INSURANCEVAULT

Privacy & Data Protection Statement

Effective Date: 1 August 2026 | Version 1.0

This Privacy and Data Protection Statement ("Statement") explains how InsuranceVault ("we", "us", "our") collects, processes, stores, and protects your personal information. It is designed to comply with the South African Protection of Personal Information Act 4 of 2013 ("POPIA"), the European Union General Data Protection Regulation 2016/679 ("GDPR"), and the EU Digital Operational Resilience Act 2022/2554 ("DORA") where applicable.

We are committed to handling your personal and asset information with the highest level of care, transparency, and security. Please read this Statement carefully. By creating an InsuranceVault account or using our services, you acknowledge that you have read and understood this Statement.

1. Who We Are

InsuranceVault is a secure, omnichannel asset management platform that enables individuals and businesses to digitise, track, and prove ownership of their inventory, and to link assets to compliance certificates and insurance policies.

Data Controller / Responsible Party
Company Name: InsuranceVault (Pty) Ltd [Registration number TBC]
Registered Address: [To be completed upon incorporation]
Information Officer (POPIA): [Name, email, telephone]
Data Protection Officer (GDPR): [Name, email, telephone]
Contact Email: privacy@insurancevault.co.za
Jurisdiction: Republic of South Africa (primary); EU/EEA (where services are offered to EU data subjects)

2. Scope of This Statement

This Statement applies to:

- All registered users of the InsuranceVault mobile application and any associated web portals;
- Insurance brokers and underwriters granted access to client shared views;
- Visitors to our website or marketing pages;
- Business entities (organisations) that use InsuranceVault under a commercial or enterprise agreement.

This Statement does not apply to third-party services linked to InsuranceVault (such as Google Drive, Microsoft OneDrive, or insurer Policy Administration Systems). Please review the privacy policies of those services independently.

3. Information We Collect

We collect only the information necessary to provide our services. The categories of personal information we process are:

3.1 Information You Provide Directly

- Identity data: full name, email address, password (hashed), profile type (personal or business);
- Organisation data: business name, registration number, role within the organisation;
- Asset data: make, model, serial number, purchase price, purchase date, asset category and status;
- Document data: uploaded invoices, warranties, certificates of compliance (CoCs), proof of payment, police affidavits, and insurance policy schedules;
- Insurance data: policy numbers, insurer name, coverage types, coverage limits, premium information;
- Broker data: broker name, FSP licence number, contact details;
- Claim data: incident date, incident type, SAPS Case Number (CAS), incident description, and supporting documentation;
- Security data: multi-factor authentication (MFA) enrolment status, authentication tokens.

3.2 Information Collected Automatically

- Device and usage data: device type, operating system version, app version, session timestamps, and feature usage events;
- Log data: error logs, crash reports, and API call metadata (no document content is included in logs);
- Camera and file access: only when you initiate a document capture or upload action; we do not access your camera or files at any other time.

3.3 Information from Third Parties

- Cloud storage providers (Google Drive, Microsoft OneDrive): when you link your own cloud account under our Bring Your Own Storage ("BYOS") model, we access only the specific folder you authorise. We do not access, read, or index any other files in your cloud account.
- Insurance brokers: brokers linked to your account may provide or verify policy schedule information through our API.

4. How We Use Your Information

Purpose of Processing	Legal Basis (POPIA / GDPR)
Creating and managing your account and organisation profile	Contractual necessity; POPIA s.11(1)(b)
Storing and organising your asset inventory and documents	Contractual necessity; POPIA s.11(1)(b)

Purpose of Processing	Legal Basis (POPIA / GDPR)
Linking assets to insurance policies and flagging coverage gaps	Contractual necessity; Legitimate interests
Generating insurance claim reports and PDF packages	Contractual necessity; POPIA s.11(1)(b)
Compliance certificate (CoC) expiry tracking and alerts	Contractual necessity; Legitimate interests
Providing brokers with your authorised shared view	Consent; POPIA s.11(1)(a)
Sending transactional notifications (CoC expiry, gap alerts)	Contractual necessity; Legitimate interests
Targeted advertising (opt-out data sharing stream only)	Consent; GDPR Art.6(1)(a); POPIA s.11(1)(a)
B2B enterprise API access and white-labelling	Contract; Legitimate interests
Security monitoring, fraud prevention, and incident response	Legal obligation; Legitimate interests; DORA
Improving platform features and user experience (anonymised analytics)	Legitimate interests; POPIA s.11(1)(f)
Complying with legal obligations (SAPS, court orders, regulators)	Legal obligation; POPIA s.11(1)(c)

