# Acord de prelucrare a datelor (DPA)

MedAdmin · Versiunea 2.1 · în vigoare din 11 noiembrie 2026

## 1. Rezumat pe scurt

- **Cine e cine.** Cabinetul este **operatorul** datelor pacienților și ale personalului său. Alucard Limited este **persoana împuternicită**: prelucrează aceste date doar ca să furnizeze MedAdmin, la instrucțiunile cabinetului (art. 28 GDPR).
- **Unde.** Pe servere Hetzner din Germania (UE). Fiecare cabinet are baza lui de date.
- **Cine mai are acces.** Doar subîmputerniciții din Anexa 2. Orice schimbare se anunță cu 30 de zile înainte; cabinetul se poate opune și poate rezilia fără penalități.
- **Incidente.** Anunțăm cabinetul în cel mult 48 de ore de la constatare, ca acesta să poată notifica ANSPDCP în termenul de 72 de ore.
- **La final.** 30 de zile pentru export, apoi ștergere; copiile de rezervă se șterg prin rotație. Confirmăm ștergerea în scris, la cerere.

**Părțile**

1. **[denumirea cabinetului]**, CUI [CUI-ul cabinetului], cu sediul în [sediul cabinetului], email [emailul cabinetului], telefon [telefonul cabinetului], în calitate de **operator** („Operatorul”);
2. **Alucard Limited** (denumirea înregistrată ALUCARD LIMITED), UBI 81569528, cu sediul social în Unit B, 11/F, 23 Thomson Road, Wan Chai, Hong Kong (RAS China), email gdpr@medadmin.ro, în calitate de **persoană împuternicită** („Împuternicitul”).

Acordul se încheie prin acceptare electronică la înscriere sau la intrarea în vigoare a unei versiuni noi și face parte din Termenii și condițiile MedAdmin („Contractul principal”). Se înregistrează versiunea, data, ora, IP-ul și utilizatorul care a acceptat.

## 2. Definiții

Termenii „date cu caracter personal”, „prelucrare”, „operator”, „persoană împuternicită”, „persoană vizată”, „date privind sănătatea” și „încălcarea securității datelor cu caracter personal” au sensul din Regulamentul (UE) 2016/679 („GDPR”). „Subîmputernicit” înseamnă o altă persoană împuternicită angajată de Împuternicit conform art. 28 alin. (2) și (4) GDPR. „Serviciul” este MedAdmin, așa cum este descris în Contractul principal.

## 3. Obiectul și durata

3.1. Împuternicitul prelucrează date cu caracter personal în numele Operatorului, exclusiv pentru furnizarea Serviciului, așa cum este descris în Anexa 1.

3.2. Acordul durează cât Contractul principal, plus perioada de returnare și ștergere de la secțiunea 12.

## 4. Instrucțiunile Operatorului

4.1. Împuternicitul prelucrează datele numai pe baza instrucțiunilor documentate ale Operatorului, inclusiv în privința transferurilor, cu excepția cazului în care dreptul Uniunii sau al unui stat membru îl obligă; în acest caz îl informează pe Operator înainte de prelucrare, dacă legea permite.

4.2. Constituie instrucțiuni documentate: Contractul principal, acest Acord, configurările făcute de Operator în Serviciu și cererile scrise trimise prin tichet sau email. Exemple de configurări care sunt instrucțiuni: activarea SMS-urilor, a e-Factura,

a raportărilor CNAS, a portalului pacientului, a plăților online, a analizelor automate de imagistică, a aplicațiilor mobile și desktop, trimiterea unui document pe email.

4.3. **Portalul pacientului.** Când activează portalul pacientului, Operatorul instruiește Împuternicitul: (a) să întrețină un index central cu amprente criptografice (HMAC) ale telefonului pacientului, ale telefonului aparținătorului și ale CNP-ului, folosit doar pentru a lega fișele de contul de portal al pacientului; (b) să afișeze pacientului și persoanelor legate de el ca aparținători datele publicate de Operator în portal; (c) să înregistreze în jurnalul Operatorului acțiunile făcute din portal. Contul de portal al pacientului este o relație separată, în care Împuternicitul este operator (vezi Politica de confidențialitate a portalului).

