Privacy policy

MedAdmin · Version 2.1 · effective from 11 November 2026

1. Summary

- **Who we are.** MedAdmin is practice management software for medical practices, operated by Alucard Limited, a company incorporated in Hong Kong, SAR China (UBI 81569528).
- **Two roles.** For the data of our client practices, their users and the visitors of our website we are the **controller**. For the data of patients and staff that practices enter into MedAdmin we are a **processor**: the controller is the practice. Patients will find the information that concerns them in the privacy policy of the patient portal and the MedAdmin Pacient app and in the practice's information notice.
- **Where the data is stored.** On Hetzner servers in Germany (European Union), with encrypted daily backups.
- **What we do not do.** We do not sell data, we do not display advertising, we do not use tracking cookies, we do not use patient data for our own purposes and we do not use it to train artificial intelligence models.
- **Your rights.** Access, rectification, erasure, restriction, portability, objection. Write to us at gdpr@medadmin.ro. You may lodge a complaint with ANSPDCP (Romania) or with the PCPD (Hong Kong).

2. Who we are and how to contact us

2.1. The controller of the data described in section 4 is Alucard Limited (registered name ALUCARD LIMITED), a private limited company registered with the Companies Registry of Hong Kong (SAR China), registration number (UBI) 81569528, with its registered office at Unit B, 11/F, 23 Thomson Road, Wan Chai, Hong Kong SAR China ("Alucard", "we", "us").

2.2. Data protection contact: gdpr@medadmin.ro. Postal correspondence: the registered office address above.

2.3. We have no establishment in the European Union. Requests from data subjects and from supervisory authorities in the Union are addressed directly to us, at gdpr@medadmin.ro, in Romanian or English, and are answered within the time limits of the GDPR. If we appoint a representative in the Union (Article 27 GDPR), we publish it in this section.

2.4. Data protection is coordinated by the company's management; the dedicated contact is gdpr@medadmin.ro, marked "Data protection". If we appoint a data protection officer (Article 37 GDPR), we publish their contact details here and notify them to ANSPDCP.

3. What MedAdmin is and to whom this policy applies

3.1. MedAdmin comprises: the practices' web platform (each practice's subdomain on medadmin.ro), the presentation website medadmin.ro, the patient portal pacient.medadmin.ro, the mobile apps MedAdmin Doctor and MedAdmin Pacient, the MedAdmin desktop application and the MedAdmin Fiscal local agent.

3.2. This policy applies to:

- persons who visit medadmin.ro or write to us (contact form, demo, waiting list, email);
- contact persons of client practices and their users (owner, doctors, nurses, reception, accountant), for the data of their own account;
- representatives and contact persons of our suppliers and partners.

3.3. It does not apply to the data that a practice processes about its patients. For that data the controller is the practice, and we process it only on the practice's instructions, under the Data Processing Agreement. Patients who use the portal or

the MedAdmin Pacient app have a separate policy, and users of the MedAdmin Doctor app another one.

4. What data we process as controller, why, on what legal basis and for how long

Category	Examples	Purpose	Legal basis (GDPR)	Retention
User account data	name, email, phone, role, practice, password (hash only), two-factor authentication settings, PIN code (hash)	creating the account, authentication, access management	Art. 6(1)(b), performance of the contract with the practice; for users who are not parties to the contract: Art. 6(1)(f), the legitimate interest in providing the service contracted by the practice	for the duration of the practice's contract and 30 days after termination (section 9)
Practice billing data	name, tax identification number (CUI), registered office, billing email, plan, payment history, invoices	invoicing, accounting records, debt recovery	Art. 6(1)(b) and (c); accounting and tax legislation of Hong Kong (Companies Ordinance, Cap. 622; Inland Revenue Ordinance, Cap. 112) and, where applicable, of Romania	7 years from the end of the financial year
Payment data	card type and last 4 digits, payment status; **full card details never reach us**, they are processed by Stripe	collecting the subscription and SMS bundle payments	Art. 6(1)(b)	as billing data
Acceptance of legal documents	the document, version, date and time, IP address, browser, user	proof of conclusion of the contract and of the Data Processing Agreement	Art. 6(1)(c) and (f)	for the duration of the contract and 6 years after termination (the general limitation period in England and Wales)
Support	tickets, emails, attachments, team notes	answering requests, history of issues	Art. 6(1)(b)	3 years from closing the ticket
Security logs	successful and failed logins, IP, browser, lockouts, support sessions with their reason, exports, permission changes	security of the service, incident investigation, proof of access	Art. 6(1)(f) and Art. 32 GDPR	12 months; technical server logs 14 days
Platform usage data	product events: page pattern (without parameters), feature used, role, practice; **no name, phone, email, personal identification number (CNP) or free text**	measuring feature usage, proactive support, product improvement	Art. 6(1)(f)	13 months in raw form, then only non-identifying aggregates
Website forms	name, email, phone, practice, speciality, message, visit source (utm parameters)	answering the request, the demo, notification when an edition launches	Art. 6(1)(b), pre-contractual steps; for the waiting list, Art. 6(1)(a), consent	12 months from the last contact, if you do not become a client
Product emails	news about features, usage tips	informing clients	legitimate interest for existing clients, with an unsubscribe link in every message (Art. 12(2) of Law 506/2004 on electronic communications)	until you unsubscribe

