

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

gemäß Art. 28 DSGVO – für die Praxisdokumentation im EVER Workspace

Version: 2.1 · **Stand:** 20. August 2026

Vertragsparteien

Dieser Vertrag wird geschlossen zwischen

der Fachanwenderin bzw. dem Fachanwender – Ärztin/Arzt, Heilpraktikerin/Heilpraktiker, Therapeutin/Therapeut oder Coach –, die oder der sich für den EVER Workspace registriert und diesen Vertrag im Rahmen der Registrierung bestätigt,

nachfolgend „Verantwortlicher“,

und

der EVER Health GmbH, Goethestraße 5, 35633 Lahnau, Deutschland, eingetragen im Handelsregister unter HRB 9344,

nachfolgend „Auftragsverarbeiter“ oder „EVER“,

gemeinsam nachfolgend „Parteien“.

Präambel: Zwei getrennte Datenräume

Der EVER Workspace enthält zwei datenschutzrechtlich unterschiedlich einzuordnende Datenräume. Dieser Vertrag gilt ausschließlich für den ersten. Die folgende Abgrenzung ist Bestandteil des Vertrages und für seine Auslegung maßgeblich.

(1) Praxisdokumentation – Gegenstand dieses Vertrages

Zur Praxisdokumentation zählen alle Inhalte, die der Verantwortliche ausschließlich für seine eigenen Zwecke der Praxis- und Behandlungsdokumentation anlegt und die der betroffenen Person in ihrem EVER-Konto nicht zugänglich sind. Dies sind insbesondere:

- interne Notizen des Verantwortlichen zu einer Patientin oder einem Patienten,
- vom Verantwortlichen hochgeladene Anamnesebögen und vergleichbare praxisinterne Dokumente,
- Patientendatensätze, die der Verantwortliche angelegt hat, deren Einladung zur Registrierung bei EVER jedoch noch nicht angenommen wurde (Vorbereitungsphase).

Über Zweck und Mittel dieser Verarbeitung entscheidet allein der Verantwortliche. EVER verarbeitet diese Daten ausschließlich weisungsgebunden und löscht sie mit Beendigung des Nutzungsverhältnisses des Verantwortlichen. Für diesen Datenraum ist EVER Auftragsverarbeiter im Sinne des Art. 28 DSGVO.

(2) Patientenakte – nicht Gegenstand dieses Vertrages

Zur Patientenakte zählen Nährstoffprotokolle, Laborwerte und alle weiteren Inhalte, die der betroffenen Person in ihrem eigenen EVER-Konto zugänglich sind.

Die betroffene Person schließt mit EVER einen eigenen Nutzungsvertrag, akzeptiert die EVER-Nutzungsbedingungen und die EVER-Datenschutzerklärung und erteilt die für die Verarbeitung ihrer Gesundheitsdaten erforderlichen Einwilligungen selbst und unmittelbar gegenüber EVER. Diese Daten bleiben der betroffenen Person auch dann erhalten, wenn der Verantwortliche sein Nutzungsverhältnis mit EVER beendet. Sie unterliegen keinem Lösungs- oder Herausgabeanspruch des Verantwortlichen.

EVER verarbeitet die Patientenakte daher nicht im Auftrag und nicht auf Weisung des Verantwortlichen, sondern als eigener Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO im Verhältnis zur betroffenen Person. Eine Auftragsverarbeitung nach Art. 28 DSGVO scheidet für diesen Datenraum aus. EVER kann insbesondere die Vorgabe des Art. 28 Abs. 3 lit. g DSGVO – Löschung oder Rückgabe der Daten nach Wahl des Verantwortlichen bei Beendigung der Leistung – für diese Daten nicht erfüllen und darf sie nicht erfüllen, weil die Daten dem eigenen Nutzungsverhältnis der betroffenen Person zugeordnet sind.