4.4. Împuternicitul informează imediat Operatorul dacă o instrucțiune încalcă, în opinia sa, GDPR sau alte norme de protecție a datelor.

4.5. Operatorul răspunde de legalitatea prelucrării, de existența temeiului juridic, de informarea pacienților și de obținerea consimțămintelor acolo unde sunt necesare.

## 5. Confidențialitatea personalului

5.1. Împuternicitul se asigură că persoanele autorizate să prelucreze datele s-au angajat să respecte confidențialitatea sau au o obligație legală de confidențialitate.

5.2. Personalul Împuternicitului accesează datele Operatorului doar pentru suport la cererea Operatorului sau pentru gestionarea incidentelor, printr-o sesiune de suport care: este implicit doar în citire; cere un motiv; permite scrierea doar cu un motiv suplimentar și codul de autentificare în doi pași al operatorului de suport; se jurnalizează și este vizibilă pentru Operator.

## 6. Securitatea prelucrării

Împuternicitul aplică măsurile tehnice și organizatorice din Anexa 3, conform art. 32 GDPR. Le poate actualiza, fără a scădea nivelul general de protecție.

## 7. Subîmputerniciți

7.1. Operatorul acordă o autorizare generală scrisă pentru subîmputernicții din Anexa 2.

7.2. Împuternicitul anunță Operatorul pe email și în aplicație cu cel puțin 30 de zile înainte de adăugarea sau înlocuirea unui subîmputernicit. Operatorul poate formula obiecții motivate în acest termen. Dacă părțile nu găsesc o soluție, Operatorul poate rezilia Contractul principal fără penalități, cu rambursarea proporțională a perioadei plătite și neconsumate.

7.3. Împuternicitul impune subîmputernicților, prin contract, obligații de protecție a datelor cel puțin echivalente cu cele din acest Acord și rămâne pe deplin răspunzător față de Operator pentru îndeplinirea lor.

## 8. Transferuri

8.1. Datele Operatorului se găzduiesc în Spațiul Economic European (Germania).

8.2. Împuternicitul are sediul în Hong Kong (RAS China), teritoriu care nu face obiectul unei decizii de adecvare a Comisiei Europene. Datele rămân stocate în SEE; accesul de la distanță al personalului Împuternicitului din Hong Kong (suport, administrare) este un transfer în sensul capitolului V GDPR și se face în temeiul clauzelor contractuale standard adoptate prin Decizia de punere în aplicare (UE) 2021/914 a Comisiei, modulul doi (operator către persoană împuternicită), pe care părțile le încheie prin acceptarea acestui Acord, cu următoarele opțiuni: clauza 7 (aderare) inclusă; clauza 9 lit. (a), opțiunea

2 (autorizare generală, cu preavizul de 30 de zile din secțiunea 7); clauza 11 fără mecanismul opțional; clauza 13: ANSPDCP; clauza 17: legea română; clauza 18: instanțele din România. Anexa I a clauzelor standard este formată din părțile și descrierea prelucrării din Anexa 1 a acestui Acord, Anexa II din măsurile din Anexa 3, iar Anexa III din subîmputerniciții din Anexa 2. În caz de conflict, clauzele standard prevalează. Împuternicitul a evaluat impactul transferului și aplică măsuri suplimentare: datele nu se copiază în afara SEE, accesul este doar în citire, jurnalizat, cu autentificare în doi pași și prin conexiuni criptate (secțiunea 5.2 și Anexa 3).

8.3. Subîmputerniciții din grupuri cu societăți în SUA (Google, Stripe, GitHub) pot transfera date către SUA numai pe baza Cadrului UE–SUA privind confidențialitatea datelor (societăți certificate) sau a clauzelor contractuale standard adoptate de Comisia Europeană (art. 46 GDPR).

