**EVER Health GmbH**

# Agreement on the Processing of Personal Data on Behalf of the Controller

pursuant to Art. 28 GDPR – for practice documentation in the EVER Workspace

**Version:** 2.1 · **Last updated:** 20 August 2026

> **Non-binding English translation.** This English text is provided for information only. The agreement is concluded exclusively in German, and only the German version is legally binding. In the event of any discrepancy between the two versions, the German version prevails. The binding German version is available at everhealth.ai/avv.

## Contracting Parties

This agreement is concluded between

the professional user – doctor, alternative practitioner (Heilpraktiker), therapist or coach – who registers for the EVER Workspace and confirms this agreement as part of the registration,

hereinafter the “Controller”,

and

EVER Health GmbH, Goethestraße 5, 35633 Lahnau, Germany, registered in the commercial register under HRB 9344,

hereinafter the “Processor” or “EVER”,

together hereinafter the “Parties”.

## Preamble: Two Separate Data Spaces

The EVER Workspace contains two data spaces that are to be classified differently under data protection law. This agreement applies exclusively to the first. The following delineation forms part of the agreement and is decisive for its interpretation.

### (1) Practice Documentation – subject matter of this agreement

Practice Documentation comprises all content that the Controller creates exclusively for its own purposes of practice and treatment documentation and that is not accessible to the data subject in their EVER account. This includes in particular:

- internal notes of the Controller on a patient,
- medical history questionnaires uploaded by the Controller and comparable internal practice documents,
- patient data sets created by the Controller whose invitation to register with EVER has not yet been accepted (preparation phase).

The Controller alone decides on the purposes and means of this processing. EVER processes these data solely on instructions and deletes them upon termination of the Controller’s user relationship. For this data space, EVER is a processor within the meaning of Art. 28 GDPR.

### (2) Patient Record – not subject matter of this agreement

The Patient Record comprises nutrient logs, laboratory values and all other content that is accessible to the data subject in their own EVER account.

The data subject concludes a separate user agreement with EVER, accepts the EVER Terms of Use and the EVER Privacy Policy, and gives the consents required for the processing of their health data personally and directly to EVER. These data remain available to the data subject even if the Controller terminates its user relationship with EVER. They are not subject to any claim by the Controller for deletion or surrender.

EVER therefore processes the Patient Record neither on behalf of nor on the instructions of the Controller, but as a controller in its own right within the meaning of Art. 4(7) GDPR in relation to the data subject. Processing on behalf pursuant to Art. 28 GDPR is ruled out for this data space. In particular, EVER cannot and may not comply with the requirement of Art. 28(3)(g) GDPR – deletion or return of the data at the choice of the Controller at the end of the provision of services – for these data, because the data are allocated to the data subject's own user relationship.

Consequently, the Controller cannot conclude a data processing agreement with EVER in respect of the Patient Record. Its role with regard to this data space is that of a recipient of a sharing authorisation granted by the data subject.

| | Practice Documentation | Patient Record |
|---|---|---|
| **Content** | Notes, medical history questionnaires, invitations not accepted | Nutrient logs, laboratory values, app content |
| **Visible to the data subject** | No | Yes – the data are allocated to their account |
| **Legal basis in relation to the data subject** | Responsibility of the Controller | Separate agreement and separate consent given to EVER |
| **Upon termination of the Controller's access** | Are deleted | Remain with the data subject |
| **Role of EVER** | Processor (Art. 28 GDPR) | Controller in its own right (Art. 4(7) GDPR) |
| **This agreement** | Applies | Does not apply |

### (3) The Controller's own responsibility towards its patients

The Controller remains independently responsible for safeguarding, under data protection law and professional law, the integration of EVER into its practice workflows and the transfer of patient data to EVER. This includes in particular informing the data subjects, the existence of a sound legal basis for transferring the contact data to EVER for the purpose of the invitation, and compliance with its professional duty of confidentiality.

## § 1 Subject Matter, Term and Termination

(1) The subject matter of this agreement is the processing of personal data of the Practice Documentation within the meaning of item (1) of the Preamble by EVER on behalf of the Controller in the context of providing the EVER Workspace.

