Data processing agreement (DPA)

MedAdmin · Version 2.1 · effective from 11 November 2026

1. Summary

- **Who is who.** The practice is the **controller** of the data of its patients and staff. Alucard Limited is the **processor**: it processes this data only to provide MedAdmin, on the practice's instructions (art. 28 GDPR).
- **Where.** On Hetzner servers in Germany (EU). Each practice has its own database.
- **Who else has access.** Only the sub-processors in Annex 2. Any change is announced 30 days in advance; the practice may object and may terminate without penalty.
- **Incidents.** We notify the practice within 48 hours of becoming aware, so that it can notify ANSPDCP (the Romanian supervisory authority) within the 72-hour deadline.
- **At the end.** 30 days for export, then deletion; backups are deleted by rotation. We confirm deletion in writing, on request.

The parties

1. **[name of the practice]**, tax identification number (CUI) [tax ID of the practice], with its registered office at [registered office of the practice], email [email of the practice], telephone [phone of the practice], as **controller** (the "Controller");
2. **Alucard Limited** (registered name ALUCARD LIMITED), UBI 81569528, with its registered office at Unit B, 11/F, 23 Thomson Road, Wan Chai, Hong Kong SAR China, email gdpr@medadmin.ro, as **processor** (the "Processor").

This Agreement is concluded by electronic acceptance at sign-up or when a new version takes effect and forms part of the MedAdmin Terms and Conditions (the "Main Contract"). The version, date, time, IP address and the user who accepted are recorded.

2. Definitions

The terms "personal data", "processing", "controller", "processor", "data subject", "data concerning health" and "personal data breach" have the meaning given in Regulation (EU) 2016/679 ("GDPR"). "Sub-processor" means another processor engaged by the Processor in accordance with art. 28(2) and (4) GDPR. The "Service" is MedAdmin, as described in the Main Contract.

3. Subject matter and duration

3.1. The Processor processes personal data on behalf of the Controller, exclusively for the provision of the Service, as described in Annex 1.

3.2. This Agreement lasts as long as the Main Contract, plus the return and deletion period in section 12.

4. The Controller's instructions

4.1. The Processor processes the data only on documented instructions from the Controller, including with regard to transfers, unless required to do so by Union or Member State law; in that case it informs the Controller before processing, unless the law prohibits this.

4.2. The following constitute documented instructions: the Main Contract, this Agreement, the settings made by the Controller in the Service and written requests sent by ticket or email. Examples of settings that are instructions: activating

SMS, e-Factura (Romanian e-invoicing), CNAS (National Health Insurance House) reporting, the patient portal, online payments, automated imaging analyses, the mobile and desktop applications, sending a document by email.

4.3. **The patient portal.** When it activates the patient portal, the Controller instructs the Processor: (a) to maintain a central index of cryptographic fingerprints (HMAC) of the patient's telephone number, the carer's telephone number and the personal numeric code (CNP), used only to link records to the patient's portal account; (b) to display to the patient and to persons linked to them as carers the data published by the Controller in the portal; (c) to record in the Controller's log the actions taken from the portal. The patient's portal account is a separate relationship, in which the Processor is the controller (see the Patient Portal Privacy Policy).

4.4. The Processor immediately informs the Controller if, in its opinion, an instruction infringes the GDPR or other data protection provisions.

4.5. The Controller is responsible for the lawfulness of the processing, for the existence of a lawful basis, for informing patients and for obtaining consents where required.

5. Confidentiality of personnel

5.1. The Processor ensures that persons authorised to process the data have committed themselves to confidentiality or are under a statutory obligation of confidentiality.

5.2. The Processor's personnel access the Controller's data only for support at the Controller's request or for incident management, through a support session which: is read-only by default; requires a reason; allows writing only with an additional reason and the two-factor authentication code of the support operator; is logged and is visible to the Controller.

6. Security of processing

The Processor applies the technical and organisational measures in Annex 3, in accordance with art. 32 GDPR. It may update them without reducing the overall level of protection.

7. Sub-processors

7.1. The Controller grants a general written authorisation for the sub-processors in Annex 2.

7.2. The Processor notifies the Controller by email and in the application at least 30 days before adding or replacing a sub-processor. The Controller may raise reasoned objections within this period. If the parties do not find a solution, the Controller may terminate the Main Contract without penalty, with a pro rata refund of the paid and unused period.

7.3. The Processor imposes on sub-processors, by contract, data protection obligations at least equivalent to those in this Agreement and remains fully liable to the Controller for their performance.