5. Bring Your Own Storage (BYOS) and End-to-End Encryption

InsuranceVault is built on a privacy-first architecture:

- Your physical documents (PDFs, images) are stored in your own private cloud account (Google Drive or Microsoft OneDrive), not on our servers. We hold only a secure pointer (URI) to the file location, together with an encrypted decryption key reference.
- All asset metadata and file pointers are encrypted locally on your device using end-to-end encryption (E2EE) before being transmitted to our database.
- Decryption keys are stored in a dedicated secrets vault and are never exposed in application logs, error reports, or API responses.
- When you revoke cloud storage authorisation, we immediately invalidate our access tokens. We do not retain cached copies of your documents.

This BYOS model means that even in the event of a security incident affecting our infrastructure, your documents remain in your own cloud environment and are not directly exposed.

6. Broker “Shared View” Access

You may choose to grant your insurance broker read-only access to your verified asset inventory. The following conditions apply:

- Shared access is activated only by your explicit, informed consent via an in-app authorisation flow;
- Brokers receive a tokenised, time-limited access link. They cannot download, copy, or modify your underlying documents;
- You may revoke broker access at any time from the Profile screen within the app. Revocation takes effect immediately;
- Access is restricted to the inventory and compliance data you have linked to a specific policy. Brokers cannot see unlinked assets;
- All broker access events are logged with timestamps in your account activity log, visible to you at any time.

---

7. How We Share Your Information

We do not sell your personal information. We share your information only in the following limited circumstances:

7.1 With Your Consent

- Insurance brokers and underwriters, when you grant Shared View access (see Section 6);
- Enterprise API partners (insurers, property management systems), under a signed data processing agreement and only where you have consented or where required by your employer's enterprise subscription.

7.2 Service Providers (Data Processors)

We engage carefully selected sub-processors who process data strictly on our instructions:

- Cloud infrastructure provider (database and authentication hosting);
- Cloud storage providers (Google Drive, Microsoft OneDrive) — under your direct authorisation;
- PDF generation and document processing libraries (processed on-device or in a sandboxed environment);
- Crash reporting and anonymised analytics providers.

All sub-processors are bound by data processing agreements (DPAs) that meet POPIA and GDPR requirements.

7.3 Legal Obligations

- We may disclose information to law enforcement, the Information Regulator (South Africa), or other regulatory authorities where we are legally required to do so, or where necessary to prevent fraud, harm, or illegal activity;
- We will notify you of any such disclosure where legally permitted to do so.

7.4 Business Transfers

In the event of a merger, acquisition, or sale of all or substantially all of our assets, your information may be transferred. You will be notified in advance and given the opportunity to delete your account before the transfer takes effect.

---

8. International Data Transfers

InsuranceVault is headquartered in South Africa. Some of our service providers may be located in other countries, including within the European Economic Area (EEA) or in third countries.

- Transfers to EEA countries are subject to GDPR adequacy decisions or Standard Contractual Clauses (SCCs) as appropriate;

- South Africa has not yet received a GDPR adequacy decision; accordingly, any transfer of EU personal data to South Africa is governed by EU Standard Contractual Clauses;
- We conduct transfer impact assessments (TIAs) for all cross-border transfers and maintain a record of international data flows in our Register of Processing Activities.

9. Data Retention

We retain personal information only for as long as necessary to fulfil the purpose for which it was collected, or as required by law:

Data Category	Retention Period
Active account data (profile, assets, documents)	For the duration of your account, plus 30 days after deletion request
Archived assets (sold, replaced)	Until account deletion or explicit removal request
Claim records and police affidavits	7 years from claim closure (SARS / insurance regulatory requirements)
Compliance certificates (CoCs)	5 years from expiry date (regulatory requirement)
Broker access logs	3 years from last access event
Anonymised analytics	Up to 3 years (no personal identifiers retained)
Security and audit logs (DORA)	Minimum 1 year; up to 5 years for ICT incident records
Backup snapshots	30 days rolling; deleted on account closure

Where retention is required by law beyond the period you request deletion, we will restrict processing to the minimum necessary for compliance purposes only.

