurate and up-to-date device records.*

9. DATA PRIVACY AND POPIA COMPLIANCE

9.1 Commitment to Privacy

Device Register (Pty) Ltd is committed to protecting personal information in accordance with the Protection of Personal Information Act 4 of 2013 (POPIA) and all applicable South African data protection legislation.

9.2 Personal Information Collected

The Company collects and processes: Subscriber information (name, company, email, contact number, address); device technical identifiers (serial numbers, IMEI numbers, MAC addresses); policy reference numbers; transaction information; and system information (login activity, audit logs). Where a Subscriber optionally provides a client identity number for fraud matching purposes, this is immediately converted to a one-way cryptographic hash (SHA-256) at the point of entry. The original identity number is never transmitted to, stored on, or accessible by Device Register servers in any form. See Clause 10 for full details.

9.3 What Device Register Does NOT Store

Device Register explicitly does not collect, store, retain, or have access to:

- Client or policyholder identity numbers (ID numbers) in any readable, decryptable, or reversible form.
- Client or policyholder contact details of any kind.
- Client financial or banking information.
- Any biometric data.
- Any sensitive personal information as defined in Section 26 of POPIA.

IMPORTANT: Device Register does not hold identity numbers. All identity-based fraud matching uses irreversible cryptographic hashes only. The actual ID number cannot be recovered, read, or accessed by Device Register or any third party under any circumstances.

9.4 Purpose of Processing

Personal information is collected and processed exclusively for: providing Platform access; processing payments; operating the registry and fraud detection services; communicating with Subscribers; and complying with legal obligations.

9.5 Data Sharing

The Company does not sell, trade, or transfer personal information to third parties, except as required for Platform operation (e.g., PayFast) or as required by law. Cross-insurer fraud flag visibility is limited to technical device identifiers and does not include personal information.

9.6 Data Retention

Device records and associated data are retained permanently to support the integrity of the national device registry. Subscriber account information is retained for a minimum of 5 years following account cancellation.

9.7 Data Security

The Company implements SSL encryption, bcrypt password hashing, SHA-256 one-way identity hashing, two-factor authentication, session management, and comprehensive audit logging to protect personal information.

9.8 Data Subject Rights

Subscribers and their clients have the right to request access to, correction of, or deletion of personal information, subject to legal obligations. Requests must be submitted to info@deviceregister.co.za.

9.9 Information Officer

Enquiries regarding data privacy may be directed to info@deviceregister.co.za.

NOTE: By using the Platform, Subscribers warrant that they have obtained all necessary consents from their clients for the processing of personal information on the Platform, including the optional submission of identity number hashes for fraud prevention purposes.

10. CLIENT IDENTITY HASHING AND BLACKLIST REGISTRY

10.1 Identity Hashing — How It Works

Where a Subscriber optionally enters a client identity number during device registration, the following process occurs immediately and automatically:

- The identity number is converted to a SHA-256 cryptographic hash within the Subscriber's browser or the Platform's processing layer before any data is transmitted.
- Only the resulting hash — a fixed-length string of letters and numbers — is transmitted to and stored on Device Register's servers.
- The original identity number is never transmitted, stored, logged, or retained by Device Register in any form.
- SHA-256 is a one-way function — it is mathematically impossible to reverse the hash to recover the original identity number.
- The hash is used exclusively for cross-insurer fraud matching — comparing whether two separately entered identity numbers belong to the same individual, without either insurer or Device Register being able to read the actual identity number.

10.2 Identity Hashing — What This Means for POPIA

Because the original identity number is never stored, transmitted, or accessible in any form, Device Register does not "process" identity numbers as defined under POPIA. The SHA-256 hash does not constitute personal information as it cannot be linked back to an individual without the original identity number. Device Register is therefore not the Responsible Party under POPIA in respect of identity numbers entered by Subscribers.

10.3 Client Blacklist Registry

The Platform provides an industry-wide Client Blacklist Registry that allows Subscribers to flag clients who have submitted fraudulent insurance claims. The following rules apply:

- Blacklist entries are submitted voluntarily by Subscribers based on their own investigation and reasonable belief of fraudulent conduct.
- Entries are visible to all active Subscribers on the Platform to enable cross-insurer fraud prevention.
- Entries contain client name, policy number, device serial number, reason for flagging, and the submitting insurer's company name. They do not contain identity numbers in any form.
- Where an ID hash has been submitted alongside a blacklist entry, only the hash is stored — the identity number itself is never retained.
- The Company reserves the right to remove any blacklist entry that is found to be false, malicious, or unsubstantiated.
- Subscribers who submit false blacklist entries may have their accounts suspended and may face legal action.