Der Verantwortliche kann über die Patientenakte folglich keinen Auftragsverarbeitungsvertrag mit EVER schließen. Seine Rolle gegenüber diesem Datenraum ist die eines Empfängers einer durch die betroffene Person erteilten Freigabe.

	Praxisdokumentation	Patientenakte
Inhalte	Notizen, Anamnesebögen, nicht angenommene Einladungen	Nährstoffprotokolle, Laborwerte, App-Inhalte
Für die betroffene Person einsehbar	Nein	Ja – die Daten sind ihrem Konto zugeordnet
Rechtsgrundlage gegenüber der betroffenen Person	Verantwortet der Verantwortliche	Eigener Vertrag und eigene Einwilligung gegenüber EVER
Bei Beendigung des Zugangs des Verantwortlichen	Werden gelöscht	Bleiben bei der betroffenen Person
Rolle von EVER	Auftragsverarbeiter (Art. 28 DSGVO)	Eigener Verantwortlicher (Art. 4 Nr. 7 DSGVO)
Dieser Vertrag	Gilt	Gilt nicht

(3) Eigenverantwortung des Verantwortlichen gegenüber seinen Patientinnen und Patienten

Der Verantwortliche bleibt eigenständig dafür verantwortlich, die Einbindung von EVER in seine Praxisabläufe sowie die Übermittlung von Patientendaten an EVER datenschutzrechtlich und berufsrechtlich abzusichern. Dies umfasst insbesondere die Information der betroffenen Personen, das Vorliegen einer tragfähigen Rechtsgrundlage für die Übermittlung der Kontaktdaten an EVER zum Zweck der Einladung sowie die Beachtung seiner berufsrechtlichen Schweigepflicht.

§ 1 Gegenstand, Dauer und Beendigung

- (1) Gegenstand dieses Vertrages ist die Verarbeitung personenbezogener Daten der Praxisdokumentation im Sinne der Präambel Ziffer (1) durch EVER im Auftrag des Verantwortlichen im Rahmen der Bereitstellung des EVER Workspace.

- (2) Die Laufzeit dieses Vertrages entspricht der Laufzeit des Nutzungsvertrages über den EVER Workspace zwischen den Parteien. Er beginnt mit der Bestätigung durch den Verantwortlichen im Rahmen der Registrierung und endet mit Beendigung des Nutzungsvertrages.
- (3) Der Verantwortliche kann diesen Vertrag jederzeit fristlos kündigen; die Kündigung umfasst zugleich die Beendigung der Nutzung der Funktionen zur Praxisdokumentation. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt für beide Parteien unberührt. Ein wichtiger Grund liegt für den Verantwortlichen insbesondere vor, wenn EVER wesentliche Pflichten aus diesem Vertrag verletzt und die Verletzung nicht innerhalb einer angemessenen Frist abstellt.

§ 2 Art, Umfang und Zweck der Verarbeitung

- (1) Art, Umfang und Zweck der Verarbeitung, die Art der verarbeiteten personenbezogenen Daten sowie die Kategorien betroffener Personen ergeben sich abschließend aus Anlage 1 zu diesem Vertrag.
- (2) Die Verarbeitung findet ausschließlich innerhalb der in Anlage 3 genannten Standorte statt. Eine Verarbeitung außerhalb dieser Standorte bedarf der vorherigen Vereinbarung nach § 11.
- (3) EVER verarbeitet die Daten der Praxisdokumentation nicht für eigene Zwecke. Eine Nutzung dieser Daten zum Training oder zur Anpassung von Modellen künstlicher Intelligenz, zu Analysezielen über die Leistungserbringung hinaus oder zu Werbezwecken findet nicht statt. EVER trainiert keine eigenen Sprachmodelle und übermittelt keine Daten der Praxisdokumentation an Anbieter von Sprachmodellen zu Trainingszwecken.
- (4) Interne Notizen des Verantwortlichen und hochgeladene Anamnesebögen werden nicht an externe Anbieter von Sprachmodellen übermittelt. Soweit KI-gestützte Funktionen Inhalte verarbeiten, werden personenbezogene Identifikationsmerkmale zuvor innerhalb der Infrastruktur von EVER entfernt; die Anfragen an das Sprachmodell enthalten keine Klardaten der betroffenen Person.

