Confidențialitate: portalul și aplicația MedAdmin Pacient

MedAdmin · Versiunea 1.1 · în vigoare din 11 noiembrie 2026

Această politică se aplică portalului pacientului **pacient.medadmin.ro** și aplicației mobile **MedAdmin Pacient** (iOS și Android).

1. Rezumat pe scurt

- **Cine are datele tale medicale.** Fișa ta, programările, documentele, rezultatele și plățile rămân la **cabinetul** la care ești pacient. Cabinetul este operatorul lor și decide cât le păstrează.
- **Ce face MedAdmin.** Alucard Limited („Alucard”, „noi”) îți oferă un singur cont cu care vezi informațiile de la toate cabinetele care folosesc MedAdmin. Pentru **contul de portal** (telefon, email, dispozitive, legăturile cu cabinetele, preferințe) suntem **operator**. Pentru datele din fișe suntem doar **persoana împuternicită** a cabinetului.
- **Fără parolă, fără reclame.** Intri cu un cod primit prin SMS sau email. Nu afișăm reclame, nu urmărim ce faci în aplicație, nu vindem date.
- **Plăți.** Plătești pe pagina securizată Stripe a cabinetului; **noi nu vedem și nu păstrăm datele cardului**.
- **Ștergere oricând.** Din Profil → Șterge contul sau, fără aplicație, la pacient.medadmin.ro/sterge-contul. Contul se șterge imediat; fișele rămân la cabinete, pentru că legea le obligă să le păstreze.
- **Contact:** gdpr@medadmin.ro. Plângeri: ANSPDCP (România) sau PCPD (Hong Kong).

2. Cine suntem

2.1. Alucard Limited (denumirea înregistrată ALUCARD LIMITED), UBI 81569528, sediul social Unit B, 11/F, 23 Thomson Road, Wan Chai, Hong Kong (RAS China). Contact pentru protecția datelor: gdpr@medadmin.ro.

2.2. Reprezentantul în UE (art. 27 GDPR) și responsabilul cu protecția datelor sunt cei din Politica de confidențialitate a platformei, secțiunea 2.

3. Cine răspunde de ce (operatori)

Date	Operator	Rolul Alucard
Contul de portal: telefonul, emailul confirmat, limba, preferințele de notificare, dispozitivele conectate, notificările din portal, legăturile cu cabinetele, cererile de legare, dovada ștergerii	Alucard	operator
Datele din cabinet: fișa medicală, programările, documentele, rezultatele, consimțămintele, soldul, devizele și plățile	**fiecare cabinet**, pentru pacienții săi	persoană împuternicită (art. 28 GDPR), conform acordului cu cabinetul
Plata cu cardul	cabinetul (beneficiarul plății) și Stripe, pentru datele cardului	nu vedem datele cardului

3.1. Ce vezi în portal se citește în timp real din baza de date a cabinetului; nu copiem fișa ta într-o bază centrală. În baza centrală păstrăm doar contul și legăturile, plus un index cu amprente criptografice (HMAC) ale numărului de telefon și ale CNP-ului, din care datele nu pot fi citite înapoi, folosit doar ca să găsim fișele care îți aparțin.

3.2. Pentru drepturile tale asupra fișei medicale (copii, corecturi, ștergere în limitele legii), adresează-te cabinetului. Dacă ne scrii nouă, transmitem cererea cabinetului în 5 zile lucrătoare și te anunțăm.

