ALGOZ

Algoz App — Data Protection & Compliance Overview

VERSION 1.0 · 03 JUL 2026

Excellence, Discreetly Delivered.

DATA & COMPLIANCE

How the Algoz App protects your data.

ALGOZ FZ-LLC · TRADE LICENCE 5033995 · TRN 105119056700001 · VERSION 1.0 · 03-JUL-2026

1. Purpose and scope

This document describes, in plain language, what data the Algoz application collects, where it lives, how it is protected, and which regulations govern it. It is an informational overview for members, clients and their advisers; it complements — and does not replace — the Algoz Privacy Policy and the Algoz App Terms of Use.

Data controller: Algoz FZ-LLC, trading as Algoz Group, Compass Building — Al Hulaila, VUNE0977, Ras Al Khaimah, UAE. Trade Licence 5033995, TRN 105119056700001. Privacy contact: privacy@algozgroup.com.

2. Regulatory framework

- **UAE Personal Data Protection Law** (Federal Decree-Law No. 45 of 2021, PDPL) — the primary framework applicable to Algoz as a UAE-registered company.
- **EU GDPR and UK GDPR** — clients located in the European Union or the United Kingdom retain their rights under these regulations.
- **RAKEZ regulations** and UAE federal law, including statutory KYC verification required before services commence, handled in strict confidence.
- All personnel and partners are bound by **non-disclosure agreements**; information travels on a need-to-know basis.

3. What the App collects

- **Account and profile data** — name, contact details, language, nationality, preferences, membership tier, assigned agents.
- **Service data** — the requests you submit, their status and history, related calendar entries and agreements.
- **Concierge conversations** — messages and attachments, encrypted end-to-end (see Section 5).
- **Location** — only when you actively share it: with a request, via Share Location, or through Urgent Assistance. Never in the background.
- **Device and usage signals** — push-notification token, app language/theme settings, sign-in and activity timestamps used for service quality and security.

4. What Algoz does not do

- Your data is **never sold and never shared with third parties** for their own purposes.
- Your contact details are **never used for newsletters or marketing** — they exist to deliver your service.
- There is **no background location tracking** and no advertising profiling of any kind inside the App.

- Members are always served by Algoz personnel — never by bots.

5. Where data lives and how it is encrypted

The App runs on Google Firebase infrastructure (Firestore database, Firebase Authentication, Cloud Storage and Cloud Messaging) — enterprise-grade infrastructure certified under ISO/IEC 27001, 27017, 27018 and SOC 1/2/3, with encryption in transit (TLS) and at rest as standard. On top of the platform encryption, Concierge Chat content is additionally encrypted at application level with **AES-256-GCM**, so message content is sealed within your Algoz circle. The database is protected by point-in-time recovery and scheduled backups.

6. Access control architecture

- **Deny by default.** Every database collection is governed by server-enforced security rules; anything not explicitly permitted is refused. Sensitive administrative collections are entirely closed to client applications.
- **Ownership enforcement.** A user can read and write only records that belong to them; identity is verified server-side on every operation, which structurally prevents cross-account access (IDOR).
- **Member gating.** Member-only actions verify an active membership record server-side; non-members cannot reach member data even with valid credentials of another account class.
- **Tamper protection.** Members can edit only a defined whitelist of their own profile fields; tier, status and entitlements are administrator-controlled.
- **Instant revocation.** Deactivated accounts are disabled at the authentication layer and ejected from all devices; revoked access ends everywhere, immediately.
- **Staff access** runs through a separate administrative console with a granular role and permission matrix, two-factor authentication (TOTP), and server-side service credentials that never leave the server. Administrative actions are recorded in an activity log.

7. Application and network security

- Strict transport security (HSTS with preload), Content-Security-Policy including frame-ancestors restrictions (clickjacking protection), X-Frame-Options, X-Content-Type-Options and a strict referrer policy on the App.
- Cross-origin requests are restricted to Algoz domains on sensitive endpoints; authentication tokens are never carried in URLs.
- Rate limiting at the network edge and per-IP at the origin, with account-level lockouts after repeated failed sign-ins and provider-level throttling on the authentication service — brute-force attempts are limited by both IP and account.
- The platform uses a NoSQL document store accessed through typed APIs — there is no SQL surface to inject into.
- Security events (rate blocks, administrative security actions) are logged and alerted.

8. Retention and deletion

Personal data is retained for the duration of the membership or client relationship, and thereafter only as long as required by UAE statutory obligations (including KYC and commercial record-keeping). Upon verified request, data not subject to a legal retention duty is deleted. Requests: privacy@algozgroup.com.

9. Sub-processors and third parties

- **Google (Firebase / Google Cloud)** — application infrastructure, authentication, database, storage, push notifications.
- **Apple App Store / Google Play** — application distribution only; no membership data or payments flow through the stores.
- **Cloudflare** — network edge and delivery protection for Algoz web infrastructure.
- Payment processing occurs outside the App under the General Terms and Conditions. Operational partners receive only the minimum information needed for a confirmed engagement, under NDA.

10. Incident response

Algoz maintains monitoring and alerting on authentication and administrative activity, point-in-time recovery and scheduled backups for data restoration, and an escalation procedure for suspected incidents. Where an incident affects personal data, Algoz notifies affected clients and the competent authorities in accordance with the UAE PDPL and, where applicable, GDPR/UK GDPR timelines.

11. Your rights

Subject to applicable law, you may request access to, correction of, deletion of, or restriction of the processing of your personal data, object to processing, and request portability. Clients in the EU/UK retain their full GDPR/UK GDPR rights, including the right to lodge a complaint with their supervisory authority. All requests are handled in confidence: **privacy@algozgroup.com**.

12. Document control

This overview is reviewed with each material change to the App's architecture and at least annually. The current version is always available at algozgroup.com/algoz-app-data-compliance. Version 1.0 — issued 03-JUL-2026.

ALGOZ FZ-LLC

Trade Licence 5033995 · TRN 105119056700001 · RAKEZ, Ras Al Khaimah, UAE · privacy@algozgroup.com

Excellence, Discreetly Delivered.