10. Your Rights

10.1 Rights Under POPIA (South African Users)

In terms of POPIA, you have the right to:

- Be notified that your personal information is being collected and processed;
- Access the personal information we hold about you (subject access request);
- Request correction or deletion of inaccurate, irrelevant, excessive, or unlawfully obtained personal information;
- Object to the processing of your personal information on reasonable grounds;
- Lodge a complaint with the Information Regulator of South Africa (see Section 14);
- Not be subject to a decision based solely on automated processing if it produces legal or similarly significant effects (we do not currently use such automated decision-making);
- Have your personal information deleted or destroyed when it is no longer needed for the purpose it was collected ("the right to be forgotten" under POPIA s.24).

10.2 Rights Under GDPR (EU / EEA Users)

If you are located in the European Economic Area, you have the following additional or equivalent rights under GDPR:

- Right of access (Art. 15): obtain a copy of all personal data we hold about you;
- Right to rectification (Art. 16): correct inaccurate personal data without undue delay;
- Right to erasure (Art. 17): request deletion of your personal data ("right to be forgotten");
- Right to restriction of processing (Art. 18): limit how we use your data in certain circumstances;
- Right to data portability (Art. 20): receive your personal data in a structured, machine-readable format (JSON export available in-app);
- Right to object (Art. 21): object to processing based on legitimate interests or for direct marketing purposes;
- Right to withdraw consent (Art. 7(3)): withdraw consent at any time without affecting prior lawful processing;
- Right to lodge a complaint with a supervisory authority (Art. 77): contact the data protection authority in your EU member state.

11. Account and Data Deletion

Built-In Data Deletion — Your Control, Always
InsuranceVault includes native in-app account and data deletion functionality.
Navigate to: Profile → Settings → Account → Delete Account & All Data
No email request required. No waiting period beyond confirmation.

When you initiate account deletion, the following actions are taken automatically:

- Immediate: your session tokens are revoked and all broker shared-access tokens are invalidated;
- Within 24 hours: all active asset records, document metadata, and policy links are permanently deleted from our primary database;
- Within 30 days: all backup snapshots containing your data are purged from our infrastructure;
- Cloud storage: your files in your BYOS cloud account (Google Drive / OneDrive) are not deleted by us — you retain full ownership and must manage deletion from within your cloud provider's interface;
- Legal retention exceptions: certain records (claim histories, CoC records) may be retained for the statutory minimum period in an isolated, restricted-access archive. You will be informed of any such retention at the time of your deletion request.

You may also request deletion of specific data items (individual assets, documents, or claims) without deleting your full account. Use the in-app deletion controls on the relevant item, or contact us at privacy@insurancevault.co.za.

To exercise your rights to access, portability, or erasure outside of the in-app controls, contact our Information Officer / DPO at the details in Section 14. We will respond within:

- South African users (POPIA): within a reasonable time, not exceeding 30 days;
- EU/EEA users (GDPR): without undue delay, and in any event within one (1) month (extendable by a further two months for complex requests, with notice).

12. Security Measures

We implement industry-standard and regulatory-grade technical and organisational security measures to protect your personal information:

12.1 Technical Measures

- End-to-end encryption (E2EE) of all asset metadata and document pointers in transit and at rest;
- AES-256 encryption for all stored data;
- TLS 1.3 for all data in transit;
- Multi-factor authentication (MFA) via TOTP (Time-based One-Time Passwords) — strongly recommended and available to all users;
- Zero-knowledge handshakes for tokenised broker access: decrypted content is never exposed to our API layer;
- Role-Based Access Control (RBAC) with principle of least privilege enforced at database level via Row Level Security (RLS);
- Secure, isolated secrets vault for encryption key management;
- Automated vulnerability scanning and dependency auditing in our software development pipeline.

12.2 Organisational Measures

- Privacy by design and by default is incorporated into all product development decisions;
- Access to production systems is restricted to authorised personnel on a need-to-know basis, with audit logging of all administrative actions;
- All staff and contractors with access to personal data are subject to confidentiality obligations and data protection training;
- We maintain a Data Processing Register and a Record of Processing Activities (ROPA) as required by GDPR Art. 30 and POPIA.