8.4. Datele privind sănătatea nu se transferă în afara SEE, cu o excepție aflată sub controlul Operatorului: documentele pe care Operatorul alege să le trimită pe email unui pacient trec prin Google Workspace (Anexa 2). Operatorul poate evita acest flux trimițând documentele prin portalul pacientului.

## 9. Asistență pentru drepturile persoanelor vizate

9.1. Serviciul pune la dispoziția Operatorului instrumente pentru drepturile pacienților: exportul dosarului (PDF și JSON), rectificarea, restricționarea, anonimizarea și ștergerea, cu respectarea termenelor de arhivare; jurnalul de acces la fișă; gestionarea consimțămintelor și a retragerii lor.

9.2. Dacă Împuternicitul primește direct o cerere de la o persoană vizată privind datele Operatorului, o transmite Operatorului în 5 zile lucrătoare și nu răspunde în fond fără instrucțiuni.

9.3. Pentru cererile pe care Operatorul nu le poate rezolva singur din Serviciu, Împuternicitul îl asistă în cel mult 10 zile lucrătoare.

## 10. Asistență pentru art. 32–36 GDPR

Împuternicitul asistă Operatorul, ținând seama de natura prelucrării și de informațiile disponibile, la asigurarea securității, la notificarea încălcărilor, la evaluările de impact (DPIA) și la consultarea prealabilă a ANSPDCP, prin furnizarea documentației tehnice disponibile (descrierea fluxurilor, a măsurilor din Anexa 3 și a subîmputerniciților).

## 11. Încălcarea securității datelor

11.1. Împuternicitul notifică Operatorul fără întârzieri nejustificate și în cel mult **48 de ore** de la momentul în care a luat cunoștință de o încălcare a securității datelor care afectează datele Operatorului, astfel încât Operatorul să poată respecta termenul de **72 de ore** față de ANSPDCP (art. 33 GDPR).

11.2. Notificarea cuprinde, în măsura în care sunt cunoscute: natura încălcării, categoriile și numărul aproximativ de persoane vizate și de înregistrări, consecințele probabile, măsurile luate sau propuse și persoana de contact. Informațiile care nu sunt disponibile de la început se transmit pe etape, fără întârzieri nejustificate.

11.3. Împuternicitul ia imediat măsurile necesare pentru limitarea efectelor, păstrează dovezile și documentează incidentul. Nu notifică ANSPDCP sau persoanele vizate în numele Operatorului fără instrucțiunea acestuia, cu excepția cazului în care legea o impune.

## 12. Returnarea și ștergerea datelor

12.1. La încetarea Contractului principal, Operatorul poate exporta datele timp de 30 de zile (PDF și JSON, plus fișierele încărcate). La cerere, în același termen, Împuternicitul furnizează o arhivă completă a bazei de date a Operatorului.

12.2. După acest termen, Împuternicitul șterge baza de date a Operatorului și fișierele din stocare. Copiile de rezervă de pe server se șterg prin rotație în cel mult 30 de zile; cele din stocarea externă, dacă este activată, conform Anexei 3. La cerere, Împuternicitul confirmă ștergerea în scris.

12.3. Împuternicitul poate păstra datele doar dacă legea îl obligă și numai în măsura acestei obligații.

12.4. Datele locale de pe stațiile, telefoanele și tabletele Operatorului (aplicația desktop, agentul, aplicațiile mobile) se șterg la deconectarea dispozitivului sau la dezinstalare; Operatorul este responsabil să deconecteze dispozitivele înainte de încetare.

## 13. Audit

13.1. Împuternicitul pune la dispoziția Operatorului informațiile necesare pentru a demonstra respectarea art. 28 GDPR: acest Acord, descrierea măsurilor din Anexa 3, lista subîmputerniciților și rapoartele de audit sau certificările publice ale acestora.

13.2. Operatorul poate efectua un audit, direct sau prin auditor independent obligat la confidențialitate, cel mult o dată pe an (și oricând după o încălcare a securității care îl afectează), cu notificare de 30 de zile, în timpul programului de lucru, fără a afecta securitatea sau datele altor clienți. Auditul se face, de regulă, documentar și la distanță. Costurile sunt ale Operatorului, cu excepția cazului în care auditul constată o încălcare semnificativă imputabilă Împuternicitului.