(2) The term of this agreement corresponds to the term of the user agreement on the EVER Workspace between the Parties. It begins with the Controller's confirmation as part of the registration and ends upon termination of the user agreement.

(3) The Controller may terminate this agreement at any time without notice; such termination also entails ending the use of the functions for practice documentation. The right of both Parties to extraordinary termination for good cause remains unaffected. Good cause exists for the Controller in particular if EVER breaches material obligations under this agreement and does not remedy the breach within a reasonable period.

## § 2 Nature, Scope and Purpose of the Processing

(1) The nature, scope and purpose of the processing, the type of personal data processed and the categories of data subjects are set out exhaustively in Annex 1 to this agreement.

(2) The processing takes place exclusively at the locations specified in Annex 3. Processing outside these locations requires prior agreement in accordance with § 11.

(3) EVER does not process the data of the Practice Documentation for its own purposes. These data are not used to train or adapt artificial intelligence models, for analytical purposes beyond the provision of the services or for advertising purposes. EVER does not train its own language models and does not transfer any data of the Practice Documentation to providers of language models for training purposes.

(4) Internal notes of the Controller and uploaded medical history questionnaires are not transferred to external providers of language models. Insofar as AI-supported functions process content, personal identifiers are first removed within EVER's infrastructure; the requests to the language model contain no identifiable data of the data subject.

## § 3 Controller's Right to Issue Instructions

(1) EVER processes the data of the Practice Documentation only on documented instructions from the Controller, unless EVER is required to process them by Union or Member State law. In such a case, EVER informs the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

(2) The Controller's use of the respective functions of the EVER Workspace constitutes an instruction within the meaning of this agreement. Further individual instructions are to be sent in text form to support@everhealth.ai and are documented by EVER.

(3) EVER informs the Controller without undue delay if EVER is of the opinion that an instruction infringes data protection provisions. EVER is entitled to suspend the execution of the instruction concerned until it is confirmed or amended.

## § 4 Confidentiality and Professional Secrecy

(1) EVER commits all persons authorised to process the data to confidentiality, insofar as they are not already subject to an appropriate statutory obligation of confidentiality. This obligation continues to apply after the end of their activity.

(2) Insofar as the Controller is subject to a duty of confidentiality under section 203 StGB (German Criminal Code), EVER acts as an "other contributing person" (sonstige mitwirkende Person) within the meaning of section 203(3), second sentence, StGB. EVER obliges the persons dealing with the data at EVER to maintain secrecy in accordance with section 203(4) StGB and ensures that this obligation is also passed on to the sub-processors engaged.

(3) Upon request, EVER provides the Controller with a separate confidentiality undertaking under section 203(4) StGB in text form. The request is to be sent to support@everhealth.ai.

(4) Within EVER, access to the Practice Documentation is restricted to those employees who require it to provide the contractual services, to rectify errors or to handle a support request from the Controller. Access for support purposes is logged.

## § 5 Technical and Organisational Measures

(1) EVER implements the technical and organisational measures required under Art. 32 GDPR to ensure a level of protection appropriate to the risk. The measures in place at the time the agreement is concluded are described in Annex 2.

(2) EVER may further develop and adapt the measures during the contractual relationship. In doing so, the agreed level of protection must not be undercut. EVER documents material changes and makes them accessible to the Controller.

(3) EVER ensures that the data of the Practice Documentation are processed logically separately from the data of other controllers (tenant separation).

## § 6 Sub-processors

(1) The Controller grants EVER general authorisation to engage other processors. The sub-processors engaged at the time the agreement is concluded are listed in Annex 3 and are hereby approved.

(2) EVER informs the Controller at least four weeks before engaging a new sub-processor or replacing an existing one. The information is provided by email to the address stored in the account or by a notice in the EVER Workspace.

(3) The Controller may object to an intended change in text form within four weeks of receipt of the information for an important reason relating to data protection. If the objection cannot be resolved, the Controller is entitled to terminate the user agreement extraordinarily with effect from the time of the changeover.

(4) EVER imposes on each sub-processor, by contract, data protection obligations that correspond to the obligations under this agreement, and is liable to the Controller for compliance with these obligations.

(5) Ancillary services of third parties that EVER uses to conduct its business, such as telecommunication services, maintenance of end devices or the disposal of data carriers, do not constitute sub-processing within the meaning of this provision. EVER ensures confidentiality in these cases as well.