4. Ce date prelucrăm pentru contul de portal, de ce și pe ce temei

Date	Scop	Temei
Numărul de telefon (obligatoriu); emailul, dacă îl adaugi și îl confirmi	autentificarea cu cod, legarea fișelor, comunicări despre cont	art. 6 alin. (1) lit. (b) GDPR, executarea contractului (Termenii portalului)
Codurile de autentificare (6 cifre, valabile 10 minute, cel mult 5 încercări)	autentificarea și confirmarea acțiunilor sensibile (de exemplu ștergerea contului)	art. 6 alin. (1) lit. (b) și (f), securitate
Ultimele 4 cifre ale CNP-ului sau data nașterii, introduse de tine la confirmarea unei potriviri sau la o cerere de legare (păstrate criptat)	verificarea că fișa găsită îți aparține ție sau unei persoane în grija ta	art. 6 alin. (1) lit. (b) și (f); pentru legătura cu fișa medicală, în numele cabinetului, art. 9 alin. (2) lit. (h)
Legăturile cu cabinetele (cabinetul, relația „eu” sau „în grija mea”, starea, sursa)	să vezi informațiile corecte de la fiecare cabinet	art. 6 alin. (1) lit. (b)
Dispozitivele conectate (numele, platforma, data ultimei folosiri), tokenurile de sesiune (păstrate doar ca hash) și tokenul de notificări push	menținerea sesiunii, deconectarea de la distanță, notificările	art. 6 alin. (1) lit. (b)
Preferințele de notificare (SMS, email, push) și notificările din portal	să primești doar ce ai ales	art. 6 alin. (1) lit. (b); pentru push, consimțământul dat în telefon (art. 6 alin. (1) lit. (a)), retras oricând din setări
Jurnale tehnice: IP, ora, acțiunea, erorile	securitate, prevenirea abuzurilor (limitarea încercărilor), investigarea incidentelor	art. 6 alin. (1) lit. (f)
Evenimente de utilizare fără date personale (de exemplu „plată începută”, „cont șters” și canalul)	statistici agregate de funcționare	art. 6 alin. (1) lit. (f)

4.1. Datele privind sănătatea pe care le vezi sau le trimiți prin portal (programări la un anumit medic, documente, răspunsuri la chestionare, consimțăminte semnate) sunt prelucrate în numele cabinetului, pe temeiul stabilit de cabinet, de regulă art. 9 alin. (2) lit. (h) GDPR (asistență medicală) și Legea 46/2003 a drepturilor pacientului.

4.2. Nu facem profilare, nu luăm decizii automate cu efecte juridice asupra ta și nu folosim datele pentru publicitate sau pentru antrenarea modelelor de inteligență artificială.

5. Persoanele în grija ta (copii și alți membri ai familiei)

5.1. Poți vedea în contul tău și persoanele pentru care cabinetul te-a trecut ca aparținător sau reprezentant (de exemplu copiii tăi): programări, documente, plăți. Legătura se face fie automat, după telefonul aparținătorului din fișă și confirmarea ultimelor 4 cifre ale CNP-ului sau a datei nașterii, fie la cererea ta, aprobată de cabinet.

5.2. Declari că ai dreptul legal să accesezi aceste informații (părinte, tutore, reprezentant legal sau persoană împuternicită de pacient). Cabinetul verifică această calitate conform Legii 46/2003 și poate șterge legătura oricând. Poți desface și tu legătura din Cabinetele mele.

5.3. **Minorii.** Contul de portal se creează pe numărul de telefon al unui adult. Minorii apar în contul părintelui sau al reprezentantului legal, ca persoane în grijă. Contul propriu se poate crea de la 18 ani. Legătura „în grija mea” se închide automat când persoana împlinește 18 ani, cu anunțarea ambelor părți; între 16 și 18 ani cabinetul poate restrânge ce vede părintele, după regulile confidențialității medicale.

6. Autentificarea prin SMS sau email

6.1. Codurile de autentificare se trimit prin SMS, prin furnizorul nostru SMSLink (România), sau pe emailul confirmat, prin Google Workspace. Mesajul conține doar codul și numele MedAdmin, fără date medicale.

6.2. Limităm numărul de coduri și de încercări (de exemplu cel mult 3 coduri în 10 minute pentru un număr și blocare de 15 minute după 5 coduri greșite), ca să împiedicăm ghicirea codurilor.