8. Transfers

8.1. The Controller's data is hosted in the European Economic Area (Germany).

8.2. The Processor has its registered office in Hong Kong (SAR China), a territory not covered by an adequacy decision of the European Commission. The data remains stored in the EEA; remote access by the Processor's personnel from Hong Kong (support, administration) is a transfer within the meaning of Chapter V GDPR and relies on the standard contractual clauses adopted by Commission Implementing Decision (EU) 2021/914, module two (controller to processor), which the parties conclude by accepting this Agreement, with the following options: clause 7 (docking) included; clause 9(a), option 2 (general authorisation, with the 30-day notice in section 7); clause 11 without the optional mechanism; clause 13:

ANSPDCP; clause 17: Romanian law; clause 18: the courts of Romania. Annex I to the standard clauses consists of the parties and the description of the processing in Annex 1 to this Agreement, Annex II of the measures in Annex 3, and Annex III of the sub-processors in Annex 2. In the event of conflict, the standard clauses prevail. The Processor has assessed the impact of the transfer and applies supplementary measures: the data is not copied outside the EEA, access is read-only, logged, with two-factor authentication and over encrypted connections (section 5.2 and Annex 3).

8.3. Sub-processors in groups with companies in the United States (Google, Stripe, GitHub) may transfer data to the United States only on the basis of the EU–US Data Privacy Framework (certified companies) or of the standard contractual clauses adopted by the European Commission (art. 46 GDPR).

8.4. Data concerning health is not transferred outside the EEA, with one exception under the Controller's control: documents that the Controller chooses to send to a patient by email pass through Google Workspace (Annex 2). The Controller can avoid this flow by sending documents through the patient portal.

9. Assistance with data subjects' rights

9.1. The Service provides the Controller with tools for patients' rights: export of the record (PDF and JSON), rectification, restriction, anonymisation and deletion, subject to archiving periods; the record access log; management of consents and their withdrawal.

9.2. If the Processor receives a request directly from a data subject concerning the Controller's data, it forwards it to the Controller within 5 working days and does not respond on the merits without instructions.

9.3. For requests that the Controller cannot resolve itself from the Service, the Processor assists it within 10 working days at most.

10. Assistance with arts. 32–36 GDPR

The Processor assists the Controller, taking into account the nature of the processing and the information available, in ensuring security, notifying breaches, carrying out data protection impact assessments (DPIA) and prior consultation with ANSPDCP, by providing the available technical documentation (description of the flows, of the measures in Annex 3 and of the sub-processors).

11. Personal data breaches

11.1. The Processor notifies the Controller without undue delay and within **48 hours** at most of becoming aware of a personal data breach affecting the Controller's data, so that the Controller can meet the **72-hour** deadline towards ANSPDCP (art. 33 GDPR).

11.2. The notification includes, to the extent known: the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed and the contact person. Information not available at first is provided in phases, without undue delay.

11.3. The Processor immediately takes the measures necessary to limit the effects, preserves the evidence and documents the incident. It does not notify ANSPDCP or the data subjects on behalf of the Controller without the Controller's instruction, unless the law requires it.

12. Return and deletion of data

12.1. Upon termination of the Main Contract, the Controller may export the data for 30 days (PDF and JSON, plus uploaded files). On request, within the same period, the Processor provides a complete archive of the Controller's database.

12.2. After this period, the Processor deletes the Controller's database and the files in storage. Backups on the server are deleted by rotation within 30 days at most; those in external storage, if activated, in accordance with Annex 3. On request, the Processor confirms the deletion in writing.

12.3. The Processor may retain data only if the law requires it, and only to the extent of that obligation.

12.4. Local data on the Controller's workstations, phones and tablets (the desktop application, the agent, the mobile applications) is deleted when the device is disconnected or uninstalled; the Controller is responsible for disconnecting devices before termination.

13. Audit

13.1. The Processor makes available to the Controller the information necessary to demonstrate compliance with art. 28 GDPR: this Agreement, the description of the measures in Annex 3, the list of sub-processors and their audit reports or public certifications.

13.2. The Controller may carry out an audit, directly or through an independent auditor bound by confidentiality, at most once a year (and at any time after a security breach affecting it), with 30 days' notice, during working hours, without affecting the security or data of other clients. The audit is normally carried out remotely and on the basis of documents. The costs are borne by the Controller, unless the audit finds a significant breach attributable to the Processor.