§ 3 Weisungsrecht des Verantwortlichen

- (1) EVER verarbeitet die Daten der Praxisdokumentation ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, EVER ist nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet. In einem solchen Fall teilt EVER dem Verantwortlichen die rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
- (2) Die Nutzung der jeweiligen Funktionen des EVER Workspace durch den Verantwortlichen gilt als Weisung im Sinne dieses Vertrages. Weitergehende Einzelweisungen sind in Textform an support@everhealth.ai zu richten und werden von EVER dokumentiert.
- (3) EVER informiert den Verantwortlichen unverzüglich, wenn EVER der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt. EVER ist berechtigt, die Durchführung der betreffenden Weisung bis zu ihrer Bestätigung oder Änderung auszusetzen.

§ 4 Vertraulichkeit und berufsrechtliche Schweigepflicht

- (1) EVER verpflichtet alle zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit, soweit sie nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung besteht auch nach Beendigung ihrer Tätigkeit fort.
- (2) Soweit der Verantwortliche einer Schweigepflicht nach § 203 StGB unterliegt, wird EVER als sonstige mitwirkende Person im Sinne des § 203 Abs. 3 Satz 2 StGB tätig. EVER verpflichtet die bei ihr mit den Daten

befassten Personen entsprechend § 203 Abs. 4 StGB zur Geheimhaltung und stellt sicher, dass diese Verpflichtung auch gegenüber eingesetzten Unterauftragsverarbeitern weitergegeben wird.

- (3) EVER stellt dem Verantwortlichen auf Anforderung eine gesonderte Verpflichtungserklärung nach § 203 Abs. 4 StGB in Textform zur Verfügung. Die Anforderung ist an support@everhealth.ai zu richten.
- (4) Der Zugriff auf die Praxisdokumentation ist innerhalb von EVER auf diejenigen Beschäftigten beschränkt, die ihn zur Erbringung der vertraglichen Leistungen, zur Fehlerbehebung oder zur Bearbeitung einer Supportanfrage des Verantwortlichen benötigen. Zugriffe zu Supportzwecken werden protokolliert.

§ 5 Technische und organisatorische Maßnahmen

- (1) EVER trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die zum Zeitpunkt des Vertragsschlusses getroffenen Maßnahmen sind in Anlage 2 beschrieben.
- (2) EVER darf die Maßnahmen im Laufe des Vertragsverhältnisses fortentwickeln und anpassen. Das vereinbarte Schutzniveau darf dabei nicht unterschritten werden. Wesentliche Änderungen dokumentiert EVER und macht sie dem Verantwortlichen zugänglich.
- (3) EVER stellt sicher, dass die Daten der Praxisdokumentation von den Daten anderer Verantwortlicher logisch getrennt verarbeitet werden (Mandantentrennung).

§ 6 Unterauftragsverarbeiter

- (1) Der Verantwortliche erteilt EVER die allgemeine Genehmigung, weitere Auftragsverarbeiter einzusetzen. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in Anlage 3 aufgeführt und werden hiermit genehmigt.
- (2) EVER informiert den Verantwortlichen mindestens vier Wochen vor der Beauftragung eines neuen oder dem Austausch eines bestehenden Unterauftragsverarbeiters. Die Information erfolgt per E-Mail an die im Konto hinterlegte Adresse oder durch eine Mitteilung im EVER Workspace.
- (3) Der Verantwortliche kann einer beabsichtigten Änderung innerhalb von vier Wochen nach Zugang der Information aus einem wichtigen datenschutzrechtlichen Grund in Textform widersprechen. Kann die Beanstandung nicht ausgeräumt werden, ist der Verantwortliche berechtigt, den Nutzungsvertrag zum Zeitpunkt der Umstellung außerordentlich zu kündigen.
- (4) EVER erlegt jedem Unterauftragsverarbeiter durch Vertrag Datenschutzpflichten auf, die den Pflichten aus diesem Vertrag entsprechen, und haftet gegenüber dem Verantwortlichen für die Einhaltung dieser Pflichten.
- (5) Nicht als Unterauftragsverarbeitung im Sinne dieser Vorschrift gelten Nebenleistungen Dritter, die EVER zur Ausübung ihrer Geschäftstätigkeit in Anspruch nimmt, etwa Telekommunikationsleistungen, Wartung von Endgeräten oder die Entsorgung von Datenträgern. EVER stellt auch hier die Vertraulichkeit sicher.

