

Confidențialitate: aplicația MedAdmin Doctor

MedAdmin · Versiunea 1.0 · În vigoare din 9 octombrie 2026 · Versiune de lucru, în revizuire juridică

Această politică se aplică aplicației mobile **MedAdmin Doctor** (iOS și Android), folosită de personalul cabinetelor care au abonament MedAdmin: medici, asistenți, recepție, titulari.

1. Rezumat pe scurt

- **Pentru cine e aplicația.** Doar pentru personalul unui cabinet-client MedAdmin. Contul îl creează cabinetul; nu îți poți face singur cont în aplicație.
- **Datele pacienților** pe care le vezi și le introduci aparțin cabinetului, care este **operatorul** lor. Sysqo Limited („Sysqo”, „noi”) le prelucrează doar ca **persoană împuternicită** a cabinetului.
- **Datele contului tău** (nume, email, rol, dispozitive) le prelucrează cabinetul, ca angajator sau colaborator, și Sysqo, ca furnizor al serviciului, conform [Politicii de confidențialitate a platformei](#).
- **Pe telefon:** datele salvate pentru lucrul fără internet sunt **criptate**, nu intră în backup-ul iCloud sau Android și se șterg la deconectare. Aplicația se blochează cu biometrie; **datele biometrice nu ajung la noi**.
- **Notificările push nu conțin date medicale.** Fără reclame, fără tracking, fără instrumente de analiză ale terților.
- **Ștergerea contului:** din aplicație, Profil → Solicită ștergerea contului. Contact: gdpr@medadmin.ro.

2. Cine suntem și cine este operatorul

2.1. Aplicația este furnizată de Sysqo Limited (denumirea înregistrată SYSQO LIMITED), Company number 14417339, sediul social 18 Old Field Road, Pencoed, Bridgend, Wales, CF35 5LJ, Regatul Unit, contact pentru protecția datelor gdpr@medadmin.ro.

2.2. Pentru **datele pacienților** (agenda, fișa, consultațiile, fotografiile clinice, semnăturile, încasările), operatorul este **cabinetul** pentru care lucrezi. Sysqo le prelucrează conform [Acordului de prelucrare a datelor](#) încheiat cu cabinetul.

2.3. Pentru **datele contului tău de utilizator**, cabinetul este operator (îți creează contul, îți stabilește rolul, îl poate dezactiva), iar Sysqo prelucrează aceste date în numele cabinetului și, pentru securitatea serviciului (jurnale, prevenirea abuzurilor), ca operator, pe baza interesului legitim.

3. Ce date prelucrează aplicația

Date	De ce	Temei
Contul tău: nume, email, rol, cabinetul, locația, permisiunile	autentificarea și afișarea doar a ce ai voie să vezi	art. 6 alin. (1) lit. (b) și (f) GDPR
Autentificarea: email și parolă (parola nu se păstrează pe telefon), codul de autentificare în doi pași, tokenul de dispozitiv	accesul securizat; tokenul se poate revoca din platformă	art. 6 alin. (1) lit. (b) și (f); art. 32
Dispozitivul: numele, platforma, versiunea aplicației, tokenul de notificări push	gestionarea dispozitivelor conectate și trimiterea notificărilor	art. 6 alin. (1) lit. (b)
Datele pacienților pe care le consulți sau le introduci: programări, fișa, consultații, fotografii clinice, semnături de consimțământ, încasări	activitatea medicală și administrativă a cabinetului	stabilit de cabinet ca operator, de regulă art. 9 alin. (2) lit. (h) GDPR și Legea 46/2003

Date	De ce	Temei
Jurnalul de acces: ce fișă ai deschis, când și de pe ce dispozitiv (inclusiv descărcările pentru lucrul fără internet)	obligația cabinetului de a ține evidența accesului la date medicale; securitate	art. 6 alin. (1) lit. (c) și (f); art. 32
Cererea de ștergere a contului și motivul, dacă îl scrii	rezolvarea cererii	art. 6 alin. (1) lit. (c) și (f)

Aplicația nu colectează locația, contactele din agenda telefonului, istoricul de navigare sau identificatorul de publicitate și nu include instrumente de analiză sau de raportare a erorilor ale terților.

4. Datele de pe telefon

4.1. **Tokenul de acces** se păstrează în Keychain (iOS) sau Keystore (Android), legat de dispozitiv.

4.2. **Lucrul fără internet.** Aplicația păstrează local agenda zilelor pe care le-ai deschis, pacienții recentți și de azi (rândul din listă și rezumatul fișei) și coada modificărilor de stare făcute fără conexiune. Totul stă într-o bază de date **criptată** (AES-256, în modul SQLCipher), cu cheia în Keychain sau Keystore. Fișele pacienților din agenda zilei se descarcă în fundal și fiecare descărcare apare în jurnalul de acces al cabinetului.

