StorePilot — Information Security & Privacy Policy

Zipf LLC (d/b/a StorePilot) · Version 1.1 · Effective August 8, 2026

1. Purpose & Scope

This policy describes how Zipf LLC (d/b/a StorePilot) protects the data it accesses and processes while operating the StorePilot platform, an AI software service that helps e-commerce sellers operate their stores through marketplace APIs (including the TikTok Shop Open API).

It applies to all company systems, personnel, and subprocessors that handle seller data, and to all data accessed under a seller's authorization.

2. Data We Access and Store

Under each seller's explicit authorization, we access store-operational data required to provide the service:

- Orders and revenue, product listings and pricing, inventory, payouts and fees, and return/refund requests.
- OAuth authorization tokens that let us call the marketplace API on the seller's behalf.

We practice data minimization: we access only what a feature needs, and we do not collect or retain buyer personal information (names, addresses, contact details) beyond what an authorized operational action strictly requires. We never move buyer personal information off the originating marketplace platform. Our document search and analytics operate on the seller's own business documents and aggregated records — never on live buyer personal data.

3. Data Classification

We classify data by sensitivity and apply controls accordingly:

- Secrets & credentials (most sensitive): marketplace OAuth tokens and encryption/signing keys. Encrypted at rest, held in a managed secret store separate from code and database, never written to logs or source control.
- Customer business data: orders, products, pricing, inventory, and payouts. Stored in a managed database encrypted at rest, and access-restricted to the seller's own account and authorized personnel.
- Buyer personal information: treated as the most privacy-sensitive class — not warehoused, not moved off the originating marketplace, and excluded from AI prompts and document indexing.
- Public information: marketing and documentation; no access restriction.

4. Encryption & Key Management

- Data in transit: all connections use TLS 1.2 or higher — between users and our application, and between our application and every marketplace and subprocessor API.

- Credentials at rest: each seller's authorization tokens are stored encrypted in a dedicated per-seller vault using authenticated symmetric encryption (AES-128 via the Fernet scheme). Tokens are never written to the database in plaintext and are decrypted only in memory at the moment of use.
- Key management: the vault encryption key is held in the hosting platform's secret store, separate from both the source code and the database. It is never committed to source control. Loss or rotation of this key is treated as a security event (see Monitoring & Incident Response).
- Database at rest: operational data is stored in a managed PostgreSQL service that encrypts data at rest with AES-256.

5. Access Control & Authentication

- Passwordless authentication via short-lived, cryptographically signed magic links — we store no passwords.
- Invite-only access: an account exists only after we explicitly provision it. Unknown parties cannot self-register or enumerate accounts.
- Role-based access: staff/administrator functions are separated from seller functions and are reachable only by authorized staff accounts.
- Least privilege, expiring sessions, and the ability to suspend an account or revoke a seller's connection immediately.

6. Least-Privilege API Authorization

We request only the API scopes our features require, and each seller grants access explicitly through the marketplace's standard OAuth consent flow. A seller may revoke that access at any time from their marketplace account or by contacting us, after which we can no longer call their store's API.

7. Human-in-the-Loop Controls

Every action that affects money or writes to a seller's store — repricing, issuing refunds, approving returns — requires explicit human approval before it executes. The platform performs no autonomous financial actions, and each approved decision is recorded.

8. Secrets & Source Control

No secrets, credentials, or seller business data are committed to our source repositories. Sensitive configuration is injected at runtime through the hosting platform's secret store, and repositories are configured to exclude environment files and any tenant data.

9. Subprocessors

We rely on a small set of reputable infrastructure providers, each under its own security commitments:

- Application hosting and managed PostgreSQL database (data storage and processing).
- DNS and edge/TLS termination.
- Transactional email (sign-in links only).

- AI processing: seller store data used to operate a store is processed via a commercial AI API. That data is used only to provide the service and is not used to train models; buyer personal information is excluded from AI prompts.

10. Data Retention & Deletion

We retain operational data only as long as needed to provide the service. When a seller disconnects a store or requests deletion, we delete the associated authorization tokens and connection. We honor marketplace account-deletion and closure notifications for the affected seller's data.

11. Monitoring, Logging & Incident Response

We maintain application and access logs to detect and investigate abnormal activity. Each access to a protected Shopify resource writes a tenant-scoped record before the provider call and an outcome record afterward. These records contain only an opaque tenant identifier, resource category, timestamp, application principal, and outcome; they never contain access tokens, queries, provider responses, customer fields, or exception text. They are stored on encrypted persistent infrastructure on a rolling retention schedule of approximately 13 months, or removed earlier with whole-tenant erasure. If the initial audit record cannot be persisted, the protected-data read is blocked. On a suspected compromise we revoke affected tokens, rotate encryption and signing keys, restore from known-good state, and notify affected sellers and marketplaces as required by contract and law.

12. Personnel & Policy Review

Access to production systems and seller data is limited to authorized personnel on a need-to-know basis. This policy is reviewed and updated at least annually, and whenever a material change to our systems or data handling occurs.

13. Contact

Security questions, disclosures, and data requests: security@storepilothq.com. Company: Zipf LLC (d/b/a StorePilot). Website: https://storepilothq.com.