Privacy: patient portal and MedAdmin Pacient app

MedAdmin · Version 1.1 · effective from 11 November 2026

This policy applies to the patient portal **pacient.medadmin.ro** and to the **MedAdmin Pacient** mobile app (iOS and Android).

1. Summary

- **Who holds your medical data.** Your record, appointments, documents, results and payments stay with the **practice** where you are a patient. The practice is their controller and decides how long they are kept.
- **What MedAdmin does.** Alucard Limited ("Alucard", "we", "us") gives you a single account with which you can see the information from all practices that use MedAdmin. For the **portal account** (phone, email, devices, links with practices, preferences) we are the **controller**. For the data in the records we are only the practice's **processor**.
- **No password, no advertising.** You sign in with a code received by SMS or email. We do not display advertising, we do not track what you do in the app and we do not sell data.
- **Payments.** You pay on the practice's secure Stripe page; **we do not see or keep your card details**.
- **Deletion at any time.** From Profil → Șterge contul (Profile → Delete account) or, without the app, at pacient.medadmin.ro/sterge-contul. The account is deleted immediately; the records stay with the practices, because the law requires them to keep them.
- **Contact:** gdpr@medadmin.ro. Complaints: ANSPDCP (Romania) or the PCPD (Hong Kong).

2. Who we are

2.1. 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. The EU representative (Article 27 GDPR) and the Data Protection Officer are those indicated in the platform Privacy Policy, section 2.

3. Who is responsible for what (controllers)

Data	Controller	Alucard's role
Portal account: phone, confirmed email, language, notification preferences, connected devices, portal notifications, links with practices, link requests, proof of deletion	Alucard	controller
Practice data: medical record, appointments, documents, results, consents, balance, estimates and payments	**each practice**, for its own patients	processor (Article 28 GDPR), under the agreement with the practice
Card payment	the practice (payee) and Stripe, for card data	we do not see card data

3.1. What you see in the portal is read in real time from the practice's database; we do not copy your record into a central database. In the central database we keep only the account and the links, plus an index of cryptographic fingerprints (HMAC) of the phone number and of the personal identification number (CNP), from which the data cannot be read back, used only to find the records that belong to you.

3.2. For your rights concerning the medical record (copies, corrections, erasure within the limits of the law), contact the practice. If you write to us, we forward the request to the practice within 5 working days and let you know.

4. What data we process for the portal account, why and on what legal basis

Data	Purpose	Legal basis
Phone number (mandatory); email, if you add and confirm it	sign-in with a code, linking records, account communications	Article 6(1)(b) GDPR, performance of the contract (Portal terms)
Authentication codes (6 digits, valid for 10 minutes, at most 5 attempts)	sign-in and confirmation of sensitive actions (for example deleting the account)	Article 6(1)(b) and (f), security
The last 4 digits of the personal identification number (CNP) or the date of birth, entered by you when confirming a match or making a link request (stored encrypted)	checking that the record found belongs to you or to a person in your care	Article 6(1)(b) and (f); for the link with the medical record, on behalf of the practice, Article 9(2)(h)
Links with practices (practice, relationship "me" or "in my care", status, source)	showing you the correct information from each practice	Article 6(1)(b)
Connected devices (name, platform, date of last use), session tokens (stored only as a hash) and the push notification token	maintaining the session, remote sign-out, notifications	Article 6(1)(b)
Notification preferences (SMS, email, push) and portal notifications	sending you only what you have chosen	Article 6(1)(b); for push, the consent given on the phone (Article 6(1)(a)), which can be withdrawn at any time in the settings
Technical logs: IP, time, action, errors	security, abuse prevention (attempt limiting), incident investigation	Article 6(1)(f)
Usage events without personal data (for example "payment started", "account deleted" and the channel)	aggregated operating statistics	Article 6(1)(f)

4.1. The health data that you see or send through the portal (appointments with a particular doctor, documents, questionnaire answers, signed consents) is processed on behalf of the practice, on the legal basis determined by the practice, usually Article 9(2)(h) GDPR (healthcare) and Law 46/2003 on patients' rights.

4.2. We do not carry out profiling, we do not take automated decisions with legal effects concerning you and we do not use the data for advertising or to train artificial intelligence models.

5. Persons in your care (children and other family members)

5.1. Your account may also show the persons for whom the practice has registered you as next of kin or representative (for example your children): appointments, documents, payments. The link is made either automatically, based on the next-of-kin phone number in the record and confirmation of the last 4 digits of the personal identification number (CNP) or of the date of birth, or at your request, approved by the practice.

5.2. You declare that you have the legal right to access this information (parent, guardian, legal representative or person authorised by the patient). The practice verifies this capacity in accordance with Law 46/2003 and may remove the link at any time. You can also remove the link yourself from Cabinetele mele (My practices).

5.3. **Minors.** A portal account is created on an adult's phone number. Minors appear in the account of the parent or legal representative, as persons in care. An own account can be created from the age of 18. The "in my care" link closes automatically when the person turns 18, with both parties notified; between 16 and 18 the practice may restrict what the parent sees, under the rules of medical confidentiality.

6. Signing in by SMS or email

6.1. Authentication codes are sent by SMS, through our provider SMSLink (Romania), or to the confirmed email address, through Google Workspace. The message contains only the code and the MedAdmin name, with no medical data.

6.2. We limit the number of codes and attempts (for example at most 3 codes in 10 minutes per number and a 15-minute lockout after 5 incorrect codes), to prevent codes being guessed.

6.3. SMS messages sent by practices (confirmations, reminders) are sent on behalf of the practice; you can stop them by replying STOP or from the portal preferences.

7. Push notifications

7.1. The app asks for permission to send notifications only after explaining what they are for. You can use the app without notifications.