4.3. Baza locală și fișierele temporare sunt **excluse din backup-ul iCloud și din backup-ul automat Android** și se șterg la deconectare, la revocarea dispozitivului din platformă și la dezinstalare.

4.4. Consultația, semnătura, fotografiile, încasările și programările noi nu se fac fără conexiune: se trimit direct la server și nu rămân pe telefon.

5. Biometria și blocarea aplicației

5.1. Aplicația se blochează după inactivitate și se deblochează cu Face ID, Touch ID sau amprentă, prin sistemul de operare.

5.2. **Datele biometrice nu ies de pe telefon și nu ajung la Sysqo sau la cabinet.** Aplicația primește de la sistem doar răspunsul „recunoscut / nerecunoscut”.

6. Permisunile

Permisune	La ce folosește	Când se cere
Camera	fotografierea unei leziuni sau a unui document, atașate în fișă pacientului	doar când apeși „Fotografiază”
Notificări	confirmări, sarcini, mesaje interne	după o explicație; aplicația funcționează și fără
Biometrie (Face ID, amprentă)	deblocarea aplicației	la activarea deblocării
Internet	comunicarea cu serverul cabinetului	implicit

Pentru alegerea unei fotografii existente aplicația folosește selectorul sistemului, care nu dă acces la toată galeria. Nu cerem acces la locație, contacte, microfon sau la fișierele telefonului.

7. Fotografiile clinice

Fotografiile făcute din aplicație se trimit direct în fișa pacientului, pe serverul cabinetului, și nu se salvează în galeria telefonului. Fotografierea pacientului în scop medical se face cu acordul acestuia, pe care cabinetul îl obține (de exemplu prin consimțământul pentru fotografii clinice din MedAdmin).

8. Notificările push

Notificările se trimit prin Firebase Cloud Messaging (Google) și au text generic, cu titlul „MedAdmin” și un mesaj ca „Agenda ta s-a actualizat.”, „Ai o sarcină nouă sau actualizată.” sau „Ai un rezultat nou de văzut.”, **fără numele pacientului, diagnostice sau alte date medicale**. Detaliile se văd în aplicație, după deblocare. Tokenul de notificări se șterge la deconectare și la revocarea dispozitivului.

9. Imagistica și analizele automate

Vizualizarea imaginilor (DICOM) din aplicație este **pentru documentare și comunicare**, nu pentru diagnostic. Analizele automate (de exemplu segmentarea dinților dintr-o tomografie) rulează pe serverele MedAdmin din UE, iar rezultatul este o **sugestie de confirmat de medic**. MedAdmin nu este dispozitiv medical.

10. Ștergerea contului

10.1. Din aplicație: **Profil → Solicită ștergerea contului**. Cererea ajunge la titularul cabinetului, ca sarcină cu termen de 7 zile, și se înregistrează la Sysqo. Contul îl dezactivează și îl șterge cabinetul, care este angajatorul sau partenerul tău contractual; dacă nu primești răspuns în 30 de zile, scrie-ne la gdpr@medadmin.ro și intervenim.

10.2. Rămân la cabinet, pentru că legea o cere: actele medicale semnate de tine, consultațiile, consimțămintele și jurnalul de acces, cu numele tău ca autor (Legea 46/2003, Legea 95/2006, normele de arhivare).

10.3. Pe telefon, deconectarea șterge imediat tokenul și datele locale.

11. Cât păstrăm datele

Datele pacienților: cât decide cabinetul, conform obligațiilor sale legale. Contul tău: cât te păstrează cabinetul ca utilizator și cel mult 30 de zile după încetarea contractului cabinetului. Jurnalele de securitate: 12 luni. Tokenurile de dispozitiv: până la deconectare sau revocare.

12. Cui transmitem datele

Furnizorilor noștri din [lista subîmpuțerniciților](#): Hetzner (găzduire, Germania), Google prin Firebase Cloud Messaging (notificări push, fără date medicale), Ploi (administrarea serverului). Datele nu se vând și nu se folosesc pentru publicitate.

13. Transferuri și securitate

Datele sunt găzduite în UE (Germania); transferul către Sysqo în Regatul Unit se bazează pe decizia de adecvare a Comisiei Europene. Google poate prelucra tokenul de notificări în SUA (Cadru UE-SUA privind confidențialitatea datelor sau clauze contractuale standard). Comunicarea se face doar prin HTTPS; aplicația aplică aceleași permisiuni ca platforma web și aceeași autentificare în doi pași.

14. Drepturile tale

Pentru datele contului tău poți cere acces, rectificare, ștergere, restricționare, portabilitate sau te poți opune prelucrării: la cabinet sau la gdpr@medadmin.ro. Plângeri: **ANSPDCP**, B-dul G-ral. Gheorghe Magheru 28-30, sector 1, București, www.dataprotection.ro; **ICO** (Regatul Unit), www.ico.org.uk.

15. Modificări

Publicăm fiecare versiune nouă la această adresă, cu versiune și dată, și o anunțăm în aplicație când schimbarea e importantă.