6.3. SMS-urile trimise de cabinete (confirmări, remindere) pleacă în numele cabinetului; le poți opri răspunzând STOP sau din preferințele portalului.

7. Notificările push

7.1. Aplicația îți cere permisiunea pentru notificări abia după ce îți explică la ce folosesc. Poți folosi aplicația și fără notificări.

7.2. Notificările se livrează prin Firebase Cloud Messaging (Google). Textul lor este generic, de exemplu „MedAdmin Pacient: Ai un document nou de la cabinet. Deschide aplicația ca să vezi detaliile.”: **nu conține numele cabinetului, diagnostice, rezultate sau alte date medicale**. Detaliile le vezi doar după ce deschizi aplicația.

7.3. Tokenul de notificări al telefonului se șterge când te deconectezi, când revoci dispozitivul sau când ștergi contul.

8. Plățile online

8.1. Dacă un cabinet a activat plata online, poți plăti din portal soldul, avansul unui plan de tratament acceptat sau o programare cu plată în avans. Plata se face pe pagina găzduită de **Stripe** pentru cabinet (Stripe Connect), deschisă în browser.

8.2. Datele cardului le introduci direct la Stripe. **MedAdmin nu primește, nu vede și nu stochează numărul cardului, data expirării sau codul CVV.** Primim doar rezultatul plății (suma, data, starea, referința), ca să o înregistrăm la cabinet.

8.3. Banii ajung direct în contul Stripe al cabinetului. Pentru datele de plată, Stripe acționează conform propriei politici de confidențialitate (stripe.com/privacy). Documentul fiscal îl emite cabinetul.

9. Datele de pe telefonul tău (aplicația MedAdmin Pacient)

9.1. Tokenurile de sesiune se păstrează în Keychain (iOS) sau Keystore (Android). Ca să meargă și fără internet, aplicația păstrează o copie locală a cabinetelor tale, a programărilor viitoare și a documentelor PDF pe care le-ai deschis, într-o bază de date **criptată** (AES-256, în modul SQLCipher), cu cheia în Keychain sau Keystore.

9.2. Copia locală este **exclusă din backup-ul iCloud și din backup-ul automat Android** și se șterge când te deconectezi, când sesiunea expiră sau când ștergi contul.

9.3. Deblocarea cu Face ID, Touch ID, amprentă sau PIN se face pe telefon. **Datele biometrice nu ajung la noi**; PIN-ul se păstrează doar ca amprentă criptografică, pe telefon.

9.4. **Permisiuni.** Aplicația cere doar acces la internet, notificări (opțional) și biometrie (opțional, pentru deblocare). Nu cere acces la locație, contacte, microfon, cameră sau galeria foto. Nu folosește identificatorul de publicitate, nu face tracking între aplicații și nu include instrumente de analiză ale terților.

9.5. Când partajezi un document din aplicație (foaia de partajare a telefonului), alegi tu destinatarul; de acolo, documentul nu mai este sub controlul nostru.

10. Exportul datelor

Din Profil → Exportă datele primești contul tău și, pentru fiecare cabinet, persoanele legate, programările și lista documentelor, în format JSON sau PDF. Exportul acoperă dreptul de acces și de portabilitate pentru datele din portal; copiile complete ale documentelor medicale le ceri cabinetului.

11. Ștergerea contului

11.1. **Din aplicație sau din portal:** Profil → Șterge contul, apoi confirmi cu codul primit prin SMS.

11.2. **Fără aplicație:** pe pacient.medadmin.ro/sterge-contul introduci numărul de telefon și codul primit prin SMS. Nu e nevoie să fii autentificat.

11.3. **Ce se șterge imediat:** contul, legăturile cu cabinetele, dispozitivele și tokenurile (inclusiv cele de notificări), notificările din portal, preferințele, codurile de autentificare. Pe telefon se șterg tokenurile și copia locală. Primești un SMS de confirmare.