## § 7 Assistance to the Controller

(1) EVER assists the Controller by appropriate technical and organisational measures in fulfilling its obligation to respond to requests from data subjects exercising their rights under Chapter III GDPR.

(2) If a data subject contacts EVER directly with regard to the Practice Documentation, EVER forwards the request to the Controller without undue delay and does not respond to it itself. If the request concerns the Patient Record within the meaning of item (2) of the Preamble, EVER handles it on its own responsibility.

(3) Taking into account the nature of the processing and the information available to it, EVER assists the Controller in complying with the obligations under Art. 32 to 36 GDPR, in particular with a data protection impact assessment and any prior consultation of the supervisory authority.

(4) EVER may demand reasonable remuneration for assistance effort that goes beyond the statutory obligations and for which EVER is not responsible. EVER points this out to the Controller before the effort is incurred.

## § 8 Personal Data Breaches

(1) EVER notifies the Controller of any personal data breach concerning the Practice Documentation without undue delay and at the latest within 48 hours of becoming aware of it. The notification is sent to the email address stored in the Controller’s account.

(2) Insofar as available, the notification contains a description of the nature of the breach, the categories and approximate number of data subjects and data records concerned, the likely consequences, the measures taken or proposed to remedy the breach, and a contact point for further enquiries.

(3) For the Practice Documentation, the notification to the supervisory authority under Art. 33 GDPR and the communication to the data subjects under Art. 34 GDPR are the responsibility of the Controller. EVER assists the Controller in this regard.

## § 9 Evidence and Audit Rights

(1) Upon request, EVER makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Art. 28 GDPR.

(2) Such evidence may be provided by means of current attestations, certifications, reports from independent bodies or an appropriate self-assessment. The Controller acknowledges that such evidence constitutes an appropriate means of control for a standardised cloud service.

(3) Where such evidence is not sufficient in an individual case, EVER enables the Controller, or an auditor mandated by the Controller who is bound to confidentiality and is not in competition with EVER, to carry out audits, including inspections. These are to be announced with reasonable advance notice of at least four weeks, are to be scheduled during normal business hours and must not unreasonably disrupt business operations. They are limited to one audit per calendar year unless there is a specific reason.

## § 10 Deletion and Return

(1) After termination of the user agreement, EVER deletes the data of the Practice Documentation. Deletion takes place no later than 30 days after the end of the agreement, unless a statutory retention obligation precludes this.

(2) Until this period expires, the Controller may request the surrender of the data of the Practice Documentation. EVER provides the data to the Controller in a common, machine-readable format. The request is to be sent in text form to support@everhealth.ai.

(3) For the avoidance of doubt: deletion under paragraph 1 covers exclusively the Practice Documentation within the meaning of item (1) of the Preamble. Content of the Patient Record within the meaning of item (2) of the Preamble remains in the account of the respective data subject. The Controller has no claim to its deletion or surrender.

(4) Deletion under paragraph 1 initially covers the production systems. Data contained in backup copies are not deleted separately; they expire when the retention period of the respective backup copy ends. During this period, the data are no longer actively processed and are held exclusively for restoration purposes. The retention period of the backup copies is stated in Annex 2.

(5) EVER may retain documentation that serves as evidence of proper data processing beyond the end of the agreement in accordance with the respective retention periods.

## § 11 Transfers to Third Countries

(1) Processing of the data of the Practice Documentation in a country outside the European Union or the European Economic Area takes place only insofar as the requirements of Art. 44 et seq. GDPR are met.

(2) If there is no adequacy decision of the European Commission for the country concerned, the transfer takes place on the basis of appropriate safeguards, in particular the EU Standard Contractual Clauses, supplemented by any necessary additional measures.

(3) The third-country connections existing at the time the agreement is concluded are set out in Annex 3.

## § 12 Obligations of the Controller

(1) The Controller is solely responsible for the lawfulness of the processing of the data of the Practice Documentation and for safeguarding the rights of the data subjects.

(2) The Controller ensures that there is a sound legal basis for the collection of the data, for their transfer to EVER and for their processing in the EVER Workspace, and that the data subjects have been informed to the extent required by law.