Category	Examples	Purpose	Legal basis (GDPR)	Retention
Desktop application and agent	installation identifier, version, operating system, connection status, update errors, technical counters	automatic updates, diagnostics, workstation security	Art. 6(1)(b) and (f)	12 months from the workstation's last connection

We send product emails only to existing clients, to the account addresses, only about MedAdmin, with one-click unsubscribe in every message. We do not send campaigns to persons who are not clients without their consent.

4.1. We do not take decisions based solely on automated processing that produce legal effects concerning you, and we do not carry out marketing profiling. The internal score of a practice's product usage serves only to offer help and does not lead to any automated decision.

4.2. Without the data marked as mandatory at sign-up we cannot create the account.

5. Data of patients and practice staff (our role as processor)

5.1. The practice decides what data it enters about patients, why and for how long it keeps it. We host and process it only to provide the service, on the practice's instructions, under the Data Processing Agreement (Article 28 GDPR).

5.2. Each practice has its own database, separate from the others. Health data is a special category (Article 9 GDPR) and receives the protection measures in Annex 3 to the Agreement.

5.3. We do not use patient data for our own purposes, we do not sell it, we do not use it for advertising and we do not train artificial intelligence models on it. Automated imaging analyses (for example tooth segmentation from a CT scan) run on our servers in the EU, only at the practice's request, and the result is a suggestion that the doctor checks.

5.4. Alucard staff access a practice's data only for support, at the practice's request, or to handle an incident. Access takes place through a support session that is read-only by default, requires a reason, is logged and is visible to the practice.

6. To whom we disclose data

6.1. To suppliers who help us provide the service, under contracts compliant with Article 28 GDPR:

Supplier	What it does	Where
Hetzner Online GmbH	hosting of servers, databases, files and backups; optionally, object storage	Germany (Falkenstein), EU
Stripe Payments Europe, Limited	payment of subscriptions and SMS bundles; through Stripe Connect, patient payments directly to practices	Ireland, EU; the Stripe group may access data from the USA
ASTINVEST COM SRL (SMSLink)	sending SMS messages: authentication codes, confirmations and reminders	Romania, EU
Google Ireland Limited (Google Workspace)	sending transactional emails and our correspondence	Ireland, EU; the Google group may process data in the USA
Google Ireland Limited (Firebase Cloud Messaging)	delivering push notifications to the mobile apps	Ireland, EU; the Google group may process data in the USA
Ploi B.V.	server administration (deployments, certificates, processes)	Netherlands, EU
GitHub B.V. and GitHub, Inc.	hosting the source code and distributing the desktop application installers; receives no patient data	EU and USA

The full list, with the purpose and safeguards of each: Sub-processors and hosting.

6.2. To authorities, where the law requires us to (courts, criminal investigation bodies, tax authorities), only to the extent of the request.

6.3. To our advisers (accountant, lawyer, auditor), who are bound by confidentiality.

6.4. To a possible buyer or successor, in the event of a reorganisation or sale of the business, with prior notice to clients and with the same safeguards.