§ 7 Unterstützung des Verantwortlichen

- (1) EVER unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen betroffener Personen auf Wahrnehmung ihrer Rechte nach Kapitel III der DSGVO nachzukommen.
- (2) Wendet sich eine betroffene Person hinsichtlich der Praxisdokumentation unmittelbar an EVER, leitet EVER den Antrag unverzüglich an den Verantwortlichen weiter und beantwortet ihn nicht selbst. Betrifft der Antrag die Patientenakte im Sinne der Präambel Ziffer (2), bearbeitet EVER ihn in eigener Verantwortung.

- (3) EVER unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihr zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus den Art. 32 bis 36 DSGVO, insbesondere bei einer Datenschutz-Folgenabschätzung und einer etwaigen vorherigen Konsultation der Aufsichtsbehörde.
- (4) Für einen über die gesetzlichen Pflichten hinausgehenden Unterstützungsaufwand, der nicht von EVER zu vertreten ist, kann EVER eine angemessene Vergütung verlangen. EVER weist den Verantwortlichen hierauf vor Entstehen des Aufwandes hin.

§ 8 Verletzungen des Schutzes personenbezogener Daten

- (1) EVER meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten der Praxisdokumentation unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntniserlangung. Die Meldung erfolgt an die im Konto des Verantwortlichen hinterlegte E-Mail-Adresse.
- (2) Die Meldung enthält, soweit verfügbar, eine Beschreibung der Art der Verletzung, die betroffenen Kategorien und die ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen, die ergriffenen oder vorgeschlagenen Abhilfemaßnahmen sowie eine Kontaktstelle für Rückfragen.
- (3) Die Meldung an die Aufsichtsbehörde nach Art. 33 DSGVO und die Benachrichtigung der betroffenen Personen nach Art. 34 DSGVO obliegen für die Praxisdokumentation dem Verantwortlichen. EVER unterstützt ihn dabei.

§ 9 Nachweise und Kontrollrechte

- (1) EVER stellt dem Verantwortlichen auf Anforderung alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten erforderlich sind.
- (2) Der Nachweis kann durch aktuelle Testate, Zertifizierungen, Berichte unabhängiger Stellen oder eine geeignete Selbstauskunft geführt werden. Der Verantwortliche erkennt an, dass solche Nachweise für eine standardisierte Cloud-Leistung ein angemessenes Kontrollmittel darstellen.
- (3) Soweit ein solcher Nachweis im Einzelfall nicht ausreicht, ermöglicht EVER dem Verantwortlichen oder einem von ihm beauftragten, zur Verschwiegenheit verpflichteten und nicht mit EVER im Wettbewerb stehenden Prüfer Überprüfungen einschließlich Inspektionen. Diese sind mit angemessener Vorlaufzeit von mindestens vier Wochen anzukündigen, auf die üblichen Geschäftszeiten zu legen und dürfen den Betriebsablauf nicht unangemessen beeinträchtigen. Sie sind auf eine Prüfung pro Kalenderjahr beschränkt, sofern kein besonderer Anlass besteht.