## 14. Răspundere

Răspunderea părților se stabilește conform art. 82 GDPR și Contractului principal. Limitarea răspunderii din Contractul principal nu se aplică încălcărilor intenționate sau din culpă gravă ale acestui Acord.

## 15. Dispoziții finale

15.1. În caz de conflict între acest Acord și Contractul principal, prevalează Acordul în privința protecției datelor.

15.2. Acordul este guvernat de aceeași lege ca și Contractul principal.

## Anexa 1. Descrierea prelucrării

| Element | Conținut |
|---|---|
| Natura prelucrării | găzduire, stocare, organizare, structurare, consultare, afișare în platformă, în portalul pacientului și în aplicații, transmitere la cererea Operatorului (SMS, email, notificări push, e-Factura către ANAF, raportări către CNAS, bon fiscal prin agentul local, plăți prin Stripe Connect), analize automate de imagistică la cererea Operatorului, copii de rezervă, export, ștergere |
| Scopul | furnizarea Serviciului: programări, evidența pacienților, fișa medicală, consultații, documente și consimțăminte, imagistică, încasări și documente fiscale, raportări CNAS, comunicări cu pacienții, portalul pacientului, rapoarte |
| Durata | pe durata Contractului principal, plus 30 de zile pentru export și termenul de rotație a copiilor de rezervă |
| Persoane vizate | pacienții Operatorului și aparținătorii sau reprezentanții lor legali (inclusiv părinții minorilor); personalul Operatorului (medici, asistenți, recepție, contabil, colaboratori); persoanele de contact ale furnizorilor și ale clienților persoane juridice ai Operatorului |

| Element | Conținut |
|---|---|
| Categorii de date | identificare (nume, prenume, CNP, data nașterii, sex, act de identitate, dacă este introdus); contact (telefon, email, adresă); date administrative (programări, istoricul vizitelor, plăți, devize, facturi, bonuri); date de asigurare (calitatea de asigurat, casa de asigurări, datele cardului național de sănătate citite la consultație); comunicări (SMS, email, notificări, răspunsurile la linkurile de confirmare și la chestionare); date tehnice ale pacientului care folosește un link sau portalul (IP, ora, browserul); date ale personalului (nume, specializare, cod de parafă, program, jurnale de acces) |
| Categorii speciale | date privind sănătatea (anamneză, diagnostice, tratamente, alergii, medicație, rezultate, imagini clinice și DICOM, chestionare, consimțăminte medicale) și, în funcție de specialitate, date privind viața sexuală (de exemplu ginecologie, urologie) sau date din consiliere psihologică, introduse de Operator |
| Frecvență | continuă, pe durata Contractului |
| Locul prelucrării | Germania (Hetzner, Falkenstein); România (SMSLink); Irlanda și, pentru date tehnice, SUA (Google, Stripe), conform Anexei 2; pe dispozitivele Operatorului, pentru copiile locale criptate ale aplicațiilor |

## Anexa 2. Subîmputerniciți autorizați

Lista publică actualizată: Subîmputerniciți și găzduire.

