

smartPOS Cloud

Privacy Policy

Effective Date: August 2026

Issued by Prodev Innovations Limited

Prodev Innovations Limited ("Prodev", "we", "us", or "our") operates smartPOS Cloud (the "Platform"). This Privacy Policy explains what personal data and business data we collect when you use the Platform, how we use it, how we protect it, and what your rights are. We are committed to protecting your privacy and handling your data with transparency and care.

1. Who We Are

1.1 Prodev Innovations Limited is the data controller for personal data processed through the Platform. We are incorporated and operating in Uganda and Rwanda, with our principal place of business in Kampala, Uganda.

1.2 You can contact our data protection contact at: legal@prodevkampala.com

2. Data We Collect

2.1 Account and Identity Data

When you register for and use the Platform, we collect:

- Full name (first name and last name) of account holders and Authorised Users
- Email address — used as your primary identifier and for communications
- Password — stored in a secure, hashed format using Supabase Auth; never stored in plaintext
- Role within your organisation (e.g., Manager, Cashier, Accountant)
- Outlet assignment — which of your business locations a user is attached to
- Onboarding progress — to guide you through initial platform setup

2.2 Business and Company Data

- Company name and unique company identifier
- Business type (Restaurant/Bar, Hotel, Retail, or Other)
- Country of operation — used for regional compliance and tax configuration
- Outlet names and locations
- Subscription package and billing status (via Stripe)

2.3 Operational and Transaction Data

In the course of running your business on the Platform, the following data is collected:

- Orders, order items, quantities, prices, and order status
- Payment settlements — payment method, amounts, and transaction references (no raw card data)
- Menu items, categories, pricing, and availability settings
- Inventory stock levels, adjustment history, and supplier records
- Table and section layouts, room bookings, and guest records (for hospitality clients)
- Financial records including journal entries, chart of accounts, and general ledger entries

- Reports and analytics data generated from the above operational data

2.4 Billing Data

- Subscription plan and billing cycle
- Stripe Customer ID and Stripe Subscription ID
- Subscription status (trialing, active, past due, or cancelled)

We do not collect, store, or have access to your credit or debit card numbers, CVV codes, or bank account details. All payment card data is handled exclusively and securely by Stripe, our PCI DSS Level 1 certified payment processor.

2.5 Technical and Usage Data

- Session tokens (JWT) issued by Supabase Auth — managed automatically and not stored in plaintext
- Device-level local data stored temporarily in offline mode (SQLite via PowerSync) — this syncs to our servers when your device reconnects to the internet
- AI menu extraction data — when you use our AI menu upload feature, the content of your uploaded menu document is processed to extract structured menu data. We do not retain the source document; only the structured output is stored.

2.6 Data We Do Not Collect

We explicitly do not collect:

- Raw payment card numbers, CVV codes, or bank account credentials
- Biometric data of any kind
- Social media profiles or third-party login tokens
- Data from individuals who are not Authorised Users of an active Client account

3. How We Use Your Data

Purpose	Data Used	Legal Basis
Providing and operating the Platform	Account, business, operational data	Contract performance
Processing payments and managing subscriptions	Billing data, Stripe identifiers	Contract performance
Authenticating users and managing access	Email, password hash, session tokens, roles	Contract performance
Sending service communications (receipts, alerts, updates)	Email address	Contract performance / Legitimate interests

Purpose	Data Used	Legal Basis
Providing technical support	Account and operational data as needed	Contract performance
Improving and developing the Platform	Aggregated, anonymised usage data	Legitimate interests
Complying with legal obligations	Any data required by applicable law	Legal obligation
Detecting and preventing fraud or security incidents	Account, session, and access data	Legitimate interests

4. Data Sharing and Third Parties

4.1 We do not sell, rent, or trade your personal data to third parties. We share data only as necessary to deliver the Platform, as described below.

Recipient	Role	Data Shared	Safeguards
Supabase	Database, Auth & Realtime infrastructure	All application data (encrypted)	SOC 2 Type II, GDPR compliant
Amazon Web Services	Cloud infrastructure (via Supabase)	All data as hosted by Supabase	ISO 27001, SOC 1/2/3, PCI DSS
Stripe	Payment processing & subscription management	Email, subscription metadata only	PCI DSS Level 1 certified
PowerSync	Offline sync engine	Sync metadata only (no PII beyond user ID)	Data remains on-device + Supabase
AI Provider (menu extraction)	Processing uploaded menu documents	Menu document content — no personal data	Subject to provider DPA

4.2 We may also disclose data: (a) to comply with applicable law, regulation, or a binding court order; (b) to protect the rights, property, or safety of Prodev, our clients, or the public; or (c) in connection with a merger, acquisition, or sale of all or part of our business, in which case the acquirer will be required to honour this Privacy Policy.

