Privacy: MedAdmin Doctor app

MedAdmin · Version 1.1 · effective from 11 November 2026

This policy applies to the **MedAdmin Doctor** mobile app (iOS and Android), used by the staff of practices that subscribe to MedAdmin: doctors, nurses, reception, owners.

1. Summary

- **Who the app is for.** Only for the staff of a MedAdmin client practice. The account is created by the practice; you cannot create an account yourself in the app.
- **Patient data** that you view and enter belongs to the practice, which is its **controller**. Alucard Limited ("Alucard", "we", "us") processes it only as the practice's **processor**.
- **Your account data** (name, email, role, devices) is processed by the practice, as employer or contracting partner, and by Alucard, as the service provider, in accordance with the platform Privacy Policy.
- **On the phone:** data saved for offline work is **encrypted**, is not included in iCloud or Android backup and is deleted on sign-out. The app locks with biometrics; **biometric data never reaches us**.
- **Push notifications contain no medical data.** No advertising, no tracking, no third-party analytics tools.
- **Account deletion:** from the app, Profil → Solicită ștergerea contului (Profile → Request account deletion). Contact: gdpr@medadmin.ro.

2. Who we are and who the controller is

2.1. The app is provided by Alucard Limited (registered name ALUCARD LIMITED), UBI 81569528, registered office Unit B, 11/F, 23 Thomson Road, Wan Chai, Hong Kong SAR China, data protection contact gdpr@medadmin.ro.

2.2. For **patient data** (schedule, record, consultations, clinical photographs, signatures, payments), the controller is the **practice** you work for. Alucard processes it under the Data Processing Agreement concluded with the practice.

2.3. For **your user account data**, the practice is the controller (it creates your account, sets your role and can deactivate it), and Alucard processes this data on behalf of the practice and, for the security of the service (logs, abuse prevention), as controller, on the basis of legitimate interest.

3. What data the app processes

Data	Why	Legal basis
Your account: name, email, role, practice, location, permissions	authentication and showing only what you are allowed to see	Article 6(1)(b) and (f) GDPR
Authentication: email and password (the password is not stored on the phone), two-factor authentication code, device token	secure access; the token can be revoked from the platform	Article 6(1)(b) and (f); Article 32
Device: name, platform, app version, push notification token	managing connected devices and sending notifications	Article 6(1)(b)
Patient data you view or enter: appointments, record, consultations, clinical photographs, consent signatures, payments	the medical and administrative activity of the practice	determined by the practice as controller, usually Article 9(2)(h) GDPR and Law 46/2003 on patients' rights

Data	Why	Legal basis
Access log: which record you opened, when and from which device (including downloads for offline work)	the practice's obligation to keep a record of access to medical data; security	Article 6(1)(c) and (f); Article 32
The account deletion request and the reason, if you give one	handling the request	Article 6(1)(c) and (f)

The app does not collect location, the phone's contacts, browsing history or the advertising identifier, and does not include third-party analytics or crash reporting tools.

4. Data on the phone

4.1. The **access token** is kept in the Keychain (iOS) or Keystore (Android), bound to the device.

4.2. **Offline work.** The app keeps locally the schedule of the days you have opened, recent and today's patients (the list row and the record summary) and the queue of status changes made without a connection. Everything is stored in an **encrypted** database (AES-256, in SQLCipher mode), with the key in the Keychain or Keystore. The records of the patients in the day's schedule are downloaded in the background and each download appears in the practice's access log.

4.3. The local database and temporary files are **excluded from iCloud backup and from Android automatic backup** and are deleted on sign-out, on revocation of the device from the platform and on uninstallation.

4.4. Consultations, signatures, photographs, payments and new appointments cannot be made offline: they are sent directly to the server and do not remain on the phone.

5. Biometrics and app lock

5.1. The app locks after inactivity and is unlocked with Face ID, Touch ID or fingerprint, through the operating system.

5.2. **Biometric data does not leave the phone and does not reach Alucard or the practice.** The app receives from the system only the answer "recognised / not recognised".

6. Permissions

Permission	What it is used for	When it is requested
Camera	photographing a lesion or a document, attached to the patient's record	only when you tap „Fotografiază” (Take photo)
Notifications	confirmations, tasks, internal messages	after an explanation; the app works without them
Biometrics (Face ID, fingerprint)	unlocking the app	when you enable unlocking
Internet	communication with the practice's server	by default

To choose an existing photograph the app uses the system picker, which does not give access to the whole gallery. We do not request access to location, contacts, microphone or the phone's files.

7. Clinical photographs

Photographs taken in the app are sent directly to the patient's record, on the practice's server, and are not saved in the phone's gallery. Photographing a patient for medical purposes requires the patient's consent, which the practice obtains (for example through the clinical photographs consent in MedAdmin).

8. Push notifications

Notifications are sent through Firebase Cloud Messaging (Google) and have generic text, with the title "MedAdmin" and a message such as „Agenda ta s-a actualizat.” ("Your schedule has been updated."), „Ai o sarcină nouă sau actualizată.” ("You have a new or updated task.") or „Ai un rezultat nou de văzut.” ("You have a new result to view."), **without the patient's name, diagnoses or other medical data**. The details are visible in the app, after unlocking. The notification token is deleted on sign-out and on revocation of the device.

9. Imaging and automated analyses

Image viewing (DICOM) in the app is **for documentation and communication**, not for diagnosis. Automated analyses (for example tooth segmentation from a CT scan) run on MedAdmin servers in the EU, and the result is a **suggestion to be confirmed by the doctor**. MedAdmin is not a medical device.

10. Deleting the account

10.1. From the app: **Profil → Solicită ștergerea contului (Profile → Request account deletion)**. The request reaches the practice owner, as a task with a 7-day deadline, and is recorded at Alucard. The account is deactivated and deleted by the practice, which is your employer or contracting partner; if you receive no answer within 30 days, write to us at gdpr@medadmin.ro and we will step in.

10.2. The following remain with the practice, because the law requires it: medical documents signed by you, consultations, consents and the access log, with your name as author (Law 46/2003 on patients' rights, Law 95/2006 on healthcare reform, archiving rules).

10.3. On the phone, signing out immediately deletes the token and the local data.

11. How long we keep data

Patient data: as long as the practice decides, in accordance with its legal obligations. Your account: as long as the practice keeps you as a user and at most 30 days after the practice's contract ends. Security logs: 12 months. Device tokens: until sign-out or revocation.

12. To whom we disclose data

To our suppliers in the list of sub-processors: Hetzner (hosting, Germany), Google through Firebase Cloud Messaging (push notifications, without medical data), Ploi (server administration). The data is not sold and is not used for advertising.

13. Transfers and security

The data is hosted in the EU (Germany); remote access by the Alucard team from Hong Kong relies on the European Commission's standard contractual clauses (Decision (EU) 2021/914), concluded with the practice through the Data Processing Agreement, and the data remains stored in the EU. Google may process the notification token in the USA (EU–US Data Privacy Framework or standard contractual clauses). Communication takes place over HTTPS only; the app applies the same permissions as the web platform and the same two-factor authentication.

14. Your rights

For your account data you may request access, rectification, erasure, restriction, portability, or object to processing: with the practice or at gdpr@medadmin.ro. Complaints: **ANSPDCP** (National Supervisory Authority for Personal Data Processing), B-dul G-ral. Gheorghe Magheru 28-30, sector 1, Bucharest, www.dataprotection.ro; **PCPD** (Hong Kong), www.pcpd.org.hk.

15. Changes

We publish each new version at this address, with a version and date, and announce it in the app when the change is important.