11.4. **Ce rămâne:** fișele medicale, programările, documentele și plățile de la fiecare cabinet, pe care cabinetul este obligat să le păstreze (Legea 46/2003, Legea 95/2006 și normele de arhivare a documentelor medicale; legislația fiscală pentru plăți). Ca dovadă a ștergerii păstrăm o înregistrare minimă: identificatorul intern al contului, amprenta criptografică a telefonului, canalul, data și numărul de legături; o păstrăm 3 ani (termenul general de prescripție), apoi o ștergem.

12. Cât păstrăm datele contului

Date	Termen
Contul și legăturile	până ștergi contul; conturile fără nicio autentificare timp de 24 de luni se șterg automat, cu avertizare prin SMS cu 30 de zile înainte
Codurile de autentificare	expiră în 10 minute; înregistrările lor se șterg după cel mult 30 de zile
Sesiunile pe dispozitive	acces 60 de minute; reîmprospătarea expiră după 60 de zile fără folosire
Notificările din portal	12 luni
Jurnalele tehnice și de securitate	12 luni; jurnalele serverului 14 zile
Copiile de rezervă	se rotesc în 30 de zile

13. Cui transmitem datele contului

Furnizorilor noștri, cu contracte conforme art. 28 GDPR: Hetzner Online GmbH (găzduire, Germania), ASTINVEST COM SRL prin SMSLink (SMS, România), Google Ireland Limited prin Google Workspace (email) și Firebase Cloud Messaging (notificări push), Ploi B.V. (administrarea serverului, Țările de Jos), Stripe Payments Europe, Limited (plăți, Irlanda). Cabinetelor la care ești legat le transmitem acțiunile tale (programări, confirmări, cereri de legare, documentele descărcate). Autorităților, doar când legea o cere. Lista completă: Subîmputerniciți și găzduire.

14. Transferuri

Datele sunt găzduite în UE (Germania). Alucard are sediul în Hong Kong; accesul echipei noastre la date din afara UE se face pe baza clauzelor contractuale standard ale Comisiei Europene (Decizia (UE) 2021/914), încheiate cu fiecare cabinet prin Acordul de prelucrare a datelor, iar datele rămân stocate în UE. Google și Stripe pot prelucra date tehnice în SUA, pe baza Cadrului UE–SUA privind confidențialitatea datelor sau a clauzelor contractuale standard. Detalii în Politica de confidențialitate a platformei, secțiunea 7.

15. Securitate

Comunicare doar prin HTTPS; autentificare fără parolă, cu coduri de unică folosință și limitarea încercărilor; tokenuri de sesiune scurte, cu rotație și detectarea refolosirii; documentele se descarcă prin linkuri semnate, valabile 5 minute și legate de contul tău, iar fiecare descărcare apare în jurnalul de acces al cabinetului; paginile cu date personale nu se indexează și nu se păstrează în cache.

16. Drepturile tale

16.1. Pentru contul de portal ai drepturile din art. 15–22 GDPR: acces, rectificare (din Profil), ștergere (secțiunea 11), restricționare, portabilitate (secțiunea 10), opoziție, retragerea consimțământului pentru notificări. Scrie-ne la gdpr@medadmin.ro; răspundem în cel mult o lună.

16.2. Pentru fișa medicală, drepturile le exerciți la cabinet (secțiunea 3.2).

16.3. Plângeri: **ANSPDCP**, B-dul G-ral. Gheorghe Magheru 28-30, sector 1, București, www.dataprotection.ro; **PCPD** (Hong Kong), Room 1303, 13/F, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, Hong Kong, www.pcpd.org.hk.

17. Aviz medical

MedAdmin nu este dispozitiv medical și nu pune diagnostice. Imaginile și rezultatele din portal sunt pentru documentare și comunicare. Pentru orice decizie medicală, discută cu medicul tău.

18. Modificări

Publicăm fiecare versiune nouă la această adresă, cu versiune și dată. Schimbările importante le anunțăm în aplicație și în portal înainte să intre în vigoare.