---

13. Digital Operational Resilience Act (DORA) Compliance

The EU Digital Operational Resilience Act (Regulation EU 2022/2554, "DORA"), in force from 17 January 2025, establishes binding requirements for the digital operational resilience of financial entities and their ICT third-party service providers operating in the EU. As InsuranceVault serves the insurance sector and may process data for EU-regulated financial entities, we have incorporated the following DORA-aligned practices:

13.1 ICT Risk Management

- We maintain a formal ICT Risk Management Framework that identifies, classifies, and addresses risks to the confidentiality, integrity, availability, and authenticity of information systems;
- Our BYOS architecture is specifically designed to reduce concentration risk by ensuring your documents reside in your own cloud environment rather than on a single centralised platform;

13.2 ICT Incident Reporting

- We maintain a formal ICT incident classification and reporting procedure;
- Major ICT incidents affecting the confidentiality, integrity, or availability of personal data are reported to relevant competent authorities within the timelines prescribed by DORA and applicable national regulations;
- Affected users are notified of personal data breaches in accordance with POPIA s.22 (within a reasonable time, as soon as reasonably possible) and GDPR Art. 33–34 (within 72 hours to supervisory authorities; without undue delay to affected individuals where high risk is identified);

- ICT incident records are retained for a minimum of one year, and up to five years for major incidents, in accordance with DORA Article 12.

13.4 ICT Third-Party Risk Management

- All critical ICT third-party service providers (cloud infrastructure, authentication services, document processing) are subject to formal vendor due diligence assessments prior to engagement;
- Contracts with ICT third-party providers include data processing agreements, audit rights, security standards requirements, and exit provisions;
- We maintain a Register of ICT Third-Party Providers and monitor the financial and operational stability of critical vendors on an ongoing basis.

13.5 Information Sharing

In alignment with DORA's information sharing provisions, InsuranceVault may participate in voluntary threat intelligence sharing arrangements within the financial sector to improve collective resilience, subject to appropriate anonymisation and confidentiality safeguards.

---

14. Cookies and Analytics

The InsuranceVault mobile application does not use browser cookies. We use the following analytics and tracking technologies:

- Anonymised in-app event tracking to understand feature usage and improve the application. No personally identifiable information is included in analytics events;
- Crash reporting to identify and fix technical errors. Crash reports contain device type, OS version, and error stack traces — no personal or document content;
- If you use our web portal, session cookies are used solely for authentication. You may disable cookies in your browser settings, but this will prevent you from accessing authenticated areas.

We do not use tracking pixels, cross-site trackers, fingerprinting, or advertising SDKs within the application itself. Advertising shown under the opt-out data sharing stream (Section 4) is served contextually based on asset categories, not on individual behavioural profiling, unless you have provided separate consent.

---

15. Children's Privacy

InsuranceVault is not directed at children under the age of 18. We do not knowingly collect personal information from children. If you believe we have inadvertently collected information from a child, please contact us immediately at privacy@insurancevault.co.za and we will delete the information without delay.

---

16. Changes to This Statement

We may update this Statement from time to time to reflect changes in our practices, legal obligations, or product features. When we make material changes, we will:

- Notify you via in-app notification and email at least 14 days before the changes take effect;
- Update the "Effective Date" at the top of this Statement;
- Maintain a version history of all previous versions of this Statement, available on request.

Your continued use of InsuranceVault after the effective date of any revised Statement constitutes your acceptance of the updated terms, subject to any consents we are required to obtain separately.

17. Contact Us and How to Complain

17.1 Contact Our Information Officer / DPO

For any privacy-related queries, data subject access requests, or to exercise your rights:

Privacy Contact Details
Email: privacy@insurancevault.co.za
Postal: [Physical address upon incorporation]
In-App: Profile → Settings → Privacy → Submit Privacy Request
Response time: within 30 days (POPIA) / 1 month (GDPR)

17.2 Regulatory Complaints — South Africa (POPIA)

If you are not satisfied with our response, you have the right to lodge a complaint with:

Information Regulator (South Africa)
Website: www.inforegulator.org.za
Email: complaints.IR@justice.gov.za
Tel: +27 (0)10 023 5200
Address: JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001

17.3 Regulatory Complaints — EU / EEA (GDPR)

EU and EEA data subjects may lodge a complaint with the data protection supervisory authority in their EU member state of habitual residence, place of work, or the place of the alleged infringement. A full directory of EU supervisory authorities is available at:

https://www.edpb.europa.eu/about-edpb/about-edpb/members_en

This Statement has been prepared in compliance with POPIA (Act 4 of 2013), GDPR (Regulation EU 2016/679), and DORA (Regulation EU 2022/2554).

InsuranceVault (Pty) Ltd • Version 1.0 • Effective 1 August 2026