Privacy Policy

Last updated: February 21, 2026

1. Introduction

Hookr ("**Hookr**", "**we**", "**us**", or "**our**") is a mobile application for Android and iOS that allows users to create and manage webhooks, receive push notifications about webhook events, and optionally forward webhook requests to their own services.

This Privacy Policy explains what data we collect, how we use it, and your rights.

Contact: **info@hookr.app**

2. Who Operates Hookr

Hookr is operated by an **individual (sole proprietor)** and is not registered as a legal entity.

Our servers are located in the **United States**.

3. Eligibility

You must be **at least 16 years old** to use Hookr. We do not knowingly collect data from children under 16.

4. Accounts & Authentication

To use Hookr, an account is required. We collect:

- Email address
- Authentication credentials (securely handled)
- OAuth identifiers (Google / Apple), if used
- Shopify shop URL (e.g., `my-shop.myshopify.com`), if connecting via Shopify OAuth

Users may delete their account at any time. Instructions are available at:

https://hookr.app/delete-account

4.1 Shopify OAuth

When you authorize Hookr through a Shopify app using OAuth 2.0 Authorization Code flow with PKCE:

- **OAuth tokens** (access and refresh tokens) are **issued by Hookr and stored by the Shopify app**, not by Hookr
- **Shopify shop URL** is stored in Hookr's database for identification
- You can disconnect at any time using the Disconnect button in your Shopify app or mobile app Settings → Integrations
- Upon disconnect, the shop URL is deleted immediately from our database but may persist in logs or backups per our standard retention policy.

5. Webhook Data Handling

5.1 Private vs Non-Private Webhooks

Each webhook includes a user-controlled **"Private"** setting.

Private Webhooks

- Webhook payloads (body, headers, query string) are **never stored**
- Data is handled only in runtime

Non-Private Webhooks

- Webhook payloads may be stored for up to **7 days**
- Limited technical data may appear in logs for up to **30 days**

6. Webhook URLs & Secrets

Webhook URLs are treated as **sensitive data**, especially when a webhook is marked as Private. We do not sell or disclose webhook URLs to third parties.

7. Webhook Forwarding

Hookr can forward incoming webhooks to user-defined URLs:

- Payloads are forwarded **as-is**
- No retries are performed
- No delivery guarantees are provided
- Forwarded requests include an **HMAC SHA-256 signature**

8. Push Notifications

Push notifications are a core feature of Hookr. We collect:

- Device identifiers
- Push notification tokens

Users may fully disable notifications or configure delivery schedules.

9. Analytics & Crash Reporting

We use the following third-party services:

- **Supabase** – database and authentication

- **Firebase** – push notifications and crash reporting
- **Aptabase** – anonymous analytics (feature usage & marketing insights)
- **RevenueCat** – subscription and in-app purchase management (may process Device ID and App User ID)

Payment information is handled entirely by Apple and Google.

10. Data Retention

Data Type	**Retention**
Account data	Until account deletion
OAuth shop identifiers (Shopify URL)	Until disconnect or account deletion;
Private webhook payloads	Not stored
Non-private webhook payloads	Up to 7 days
Logs	Up to 30 days
Backups	Up to 30 days
Analytics	Anonymous & aggregated
Subscription identifiers (Device ID, App User ID)	While account is active and as required for legal/accounting purposes

11. International Data Transfers

By using Hookr, you consent to your data being processed in the **United States**.

12. Your Rights

You may request access, correction, or deletion of your data by contacting **info@hookr.app**.

13. GDPR (EEA Residents)

Legal Basis

We process personal data based on:

- Contractual necessity
- User consent
- Legitimate interests
- Legal obligations

Your GDPR Rights

You have the right to access, correct, delete, restrict, or object to processing, and to request data portability. You may also lodge a complaint with your local data protection authority.

14. CCPA / CPRA (California Residents)

Categories of Data

We may collect identifiers, device information, usage data, and technical diagnostics.

Your Rights

California residents have the right to know, access, correct, and delete personal data. Hookr does **not sell or share** personal data for advertising purposes.

Requests can be made via **info@hookr.app**.

15. Changes

We may update this Privacy Policy from time to time. Updates will be published in the app or on our website.