SCANTIQUE AI — PRIVACY POLICY

Last Updated: December 19, 2025

Operator / Data Controller: Ruslan Badaev (individual)

Contact (privacy + support): dev.badaeff@gmail.com

This Privacy Policy explains how Scantique AI (“Scantique AI”, the “App”, the “Service”, “we”, “us”, “our”) collects, uses, shares, and protects information when you use the Service.

This policy is intended to describe our data handling in a clear way and to support common app-store disclosure expectations. If you do not agree with this policy, do not use the App.

1) Scope

This policy covers the Scantique AI mobile application and related services, including any websites we operate for the Service (for example, pages used to host Terms and this Privacy Policy).

It does not cover third-party websites or services you access via links (for example, the “Sell” feature opening an external browser search).

2) Key points (plain-language)

• You can upload 1–4 photos, optional text description, and optional manual location text (you decide what to provide).

• Your Inputs are sent to our server and then to service providers (including AI providers) to generate results.

• We do not store your uploaded photos on our servers by design.

• We store scan results/records (the object you see on your dashboard) so you can view them later; you can delete them in the App.

• We use third-party providers (such as Firebase, RevenueCat, AI providers, and hosting providers) to operate the Service.

• We do not run ads and do not sell data for advertising.

3) Information we collect

3.1 Information you provide

A) Scan Inputs (“User Content”)

• Photos/images you upload (1–4).

• Description text you type.

• Location text you type (optional). We do not require GPS; if you provide location, it is manual text unless your device or app features provide otherwise.

Important: You control what you submit. Do not submit sensitive personal data if you do not want it processed (e.g., IDs, financial info, private documents, or third-party private information).

3.2 Information collected automatically

A) Device + technical data (logs)

We (and our providers) may collect technical data such as:

• IP address.

• Language/locale, device model, operating system version, and app version.

• Approximate region derived from IP, user agent (where applicable), timestamps, diagnostics, and performance metrics.

B) Crash & diagnostics

We use crash reporting (e.g., Firebase Crashlytics). Crash logs may include stack traces and associated device/app diagnostics to help us fix reliability issues.

C) Identifiers

• Firebase Anonymous ID (anonymous authentication identifier).

• RevenueCat identifiers and entitlement information.

• Store-related identifiers (where provided by Apple/Google/RevenueCat).

We do not require account registration and do not ask for your name, phone number, or address.

3.3 Subscription and purchase data

Subscriptions are handled through Apple App Store In-App Purchases and/or Google Play Billing. We use RevenueCat to verify subscription status and entitlements.

We may receive and store data such as subscription status (active/expired/trial), product identifiers, purchase/renewal timestamps, and transaction identifiers/receipts as needed for verification, fraud prevention, entitlement restoration, and operations.

We do not receive your full payment card details from Apple/Google.

3.4 Website contact

Our website contact flow is designed to open your mail app to email us. We do not run site tracking by design. If you email us, we will receive whatever you send as part of normal email communication.

4) How we use information

We use information to:

• Provide the Service (process Inputs, generate outputs, and display scan results).

• Operate subscriptions (verify entitlements, prevent fraud, restore access).

• Safety, security, and abuse prevention (including rate limiting, suspicious behavior detection, and manual review).

• Diagnostics and reliability (crash investigation, bug fixing, performance improvements).

• Compliance and enforcement (comply with lawful requests where required and enforce our Terms).

5) How we share information

We share data only as needed to run the Service, with vendors acting as service providers/processors.

Providers may include (non-exhaustive):

• AI providers (e.g., OpenAI, Google services, DeepSeek, or other AI vendors).

• Firebase / Google Cloud (anonymous authentication, crash reporting, push notifications if enabled).

• RevenueCat (subscription and entitlement verification).

• Branch.io (attribution/deep linking, if enabled).

• Hosting/infrastructure providers (including VPS hosting).

We may also share information for legal compliance (when required by law) and to protect rights, safety, and security (e.g., investigating fraud or abuse).

No ads / no data brokerage: We do not sell personal data to data brokers and do not share personal data for cross-context behavioral advertising.

6) AI processing, photos, and outputs

6.1 What happens to your Inputs

Your photos/text are transmitted to our server and then to relevant providers to produce results. This is necessary to provide the Service.

6.2 Storage of photos and outputs

• Uploaded photos: we are designed not to store them on our servers after processing.

• Scan results/records: we store the scan results object shown in your dashboard so you can view it later, until deletion/retention limits.

• Local storage: the App may store results and related metadata locally on your device (database/shared storage) for usability.

6.3 Training

We do not use your Inputs to train our models by default, and we do not allow training use unless we implement a clear opt-in mechanism.

6.4 Moderation

We may review activity and related data (and, where needed, associated content) to investigate abuse, fraud, prohibited content, or security incidents.

7) Push notifications

We may use Firebase Cloud Messaging and/or local notifications for service/operational notices and product updates (if enabled). You can control notifications in your device settings. We do not guarantee delivery.

8) Data retention

Unless a longer period is required or justified for legal or security reasons, we may retain:

• Scan results/records: up to 365 days.

• Technical logs/diagnostics/anti-abuse signals: up to 365 days.

• Purchase/subscription records: up to 365 days (or longer if needed for disputes, fraud prevention, or accounting/operations).

Backups: We may keep server backups (typically monthly), and backup/retention practices may change at our discretion.

Important: Deleting the App from your device does not automatically delete server-side records.

9) Your choices and controls

9.1 In-app deletion

• You can delete scan results/objects from the dashboard.

• You can use an in-app clear/cleanup option (where available) to remove local app data.

9.2 Requests (access/deletion)

You can request access or deletion by contacting us (or via the website flow that emails us). To help verify the request and prevent unauthorized deletion, we may ask you to provide your Firebase Anonymous ID and/or RevenueCat identifier and supporting details.

We may deny or limit requests where we cannot verify identity, where the request is abusive, or where we must retain data for legal/security reasons.

10) International data transfers

Our primary server/infrastructure may be located in the United Arab Emirates (UAE), and our providers may process data in other countries where they operate. By using the Service, you understand your data may be transferred and processed outside your country of residence.

11) Security

We use reasonable safeguards, including HTTPS/TLS in transit. No system is 100% secure; we cannot guarantee absolute security.

12) Children

The Service is not directed to children. We do not implement age verification. If you are a parent/guardian and believe a minor has provided personal data, contact us and we will handle it as appropriate.

13) Legal bases and privacy rights (jurisdiction-dependent)

Some jurisdictions grant specific privacy rights (e.g., access, deletion, correction, portability, and objection). Where required by applicable law, we will honor eligible requests. We may request information to verify you.

We do not sell or share personal information for cross-context behavioral advertising. If you still want to submit an opt-out request where applicable, contact us.

14) Changes to this Privacy Policy

We may update this policy from time to time by changing the “Last Updated” date and/or providing notice in the App. Continued use after updates means you accept the updated policy.

15) Contact

For privacy questions or requests: **dev.badaeff@gmail.com**
Subject suggestion: **Scantique AI — Privacy Request**