14. Liability

The parties' liability is determined in accordance with art. 82 GDPR and the Main Contract. The limitation of liability in the Main Contract does not apply to intentional or grossly negligent breaches of this Agreement.

15. Final provisions

15.1. In the event of a conflict between this Agreement and the Main Contract, this Agreement prevails in matters of data protection.

15.2. This Agreement is governed by the same law as the Main Contract.

Annex 1. Description of the processing

Element	Content
Nature of the processing	hosting, storage, organisation, structuring, consultation, display in the platform, in the patient portal and in the applications, transmission at the Controller's request (SMS, email, push notifications, e-Factura to ANAF (the Romanian tax authority), reporting to CNAS, fiscal receipts through the local agent, payments through Stripe Connect), automated imaging analyses at the Controller's request, backups, export, deletion
Purpose	provision of the Service: appointments, patient records, medical record, consultations, documents and consents, imaging, receipts and tax documents, CNAS reporting, communications with patients, the patient portal, reports
Duration	for the duration of the Main Contract, plus 30 days for export and the backup rotation period
Data subjects	the Controller's patients and their carers or legal representatives (including the parents of minors); the Controller's staff (doctors, nurses, reception, accountant, collaborators); the contact persons of the Controller's suppliers and corporate clients

Element	Content
Categories of data	identification (surname, first name, personal numeric code (CNP), date of birth, sex, identity document, if entered); contact (telephone, email, address); administrative data (appointments, visit history, payments, estimates, invoices, receipts); insurance data (insured status, health insurance fund, data from the national health insurance card read during the consultation); communications (SMS, email, notifications, responses to confirmation links and questionnaires); technical data of the patient using a link or the portal (IP address, time, browser); staff data (name, specialty, stamp code, schedule, access logs)
Special categories	data concerning health (medical history, diagnoses, treatments, allergies, medication, results, clinical and DICOM images, questionnaires, medical consents) and, depending on the specialty, data concerning sex life (for example gynaecology, urology) or data from psychological counselling, entered by the Controller
Frequency	continuous, for the duration of the Contract
Place of processing	Germany (Hetzner, Falkenstein); Romania (SMSLink); Ireland and, for technical data, the United States (Google, Stripe), in accordance with Annex 2; on the Controller's devices, for the encrypted local copies of the applications

Annex 2. Authorised sub-processors

Updated public list: Sub-processors and hosting.

Sub-processor	Location of data	Purpose	Controller's data	Safeguards
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany	Germany (Falkenstein data centre)	hosting of servers, databases, files, backups; optionally, object storage for imaging and external backups	all categories in Annex 1	data processing agreement under art. 28 GDPR; data in the EU; ISO/IEC 27001 certified data centres
Ploi B.V., the Netherlands	the Netherlands (administration panel); the data remains on the Hetzner servers	server administration: deployment of versions, TLS certificates, processes, scheduled tasks	does not store the Controller's data; has technical administrative access to the server	data processing agreement under art. 28 GDPR; data in the EU
ASTINVEST COM SRL, CUI 9250710, through the SMSLink platform, Romania	Romania	sending SMS messages to patients (confirmations, reminders, links, authentication codes) and receiving replies	telephone number; content of the SMS (first name, date and time, practice name, link or code), without medical data	contract with art. 28 GDPR clauses; data in Romania
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland (Google Workspace)	Ireland / EU; possibly the US	sending transactional emails: invitations, codes, notifications and the PDF documents the Controller chooses to send by email	email address, name, message content and, at the Controller's request, the attached document	Google Cloud Data Processing Addendum; standard contractual clauses; EU–US Data Privacy Framework
Google Ireland Limited (Firebase Cloud Messaging)	Ireland / EU; possibly the US	delivering push notifications to the MedAdmin Doctor and MedAdmin Pacient applications	the device's notification token; generic text, without medical data	Firebase Data Processing and Security Terms; standard contractual clauses; EU–US Data Privacy Framework

Sub-processor	Location of data	Purpose	Controller's data	Safeguards
Stripe Payments Europe, Limited, 1 Grand Canal Street Lower, Dublin 2, Ireland	Ireland / EU; possibly the US	for patient payments (Stripe Connect): creating the payment session in the Controller's Stripe account	the amount, the payment description, the internal reference; the card details are entered by the patient directly with Stripe	Stripe Data Processing Agreement; EU–US Data Privacy Framework and standard contractual clauses. For payment data, Stripe contracts directly with the Controller
GitHub B.V. / GitHub, Inc.	EU / US	hosting of the source code and distribution of the desktop application installation files	none (receives no Controller data)	listed for transparency

Recipients that are not sub-processors: ANAF (e-Factura) and the health insurance funds (SIUI, the health insurance IT system), to which the Service transmits data only on the Controller's instruction, as authorities towards which the Controller has its own obligations.