10.4 Lawful Basis for Blacklist Processing

The processing of blacklist data is conducted on the lawful basis of legitimate interest in fraud prevention, which is explicitly recognised as a valid basis for data processing under POPIA. All Subscribers consent to participation in the Blacklist Registry as a condition of Platform use, as confirmed in the POPIA Consent and Acknowledgement Form.

> *NOTE: Participation in the Client Blacklist Registry is a shared responsibility. Subscribers must exercise good faith and reasonable diligence before submitting any blacklist entry.*

11. INTELLECTUAL PROPERTY

11.1 Ownership

The Platform, including all software, code, design, interface, content, trademarks, logos, and documentation, is the exclusive intellectual property of Device Register (Pty) Ltd. All rights are reserved.

11.2 Licence to Use

The Company grants Subscribers a limited, non-exclusive, non-transferable, revocable licence to access and use the Platform solely for the purposes described in these Terms during the active subscription period.

11.3 Restrictions

Subscribers may not copy, reproduce, distribute, reverse-engineer, decompile, sub-license, or create derivative works of the Platform or any part thereof.

11.4 User Content

Subscribers retain ownership of the device data they submit. By submitting data, Subscribers grant the Company a perpetual, irrevocable licence to store, process, and use such data for the operation of the Registry and fraud detection services.

12. LIMITATION OF LIABILITY

12.1 Platform Provided "As Is"

The Platform is provided on an "as is" and "as available" basis. The Company makes no warranties, express or implied, regarding the accuracy, reliability, completeness, or fitness for a particular purpose of the Platform or the Registry.

12.2 Exclusion of Liability

To the maximum extent permitted by applicable law, the Company shall not be liable for any indirect, incidental, special, consequential, or punitive damages; loss of profits or data; losses from reliance on inaccurate records; system downtime; unauthorised access; or undetected fraud.

12.3 Cap on Liability

In no event shall the Company's total liability to any Subscriber exceed the total subscription fees paid by that Subscriber in the 12 months preceding the event giving rise to the claim.

12.4 Force Majeure

The Company shall not be liable for any failure or delay caused by circumstances beyond its reasonable control, including acts of God, cyberattacks, internet outages, or government action.

> *NOTE: Nothing in these Terms limits rights that cannot be excluded by law, including certain consumer protections under the Consumer Protection Act 68 of 2008.*

13. INDEMNIFICATION

Subscribers agree to indemnify, defend, and hold harmless Device Register (Pty) Ltd, its directors, employees, agents, and service providers from and against any claims, damages, losses, liabilities, costs, and expenses (including legal fees) arising from:

- Any breach of these Terms by the Subscriber.
- The submission of inaccurate, false, or fraudulent device data.
- The submission of false or unsubstantiated blacklist entries.
- Violation of any applicable laws or regulations.
- Infringement of any third-party rights.
- Any claim by a third party arising from the Subscriber's use of the Platform.

14. TERMINATION

14.1 Termination by Subscriber

Subscribers may terminate their account at any time in accordance with Clause 7. Termination does not entitle the Subscriber to any refund.

14.2 Termination by the Company

The Company may terminate or suspend access immediately and without notice if a Subscriber breaches any provision of these Terms, engages in fraudulent or unlawful conduct, fails to make payment, or provides false registration information.

14.3 Effect of Termination

Upon termination, access ceases immediately. Device records remain in the Registry permanently. Clauses 5.5, 9, 10, 11, 12, 13, and 15 survive termination.

15. GOVERNING LAW AND DISPUTE RESOLUTION

15.1 Governing Law

These Terms shall be governed by and construed in accordance with the laws of the Republic of South Africa.

15.2 Jurisdiction

The parties consent to the non-exclusive jurisdiction of the South African courts in respect of any dispute arising from these Terms.

15.3 Dispute Resolution

In the event of a dispute, the parties agree to first attempt resolution through good-faith negotiation. If unresolved within 30 days, either party may refer the matter to mediation before initiating formal legal proceedings.

16. GENERAL PROVISIONS

16.1 Entire Agreement

These Terms, together with any other policies published on the Platform, constitute the entire agreement between the Company and the Subscriber.

16.2 Severability

If any provision is found invalid or unenforceable, the remaining provisions shall continue in full force and effect.

16.3 Waiver

Failure to enforce any right or provision shall not constitute a waiver of such right or provision.

16.4 Assignment

Subscribers may not assign rights or obligations without prior written consent. The Company may assign without restriction.

16.5 Notices

All legal notices to the Company must be sent to info@deviceregister.co.za. Notices to Subscribers will be sent to the registered email address on file.

16.6 Language

These Terms are written in English. In the event of any conflict arising from a translation, the English version shall prevail.

For and on behalf of:
Device Register (Pty) Ltd
deviceregister.co.za

Date of Issue: 23 March 2026 | Version: 1.1
info@deviceregister.co.za | accounts@deviceregister.co.za