7.2. Notifications are delivered through Firebase Cloud Messaging (Google). Their text is generic, for example "MedAdmin Pacient: Ai un document nou de la cabinet. Deschide aplicația ca să vezi detaliile." ("You have a new document from the practice. Open the app to see the details."): **it does not contain the name of the practice, diagnoses, results or other medical data**. You see the details only after opening the app.

7.3. The phone's notification token is deleted when you sign out, when you revoke the device or when you delete the account.

8. Online payments

8.1. If a practice has enabled online payment, you can pay from the portal the balance, the deposit for an accepted treatment plan or an appointment that requires advance payment. Payment takes place on the page hosted by **Stripe** for the practice (Stripe Connect), opened in the browser.

8.2. You enter your card details directly with Stripe. **MedAdmin does not receive, see or store the card number, expiry date or CVV code.** We receive only the payment result (amount, date, status, reference), in order to record it at the practice.

8.3. The money goes directly to the practice's Stripe account. For payment data, Stripe acts under its own privacy policy (stripe.com/privacy). The tax receipt or invoice is issued by the practice.

9. Data on your phone (the MedAdmin Pacient app)

9.1. Session tokens are kept in the Keychain (iOS) or Keystore (Android). To work offline as well, the app keeps a local copy of your practices, your upcoming appointments and the PDF documents you have opened, in an **encrypted** database (AES-256, in SQLCipher mode), with the key in the Keychain or Keystore.

9.2. The local copy is **excluded from iCloud backup and from Android automatic backup** and is deleted when you sign out, when the session expires or when you delete the account.

9.3. Unlocking with Face ID, Touch ID, fingerprint or PIN takes place on the phone. **Biometric data never reaches us**; the PIN is stored only as a cryptographic fingerprint, on the phone.

9.4. **Permissions.** The app asks only for internet access, notifications (optional) and biometrics (optional, for unlocking). It does not ask for access to location, contacts, microphone, camera or photo library. It does not use the advertising identifier, does not track across apps and does not include third-party analytics tools.

9.5. When you share a document from the app (the phone's share sheet), you choose the recipient; from that point the document is no longer under our control.

10. Data export

From Profil → Exportă datele (Profile → Export data) you receive your account and, for each practice, the linked persons, the appointments and the list of documents, in JSON or PDF format. The export covers the right of access and the right to data portability for the portal data; you request full copies of medical documents from the practice.

11. Deleting the account

11.1. **From the app or the portal:** Profil → Șterge contul (Profile → Delete account), then confirm with the code received by SMS.

11.2. **Without the app:** at pacient.medadmin.ro/sterge-contul enter your phone number and the code received by SMS. You do not need to be signed in.

11.3. **What is deleted immediately:** the account, the links with practices, the devices and tokens (including notification tokens), the portal notifications, the preferences, the authentication codes. On the phone, the tokens and the local copy are deleted. You receive a confirmation SMS.

11.4. **What remains:** the medical records, appointments, documents and payments held by each practice, which the practice is required to keep (Law 46/2003 on patients' rights, Law 95/2006 on healthcare reform and the rules on archiving medical documents; tax legislation for payments). As proof of deletion we keep a minimal record: the internal account identifier, the cryptographic fingerprint of the phone number, the channel, the date and the number of links; we keep it for 3 years (the general limitation period), then delete it.

12. How long we keep account data

Data	Period
Account and links	until you delete the account; accounts with no sign-in for 24 months are deleted automatically, with an SMS warning 30 days beforehand
Authentication codes	expire after 10 minutes; their records are deleted after 30 days at most
Device sessions	access 60 minutes; the refresh expires after 60 days without use
Portal notifications	12 months
Technical and security logs	12 months; server logs 14 days
Backups	rotated within 30 days

13. To whom we disclose account data

To our suppliers, under contracts compliant with Article 28 GDPR: Hetzner Online GmbH (hosting, Germany), ASTINVEST COM SRL through SMSLink (SMS, Romania), Google Ireland Limited through Google Workspace (email) and Firebase Cloud Messaging (push notifications), Ploi B.V. (server administration, Netherlands), Stripe Payments Europe, Limited (payments, Ireland). To the practices you are linked with we pass on your actions (appointments, confirmations, link requests, downloaded documents). To authorities, only where the law requires. Full list: Sub-processors and hosting.

14. Transfers

The data is hosted in the EU (Germany). Alucard has its registered office in Hong Kong; access to the data by our team from outside the EU relies on the European Commission's standard contractual clauses (Decision (EU) 2021/914), concluded with each practice through the Data Processing Agreement, and the data remains stored in the EU. Google and Stripe may process technical data in the USA, on the basis of the EU–US Data Privacy Framework or standard contractual clauses. Details in the platform Privacy Policy, section 7.

15. Security

Communication over HTTPS only; passwordless sign-in, with one-time codes and attempt limiting; short-lived session tokens, with rotation and reuse detection; documents are downloaded through signed links, valid for 5 minutes and bound to your account, and every download appears in the practice's access log; pages containing personal data are not indexed and are not cached.

16. Your rights

16.1. For the portal account you have the rights under Articles 15–22 GDPR: access, rectification (from Profil (Profile)), erasure (section 11), restriction, portability (section 10), objection, withdrawal of consent for notifications. Write to us at gdpr@medadmin.ro; we respond within one month at the latest.

16.2. For the medical record, you exercise your rights with the practice (section 3.2).

16.3. 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), Room 1303, 13/F, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, Hong Kong, www.pcpd.org.hk.

17. Medical notice

MedAdmin is not a medical device and does not diagnose. The images and results in the portal are for documentation and communication. For any medical decision, talk to your doctor.

18. Changes

We publish each new version at this address, with a version and date. We announce important changes in the app and in the portal before they take effect.