Providers inactive today, which will be added only with the 30-day notice in section 7.2: an error reporting service (Sentry, configured without personal data) and an invoicing service (SmartBill), which would process only the Controller's invoicing data.

Annex 3. Technical and organisational measures

Data isolation

- A separate database for each practice; on each request the application opens only the database of the authenticated practice.
- Each practice's files are kept in a dedicated, non-public directory; downloads are made only through the application, after checking permissions, or through short-lived signed links.
- Backups can be restored individually, per practice.
- Patient portal: the central database holds only the account, the links and the HMAC fingerprints; medical data is read from the practice's database on each request, only for active links.

Encryption

- In transit: HTTPS (TLS) for all traffic, with HSTS; the mobile and desktop applications communicate only over HTTPS.
- At rest, at field level: the CNP, allergies, chronic conditions, medication and integration secrets (for example ANAF tokens) are encrypted with the application key (AES-256), kept separately from the database; searches by CNP are made through an HMAC fingerprint per practice.
- Backups: archives encrypted with AES-256 using a passphrase kept separately from the server.
- Passwords: hash only (bcrypt); PINs: hash only.
- On devices: the mobile applications keep offline data in an AES-256 encrypted database (SQLCipher), with the key in the Keychain or Keystore, excluded from backup; the desktop agent's tokens are protected with DPAPI (Windows), and those of the desktop application in Windows Credential Manager or the Keychain.
- The server disk is not fully encrypted; protection at rest is ensured through field-level encryption of sensitive data and encryption of the backups, and the data centre (Hetzner, Germany, ISO 27001 certified) physically controls access to the equipment.

Access control

- Roles and permissions per practice (account holder, administrator, doctor, nurse, reception, accountant), following the principle of least privilege; confidential notes (for example in psychology) are visible only to their author.
- Two-factor authentication (TOTP) mandatory for account holders, administrators and the Processor's team; the account holder may require it for the whole team; recovery codes; trusted device for at most 30 days.
- Attempt limiting: 5 failed attempts per account and IP address lock the account for 15 minutes, with an email alert to the account holders.
- Screen lock after inactivity (15 minutes by default), unlocked with a PIN or password; sessions with expiry, individual closing and "sign me out everywhere".
- Mobile devices and desktop workstations have individual tokens, revocable from the platform; revocation deletes local data at the next connection.
- Access by the Processor's personnel: read-only support session, with a reason, logged (section 5.2); access to servers only with named SSH keys and through the administration panel protected by two-factor authentication.

Logging and monitoring

- Patient record access log (who, what, when, from where), including downloads from the portal and the applications, available to the Controller.
- Log of authentications, lockouts, exports, deletions, permission changes and support sessions.
- Monitoring of availability and scheduled tasks (checked every minute), with alerts.
- Technical server logs are kept for 14 days; activity logs for 12 months.

Availability and resilience

- Daily full backups (at 03:00) of the central database, of all practice databases and of the files, encrypted, kept for 30 days.
- Optional external copy in object storage in the EU (Hetzner Object Storage), in another data centre, with a lifecycle rule of at most 35 days.
- Restoration per practice, with prior saving of the current state; monthly restoration test recommended.
- Zero-downtime deployment and quick rollback to the previous version.

Minimisation and retention

- SMS messages and push notifications contain no medical data; links sent to patients are signed, expire and, where appropriate, require a verification code.
- The practices' public pages and the portal do not use tracking cookies; usage statistics contain no personal data.
- Automated imaging analyses run on the Processor's servers, without transmitting images to third parties; the Controller's data is not used to train models.
- Error reporting, if activated, does not send personal data.
- Development and demonstration environments use only fictitious data.
- Exports uploaded for migration from another software are deleted automatically 30 days after the migration is completed or cancelled.

Organisational measures

- Confidentiality undertakings for staff and collaborators.
- Documented procedure for managing incidents and security breaches.
- Assessment of providers before contracting and annual review of the list of sub-processors.
- Secure development: code review, automated tests, up-to-date dependencies.

- Staff training on data protection at the start of the collaboration and at least once a year; an annual, documented incident response exercise.