| Subîmputernicit | Locul datelor | Scop | Date ale Operatorului | Garanții |
|---|---|---|---|---|
| Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germania | Germania (centrul de date Falkenstein) | găzduirea serverelor, a bazelor de date, a fișierelor, a copiilor de rezervă; opțional, stocare de obiecte (Object Storage) pentru imagistică și copii de rezervă externe | toate categoriile din Anexa 1 | acord de prelucrare conform art. 28 GDPR; date în UE; centre de date certificate ISO/IEC 27001 |
| Ploi B.V., Țările de Jos | Țările de Jos (panoul de administrare); datele rămân pe serverele Hetzner | administrarea serverului: implementarea versiunilor, certificate TLS, procese, sarcini programate | nu stochează datele Operatorului; are acces tehnic de administrare la server | acord de prelucrare conform art. 28 GDPR; date în UE |
| ASTINVEST COM SRL, CUI 9250710, prin platforma SMSLink, România | România | trimiterea SMS-urilor către pacienți (confirmări, remindere, linkuri, coduri de autentificare) și primirea răspunsurilor | număr de telefon; conținutul SMS-ului (prenume, data și ora, numele cabinetului, link sau cod), fără date medicale | contract cu clauze art. 28 GDPR; date în România |
| Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irlanda (Google Workspace) | Irlanda / UE; posibil SUA | trimiterea emailurilor tranzacționale: invitații, coduri, notificări și documentele PDF pe care Operatorul alege să le trimită pe email | adresă de email, nume, conținutul mesajului și, la cererea Operatorului, documentul atașat | Cloud Data Processing Addendum Google; clauze contractuale standard; Cadrul UE–SUA |
| Google Ireland Limited (Firebase Cloud Messaging) | Irlanda / UE; posibil SUA | livrarea notificărilor push către aplicațiile MedAdmin Doctor și MedAdmin Pacient | tokenul de notificări al dispozitivului; text generic, fără date medicale | Firebase Data Processing and Security Terms; clauze contractuale standard; Cadrul UE–SUA |

| Subîmputernicit | Locul datelor | Scop | Date ale Operatorului | Garanții |
|---|---|---|---|---|
| Stripe Payments Europe, Limited, 1 Grand Canal Street Lower, Dublin 2, Irlanda | Irlanda / UE; posibil SUA | pentru plățile pacienților (Stripe Connect): crearea sesiunii de plată în contul Stripe al Operatorului | suma, descrierea plății, referința internă; datele cardului le introduce pacientul direct la Stripe | Stripe Data Processing Agreement; Cadrul UE–SUA și clauze contractuale standard. Pentru datele de plată, Stripe contractează direct cu Operatorul |
| GitHub B.V. / GitHub, Inc. | UE / SUA | găzduirea codului sursă și distribuirea fișierelor de instalare ale aplicației desktop | niciuna (nu primește date ale Operatorului) | listat pentru transparență |

Destinatari care nu sunt subîmputerniciți: ANAF (e-Factura) și casele de asigurări de sănătate (SIUI), cărora Serviciul le transmite date doar la instrucțiunea Operatorului, ca autorități în fața cărora Operatorul are obligații proprii.

Furnizori inactivi azi, care se adaugă doar cu notificarea de 30 de zile de la secțiunea 7.2: un serviciu de raportare a erorilor (Sentry, configurat fără date personale) și un serviciu de facturare (SmartBill), care ar prelucra doar date de facturare ale Operatorului.

## Anexa 3. Măsuri tehnice și organizatorice

**Izolarea datelor**

- Bază de date separată pentru fiecare cabinet; aplicația deschide la fiecare cerere doar baza cabinetului autentificat.
- Fișierele fiecărui cabinet stau într-un director propriu, nepublic; descărcarea se face doar prin aplicație, după verificarea permisiunii, sau prin linkuri semnate cu durată scurtă.
- Copiile de rezervă se pot restaura individual, pe cabinet.
- Portalul pacientului: în baza centrală stau doar contul, legăturile și amprentele HMAC; datele medicale se citesc din baza cabinetului la fiecare cerere, doar pentru legăturile active.

**Criptare**

- În tranzit: HTTPS (TLS) pentru tot traficul, cu HSTS; aplicațiile mobile și desktop comunică doar prin HTTPS.
- În repaus, la nivel de câmp: CNP-ul, alergiile, bolile cronice, medicația și secretele integrărilor (de exemplu tokenurile ANAF) sunt criptate cu cheia aplicației (AES-256), păstrată separat de baza de date; căutarea după CNP se face printr-o amprentă HMAC per cabinet.
- Copiile de rezervă: arhive criptate AES-256 cu o frază-cheie păstrată separat de server.
- Parolele: doar hash (bcrypt); PIN-urile: doar hash.
- Pe dispozitive: aplicațiile mobile păstrează datele offline într-o bază criptată AES-256 (SQLCipher), cu cheia în Keychain sau Keystore, exclusă din backup; tokenurile agentului desktop sunt protejate cu DPAPI (Windows), iar ale aplicației desktop în Windows Credential Manager sau Keychain.
- Discul serverului nu este criptat integral; protecția în repaus se asigură prin criptarea la nivel de câmp a datelor sensibile și a copiilor de rezervă, iar centrul de date (Hetzner, Germania, certificat ISO 27001) controlează fizic accesul la echipamente.