(3) The Controller designates to EVER a contact person for data protection matters in connection with this agreement.

(4) The Controller informs EVER without undue delay if it discovers errors or irregularities in the processing by EVER.

## § 13 Liability

(1) The liability of the Parties is governed by Art. 82 GDPR.

(2) In all other respects, the liability provisions of the user agreement on the EVER Workspace concluded between the Parties apply, insofar as they do not conflict with mandatory statutory requirements.

## § 14 Conclusion of the Agreement in Electronic Form

(1) This agreement is concluded in electronic format pursuant to Art. 28(9) GDPR. The Controller confirms it by active consent as part of the registration for the EVER Workspace.

(2) EVER documents the time of consent, the consenting user ID and the version of this agreement consented to, and provides evidence thereof to the Controller upon request.

(3) The Controller can access the version of this agreement applicable to it at any time in its account and download it as a PDF.

(4) EVER may amend this agreement insofar as this is necessary to adapt it to changes in the legal situation, case law or requirements of the supervisory authorities. EVER informs the Controller of the amendment at least six weeks before it takes effect. If the Controller does not object within six weeks, the new version is deemed accepted. EVER expressly points out the significance of silence in the amendment notice. In the event of an objection, each Party is entitled to terminate the user agreement with effect from the time the amendment takes effect.

## § 15 Final Provisions

(1) In the event of conflicts between this agreement and the user agreement on the EVER Workspace, the provisions of this agreement take precedence insofar as the processing of personal data of the Practice Documentation is concerned.

(2) Should any provision of this agreement be or become invalid, the validity of the remaining provisions remains unaffected. The Parties shall replace the invalid provision with a valid provision that comes closest to the economic purpose of the invalid provision.

(3) This agreement is governed by the law of the Federal Republic of Germany, excluding the UN Convention on Contracts for the International Sale of Goods (CISG).

(4) Annexes 1 to 3 form part of this agreement.

## Annex 1 – Description of the Processing

### 1. Subject matter of the processing

Storage, structuring, provision and deletion of the Practice Documentation created by the Controller in the EVER Workspace in the context of providing the software service.

### 2. Purpose of the processing

- Provision of the functions for practice and treatment documentation for the Controller
- Preparation of the invitation of a patient to register with EVER in their own right
- technical operation, data backup, troubleshooting and support

### 3. Nature of the processing

Collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, restriction, erasure and destruction – in each case within the scope of the functions used by the Controller.

### 4. Categories of data subjects

- Patients and clients of the Controller
- Employees of the Controller who use the EVER Workspace

### 5. Type of personal data

Within the Practice Documentation, the following data in particular are processed:

- Master data: first name, surname, date of birth
- Contact data: email address
- Free-text content from internal notes of the Controller
- medical history questionnaires uploaded by the Controller and comparable internal practice documents
- Processing metadata: times of creation and modification, allocation to the Controller's account, status of an invitation sent

Special categories of personal data: the aforementioned content may include health data within the meaning of Art. 9(1) GDPR. The processing takes place in compliance with the heightened requirements of Art. 9 GDPR and subject to the protective measures described in Annex 2.

### 6. Not covered

Nutrient logs, laboratory values and all other content that is accessible to the data subject in their own EVER account are not the subject matter of this processing on behalf. For these, EVER is a controller in its own right; see item (2) of the Preamble.

### 7. Duration of the processing

For the term of the user agreement on the EVER Workspace, followed by deletion in accordance with § 10.

### 8. Contact points

Processor: EVER Health GmbH, Goethestraße 5, 35633 Lahnau, support@everhealth.ai

Data protection officer of the Processor: RPA Datenschutz + Compliance GmbH, Hauser Gasse 19b, 35578 Wetzlar, info@rpa-datenschutz.de

## Annex 2 – Technical and Organisational Measures

The structure follows Art. 32(1) GDPR. The measures describe the status at the time the agreement is concluded.

