Picco
Privacy Policy

Effective: May 7, 2026 · Last updated: May 7, 2026

1. Introduction

This Privacy Policy describes how Picco Technologies ("we", "our", or "us") collects, uses, and shares information when you use the Picco platform. We are committed to protecting your personal data in accordance with Ghana's Data Protection Act, 2012 (Act 843) and other applicable privacy laws.

2. Information We Collect

2.1 Account Information. When you register we collect your name, email address, phone number, password (hashed), and user role (photographer or client).

2.2 Profile and Event Data. Photographers provide event names, descriptions, and pricing. Clients may provide a profile photo.

2.3 Biometric / Facial Data. When you use the face-search feature we process facial feature vectors extracted from your reference photo. This constitutes biometric data under applicable law.

2.4 Payment Data. We collect transaction records (amount, timestamp, reference ID). Full card numbers are processed and stored exclusively by Paystack — we never see or store raw card details.

2.5 Usage and Technical Data. We automatically collect IP addresses, device type, browser information, pages visited, and timestamps to operate, secure, and improve the platform.

2.6 Communications. If you contact support, we retain a record of that correspondence.

3. How We Use Your Information

We use your information to: (a) create and maintain your account; (b) match your face to event photos (biometric processing); (c) process payments and payouts; (d) send transactional emails and SMS notifications; (e) detect fraud and enforce these policies; (f) comply with legal obligations; and (g) improve our services through aggregated, anonymised analytics.

4. Facial Recognition and Biometric Data

Biometric data is classified as special category data under data protection law and is subject to the highest level of protection we apply.

4.1 What Biometric Data We Process. When you choose to use the face-search feature, we process a mathematical representation of your facial features (a "face template" or "facial embedding") derived from your uploaded reference photo. We do not store raw reference photos for ongoing recognition.

4.2 Purpose of Biometric Processing. We use biometric data solely to: (i) identify and locate photos of you from event images uploaded to the platform; and (ii) improve matching accuracy for your

personal account. We do NOT use it for advertising, marketing, user profiling, identity verification outside this feature, or training unrelated AI models.

4.3 Legal Basis — Explicit Consent. We process biometric data only on the basis of your explicit, freely-given, specific, and informed consent. Consent is collected through a dedicated opt-in screen before any biometric processing begins. We log the timestamp and policy version of your consent as a legal record. You may withdraw consent at any time.

4.4 Consent Is Freely Given — No Penalty for Refusal. Refusing or withdrawing consent for facial recognition will never prevent you from using the rest of the platform. You can browse, purchase, and communicate without ever enabling the feature.

4.5 Third-Party Processor. Facial feature extraction is performed by a third-party AI service. This provider operates under a data processing agreement that: (i) restricts use to providing the recognition service to us; (ii) prohibits use of your data for the provider's own commercial purposes; and (iii) requires deletion of your data upon our request.

4.6 Retention. Ephemeral face vectors created during a single search request are deleted immediately after results are returned. Persistent face models linked to your account are retained only while your account is active and the feature is enabled. Upon account deletion or withdrawal of consent, all biometric data is purged within 30 days.

4.7 No Sale of Biometric Data. We will never sell, rent, lease, or otherwise trade your biometric data to any third party for any commercial purpose.

4.8 Security of Biometric Data. Face templates are encrypted at rest and in transit, stored separately from directly-identifying personal data where technically feasible, and access is restricted to the minimum number of personnel and systems required.

4.9 Scope of Matching. Our system only runs facial recognition in response to a specific, user-initiated search request. We do not perform background scanning, persistent surveillance, or automatic identification of individuals across all uploaded photos without a direct user request.

5. Sharing of Information

We share your information only in the following circumstances:

5.1 Service Providers. We share data with third-party service providers who assist us in operating the platform: Cloudinary (image storage), Paystack (payments), SendGrid (email), Arkesel (SMS), and our facial recognition AI provider. Each is bound by data processing agreements.

5.2 Photographers and Clients. Photographer profile information is visible to Clients browsing events. Client identity is not revealed to Photographers beyond what is necessary to fulfil a transaction.

5.3 Legal Requirements. We may disclose information if required by law, court order, or governmental authority, or where necessary to protect the rights, property, or safety of our users or the public.

5.4 Business Transfers. In the event of a merger, acquisition, or sale of assets, your data may be transferred to the successor entity, subject to equivalent privacy protections.

6. Data Retention

We retain account and transaction data for as long as your account is active and for up to 7 years thereafter to comply with financial record-keeping obligations. Biometric data linked to deleted accounts is purged within 30 days of account deletion. Server access logs are retained for 90 days.

7. Your Rights

Under Ghana's Data Protection Act 2012 (Act 843) and, where applicable, international standards (GDPR / CCPA), you have the following rights:

(a) Access — request a copy of all personal data we hold about you, including a confirmation of whether we are processing your biometric data.

(b) Rectification — ask us to correct inaccurate or incomplete data.

(c) Erasure ('Right to be Forgotten') — request deletion of your personal data. For biometric data we will purge all face templates and request erasure from third-party processors within 30 days. Certain financial records may be retained to meet statutory obligations.

(d) Withdrawal of Consent — withdraw consent for biometric (facial recognition) processing at any time, in-app or by contacting us. Withdrawal does not affect the lawfulness of prior processing.

(e) Restriction — ask us to pause processing while a complaint is resolved.

(f) Data Portability — receive your account data in a structured, machine-readable format (JSON or CSV).

(g) Objection — object to any processing we conduct on the basis of legitimate interests.

To exercise any of these rights, email skiddodanso@gmail.com. We will acknowledge within 5 business days and respond in full within 30 days. We will not charge a fee for standard requests.

8. Security

We implement industry-standard security measures including: TLS encryption in transit, bcrypt password hashing, JWT-based authentication, Redis-backed rate limiting, and access controls. However, no system is completely secure. You are responsible for keeping your account credentials confidential.

9. Cookies and Tracking

Our API does not set browser cookies directly. If you access the platform through a web or mobile application, that application may use local storage or device identifiers solely for session management and user experience purposes. We do not use third-party advertising trackers.

10. Children's Privacy

The platform is not directed to children under 18. We do not knowingly collect personal data from minors. If you believe a minor has provided us with personal data, please contact skiddodanso@gmail.com and we will delete it promptly.

11. International Data Transfers

Some of our service providers are located outside Ghana. When we transfer your data internationally we ensure appropriate safeguards are in place, such as standard contractual clauses

or adequacy decisions, to protect your information to an equivalent standard.

12. Changes to This Policy

We may update this Privacy Policy periodically. If we make material changes we will notify you by email at least 14 days before the changes take effect. The updated policy will be accessible at this URL with a revised effective date.

13. Contact and Data Controller

Picco Technologies is the data controller for personal data processed through the platform. For any privacy-related queries or complaints, contact us at skiddodanso@gmail.com or write to Picco Technologies, Accra, Ghana.