7. International transfers

7.1. Alucard is established in Hong Kong (SAR China), and the data is hosted in the European Union (Germany). Hong Kong is not covered by an adequacy decision of the European Commission. For the data we collect directly from you, as controller (the account, the website, billing), our processing from Hong Kong is fully subject to the GDPR (Article 3(2)). For the practices' data, which we process as processor, remote access by our team from Hong Kong (support, administration) relies on the standard contractual clauses adopted by the European Commission in Implementing Decision (EU) 2021/914, module two, concluded with each practice through the Data Processing Agreement (Article 46(2)(c) GDPR), with supplementary measures: the data remains stored in the Union, access is read-only, logged, with two-factor authentication and over encrypted connections, with no local copies outside the European Economic Area.

7.2. Some suppliers (Stripe, Google, GitHub) belong to groups with companies in the USA. Any transfers to the USA rely on the EU–US Data Privacy Framework (for certified companies) or on the standard contractual clauses adopted by the European Commission, together with the UK Extension or the UK International Data Transfer Agreement (IDTA).

7.3. Health data from patient records remains hosted in the EU. Exception: PDF documents that the practice chooses to send to the patient by email pass through Google Workspace (section 6.1).

8. How we protect data

Encryption in transit (TLS, HSTS); encrypted AES-256 daily backups; encryption of sensitive fields (for example the personal identification number (CNP), allergies, chronic conditions, medication); a separate database for each practice; two-factor authentication, mandatory for practice owners and administrators and for our team; screen lock after inactivity; login attempt limiting; access log for patient records; read-only, logged support sessions. The full list is in Annex 3 to the Data Processing Agreement.

9. How long we keep data after the contract ends

9.1. When a practice terminates the contract or stops paying, the account switches to read-only mode. The practice has 30 days to export, after which the practice's data is deleted from production, following a notice sent 7 days beforehand.

9.2. Backups are deleted by rotation: those on the server after 30 days; those in external storage, if enabled, after at most 35 days.

9.3. We keep data longer only where the law requires it or where we need it to defend a right (invoices, proof of acceptance of the contract), as set out in the table in section 4.

10. Your rights

10.1. You have the right: of access to your data (Article 15 GDPR); to rectification (Article 16); to erasure (Article 17); to restriction of processing (Article 18); to data portability (Article 20); to object (Article 21), including, at any time and without

giving reasons, to direct marketing; to withdraw your consent, without affecting the processing carried out before the withdrawal (Article 7(3)); not to be subject to a decision based solely on automated processing (Article 22).

10.2. Write to us at gdpr@medadmin.ro. We may ask you to confirm your identity. We respond without undue delay and within one month at the latest; for complex requests the period may be extended by two months, and we will inform you. Responding is free of charge, except for manifestly unfounded or excessive requests.

10.3. If you are a patient of a practice and write to us about your record, we forward the request to the practice within 5 working days and let you know. The practice responds on the merits.

10.4. You may lodge a complaint with a supervisory authority:

- **Romania**: the National Supervisory Authority for Personal Data Processing (ANSPDCP), B-dul G-ral. Gheorghe Magheru 28-30, sector 1, Bucharest, www.dataprotection.ro;
- **Hong Kong**: the Office of the Privacy Commissioner for Personal Data (PCPD), Room 1303, 13/F, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, Hong Kong, www.pcpd.org.hk.

11. Cookies and local storage

We use only strictly necessary cookies (session, CSRF protection, "remember me", trusted device for two-factor authentication) and the browser's local storage for display preferences. Our usage statistics use neither cookies nor persistent identifiers. We use no advertising and no third-party analytics tools. Full list: Cookie policy.

12. Minors

The practice account and the accounts of practice users are intended exclusively for adults working in the practice. Data of minors as patients is entered by the practice, as controller; for the portal, see the patient portal privacy policy.

13. Applicable legislation

We process data in accordance with Regulation (EU) 2016/679 (GDPR), Law 190/2018 on measures implementing the GDPR, Law 506/2004 on electronic communications and, for Alucard as a Hong Kong company, the Personal Data (Privacy) Ordinance (Cap. 486).

14. Changes

We publish each new version at the same address, with a version number and date; previous versions remain available from the page's version selector. We announce important changes to clients by email and in the application at least 30 days in advance.