### 1. Confidentiality

- Physical access control: processing takes place exclusively in Amazon Web Services data centres in the eu-central-1 region (Frankfurt am Main). Physical access protection is ensured by AWS and is evidenced by AWS's certifications.
- System access control: authentication and authorisation are carried out via Auth0 (EU tenant). Sign-in is by email and password and, for data subjects, optionally also via Google sign-in. Multi-factor authentication is not currently offered; its introduction for professional user accounts is part of the 2026 security roadmap.
- Data access control: role-based access control concept (RBAC) with separate roles for professional users, data subjects and internal administration. Administrative access to production systems takes place exclusively via a jump host using AWS Systems Manager Session Manager and is logged.
- Network isolation: application services and databases are located in private subnets within separate virtual private clouds. Incoming traffic is routed via an Application Load Balancer with an upstream web application

firewall.

- Environment separation: development and production run in completely separate environments with separate data sets.
- Tenant separation: the data of different professional users are processed logically separately at application level. A professional user can access only the data records assigned to them.
- Encryption: encryption in transit via TLS and at rest via the encryption services of AWS. Key management is carried out via the AWS Key Management Service in accordance with the provider's default settings.
- Separation of AI processing and identifiable data: before every request to an external language model, personal identifiers are removed within the EVER infrastructure. As a matter of principle, notes and medical history questionnaires are not transferred to external language models.

### 2. Integrity

- Transfer control: transport encryption of all connections between clients, API services and databases; delivery of static content via Amazon CloudFront.
- Input control: logging of the creation, modification and deletion of content, and audit trails for releases by the professional user.
- Infrastructure as code: the infrastructure is versioned using Terraform; changes run through automated CI/CD pipelines with GitHub Actions and are traceable.

### 3. Availability and resilience

- Stateless, horizontally scalable application services on Amazon ECS behind load balancers.
- Central logging, monitoring and alerting via Amazon CloudWatch.
- Data backup: automated backups via Amazon RDS within the eu-central-1 region. The retention period of the backup copies is 35 days.
- Recovery: the target recovery time after a system failure is 24 hours.
- Contingency plan: a documented contingency and restart plan is being prepared and is part of the 2026 security roadmap.

### 4. Process for regular review

- An AWS security audit has been carried out; a security and hardening roadmap for 2026 has been defined and is being implemented.
- Processor control: sub-processors are vetted before being engaged and are contractually bound in accordance with Art. 28 GDPR.
- Data protection management: EVER Health GmbH has appointed RPA Datenschutz + Compliance GmbH as its external data protection officer.
- Certifications: the AWS infrastructure used is covered by the provider's attestations, including the BSI C5 attestation (German Federal Office for Information Security). EVER Health GmbH does not currently hold a certification of its own.
- Deletion concept: deletion under § 10 takes place in the production systems; data contained in backup copies expire with their retention period. A documented deletion concept is part of the 2026 security roadmap.

## Annex 3 – Sub-processors and Processing Locations

| Company | Service and place of processing | Third-country connection and safeguard |
|---|---|---|
| **Amazon Web Services EMEA SARL, Luxembourg** | Hosting of the entire platform (ECS, RDS, S3, CloudFront, CloudWatch), including data backup. Processing in the eu-central-1 region, Frankfurt am Main. | Processing within the EU. The AWS Standard Contractual Clauses apply to support and remote access. |

| Company | Service and place of processing | Third-country connection and safeguard |
|---|---|---|
| **Auth0 / Okta** | Authentication and authorisation of user accounts (login credentials, account identifiers). | EU tenant, processing within the EU. |
| **OpenAI Ireland Ltd.** | AI-supported functions (EVER Guide): text generation and summarisation. Receives no identifiable data – identifiers are removed at EVER beforehand. Notes and medical history questionnaires are not transferred. | The contracting party is OpenAI Ireland Ltd. A data processing agreement including the EU Standard Contractual Clauses is in place. |
| **Stripe Payments Europe Ltd., Ireland** | Processing of the professional user's subscription payments. | Processing within the EU. Does not affect the Practice Documentation. |
| **GitHub Inc.** | Source code management and CI/CD pipelines. | No access to production data of the Practice Documentation. |

Not engaged as sub-processing: the invitation emails to patients are sent by the EVER application itself using open-source software libraries on EVER's own infrastructure in the eu-central-1 region. No external email delivery service provider is used for this purpose. HubSpot is used exclusively for marketing communication and receives no data of the Practice Documentation.