5. Data Retention

Data Category	Retention Period	Notes
User accounts	Duration of active subscription + 90 days post-cancellation	Deleted on company data purge request
Operational & transaction data	For the duration of the subscription	Retained for audit and reporting
Financial / accounting records	For the duration of the subscription	Required for business compliance

Data Category	Retention Period	Notes
Accommodation & hospitality records	For the duration of the subscription	Required for historical reporting
Session tokens (JWT)	~1 hour, auto-refreshed	Auto-expired by Supabase Auth
Stripe billing data	Managed by Stripe	Per Stripe's retention policy
AI menu extraction (source docs)	Not retained	Only structured output is stored
Offline sync cache	Local device only, until app reinstall	Synced data persists in Supabase

5.1 After your Subscription is terminated, we will retain your data for ninety (90) days to allow you to export it. After that period, your data will be permanently and irreversibly deleted from our systems.

6. Data Security

6.1 We implement a multi-layer security model to protect your data:

- **Encryption at rest and in transit** — all data stored in our database and transmitted between your device and our servers is encrypted using industry-standard protocols (TLS/SSL).
- **Row Level Security (RLS)** — enforced at the database level, ensuring that each client can only access data belonging to their own company. Cross-tenant data access is structurally prevented.
- **JWT Authentication** — all access to the Platform requires a valid, time-limited JSON Web Token issued by Supabase Auth. Unauthenticated requests are rejected.
- **Role-Based Access Control (RBAC)** — within your account, each user role is granted access only to the data and functions appropriate to their responsibilities.
- **Payment isolation** — all payment transactions are handled by Stripe; no raw payment card data ever touches our servers.

6.2 Despite these measures, no method of electronic transmission or storage is 100% secure. We cannot guarantee the absolute security of your data. In the event of a data breach that is likely to affect your rights or interests, we will notify you without undue delay as required by applicable law.

7. Your Rights

7.1 Depending on your jurisdiction, you may have the following rights in relation to your personal data:

- **Right of access** — to request a copy of the personal data we hold about you.
- **Right to rectification** — to request correction of inaccurate or incomplete personal data.
- **Right to erasure** — to request deletion of your personal data in certain circumstances.
- **Right to restriction** — to request that we restrict processing of your data in certain circumstances.

- **Right to data portability** — to receive your data in a structured, machine-readable format.
- **Right to object** — to object to processing based on legitimate interests.

7.2 To exercise any of these rights, please contact us at legal@prodevkampala.com. We will respond to all legitimate requests within thirty (30) days. In some cases, we may need to verify your identity before processing your request.

7.3 We will not discriminate against you for exercising any of these rights.

8. Cookies and Local Storage

8.1 The web-based components of the Platform use session cookies and local storage solely for authentication (to maintain your login session) and to store user preferences. We do not use advertising cookies or third-party tracking technologies.

8.2 You can configure your browser to refuse cookies, but doing so may prevent the Platform from functioning correctly.

9. International Data Transfers

9.1 Your data is hosted by Supabase on Amazon Web Services infrastructure. Depending on the AWS region configured, your data may be stored and processed outside Uganda. We take steps to ensure that such transfers are carried out in accordance with applicable data protection requirements and that your data receives an equivalent level of protection.

10. Children's Privacy

10.1 The Platform is a business-to-business service and is not intended for use by individuals under the age of 18. We do not knowingly collect personal data from minors. If you believe we have inadvertently collected such data, please contact us at legal@prodevkampala.com and we will delete it promptly.

11. Changes to This Policy

11.1 We may update this Privacy Policy from time to time to reflect changes in the Platform, applicable law, or our data practices. When we make material changes, we will notify you via email or a prominent in-platform notice at least fourteen (14) days before the updated Policy takes effect.

11.2 The current version of this Privacy Policy, including its effective date, will always be available at prodevkampala.com/privacy.

12. Contact Us

For any privacy-related questions, concerns, or requests, please contact us:

- **Company:** Prodev Innovations Limited
- **Data Contact Email:** legal@prodevkampala.com
- **Phone:** +256 780 101 601
- **Website:** prodevkampala.com
- **Address:** Kampala, Uganda

We are committed to resolving any privacy concerns you may have. If you are unsatisfied with our response, you may have the right to lodge a complaint with your applicable data protection authority.