**Controlul accesului**

- Roluri și permisiuni per cabinet (titular, administrator, medic, asistent, recepție, contabil), după principiul privilegiului minim; notele confidențiale (de exemplu în psihologie) sunt vizibile doar autorului.

- Autentificare în doi pași (TOTP) obligatorie pentru titulari, administratori și echipa Împuternicitului; titularul o poate impune întregii echipe; coduri de rezervă; dispozitiv de încredere cel mult 30 de zile.
- Limitarea încercărilor: 5 încercări greșite pe cont și IP blochează 15 minute, cu alertă pe email către titulari.
- Blocarea ecranului după inactivitate (implicit 15 minute), cu deblocare prin PIN sau parolă; sesiuni cu expirare, închidere individuală și „deconectează-mă de peste tot”.
- Dispozitivele mobile și stațiile desktop au tokenuri individuale, revocabile din platformă; revocarea șterge datele locale la următoarea conexiune.
- Accesul personalului Împuternicitului: sesiune de suport doar în citire, cu motiv, jurnalizată (secțiunea 5.2); accesul la servere doar cu chei SSH nominale și prin panoul de administrare protejat cu autentificare în doi pași.

**Jurnalizare și monitorizare**

- Jurnal de acces la fișa pacientului (cine, ce, când, de unde), inclusiv descărcările din portal și din aplicații, consultabil de Operator.
- Jurnal de autentificări, blocări, exporturi, ștergeri, modificări de permisiuni și sesiuni de suport.
- Monitorizarea disponibilității și a sarcinilor programate (verificare la fiecare minut), cu alerte.
- Jurnalele tehnice ale serverului se păstrează 14 zile; jurnalele de activitate, 12 luni.

**Disponibilitate și reziliență**

- Copii de rezervă zilnice (ora 03:00), complete, ale bazei centrale, ale tuturor bazelor cabinetelor și ale fișierelor, criptate, păstrate 30 de zile.
- Copie externă opțională în stocare de obiecte în UE (Hetzner Object Storage), în alt centru de date, cu regulă de ciclu de viață de cel mult 35 de zile.
- Restaurare pe cabinet, cu salvarea prealabilă a stării curente; test de restaurare recomandat lunar.
- Implementare fără întrerupere și revenire rapidă la versiunea anterioară.

**Minimizare și păstrare**

- SMS-urile și notificările push nu conțin date medicale; linkurile trimise pacienților sunt semnate, expiră și, unde e cazul, cer un cod de verificare.
- Paginile publice ale cabinetului și portalul nu folosesc cookie-uri de urmărire; statistica de utilizare nu conține date personale.
- Analizele automate de imagistică rulează pe serverele Împuternicitului, fără transmiterea imaginilor către terți; datele Operatorului nu se folosesc pentru antrenarea modelelor.
- Raportarea erorilor, dacă este activată, nu trimite date personale.
- Mediile de dezvoltare și demonstrație folosesc doar date fictive.
- Exporturile urcate pentru migrarea din alt soft se șterg automat la 30 de zile după finalizarea sau anularea migrării.

**Măsuri organizatorice**

- Angajamente de confidențialitate pentru personal și colaboratori.
- Procedură documentată de gestionare a incidentelor și a încălcărilor de securitate.
- Evaluarea furnizorilor înainte de contractare și revizuirea anuală a listei de subîmputerniciți.
- Dezvoltare securizată: revizie de cod, teste automate, dependențe actualizate.
- Instruirea personalului privind protecția datelor la începutul colaborării și cel puțin o dată pe an; exercițiu anual de răspuns la incident, documentat.