§ 10 Löschung und Rückgabe

- (1) Nach Beendigung des Nutzungsvertrages löscht EVER die Daten der Praxisdokumentation. Die Löschung erfolgt spätestens 30 Tage nach Vertragsende, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht.
- (2) Der Verantwortliche kann bis zum Ablauf dieser Frist die Herausgabe der Daten der Praxisdokumentation verlangen. EVER stellt sie ihm in einem gängigen, maschinenlesbaren Format bereit. Die Anforderung ist in Textform an support@everhealth.ai zu richten.
- (3) Klarstellend gilt: Die Löschung nach Absatz 1 erfasst ausschließlich die Praxisdokumentation im Sinne der Präambel Ziffer (1). Inhalte der Patientenakte im Sinne der Präambel Ziffer (2) bleiben im Konto der jeweiligen betroffenen Person bestehen. Ein Anspruch des Verantwortlichen auf deren Löschung oder Herausgabe besteht nicht.

- (4) Die Löschung nach Absatz 1 erfasst zunächst die Produktivsysteme. In Sicherungskopien enthaltene Daten werden nicht gesondert gelöscht; sie laufen mit dem Ablauf der Aufbewahrungsfrist der jeweiligen Sicherungskopie aus. Innerhalb dieses Zeitraums werden die Daten nicht mehr aktiv verarbeitet und ausschließlich zu Wiederherstellungszwecken vorgehalten. Die Aufbewahrungsfrist der Sicherungskopien ist in Anlage 2 ausgewiesen.
- (5) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, darf EVER über das Vertragsende hinaus entsprechend den jeweiligen Aufbewahrungsfristen aufbewahren.

§ 11 Übermittlung in Drittländer

- (1) Eine Verarbeitung der Daten der Praxisdokumentation in einem Land außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums findet nur statt, soweit die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.
- (2) Besteht für das betreffende Land kein Angemessenheitsbeschluss der Europäischen Kommission, erfolgt die Übermittlung auf Grundlage geeigneter Garantien, insbesondere der EU-Standardvertragsklauseln, ergänzt um erforderliche zusätzliche Maßnahmen.
- (3) Die zum Zeitpunkt des Vertragsschlusses bestehenden Drittlandbezüge sind in Anlage 3 ausgewiesen.

§ 12 Pflichten des Verantwortlichen

- (1) Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung der Daten der Praxisdokumentation sowie für die Wahrung der Rechte der betroffenen Personen allein verantwortlich.
- (2) Der Verantwortliche stellt sicher, dass für die Erhebung der Daten, für ihre Übermittlung an EVER und für ihre Verarbeitung im EVER Workspace eine tragfähige Rechtsgrundlage besteht, und dass die betroffenen Personen in dem gesetzlich erforderlichen Umfang informiert wurden.
- (3) Der Verantwortliche benennt EVER eine Ansprechperson für Fragen des Datenschutzes im Zusammenhang mit diesem Vertrag.
- (4) Der Verantwortliche unterrichtet EVER unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung durch EVER feststellt.

§ 13 Haftung

- (1) Für die Haftung der Parteien gilt Art. 82 DSGVO.
- (2) Im Übrigen gelten die Haftungsregelungen des zwischen den Parteien geschlossenen Nutzungsvertrages über den EVER Workspace, soweit sie zwingenden gesetzlichen Vorgaben nicht entgegenstehen.

§ 14 Vertragsschluss in elektronischer Form

- (1) Dieser Vertrag wird gemäß Art. 28 Abs. 9 DSGVO in elektronischem Format geschlossen. Der Verantwortliche bestätigt ihn im Rahmen der Registrierung für den EVER Workspace durch aktive Zustimmung.
- (2) EVER dokumentiert Zeitpunkt der Zustimmung, die zustimmende Nutzerkennung und die zugestimmte Fassung dieses Vertrages und weist dies dem Verantwortlichen auf Anforderung nach.
- (3) Der Verantwortliche kann die jeweils für ihn geltende Fassung dieses Vertrages jederzeit in seinem Konto abrufen und als PDF herunterladen.

- (4) EVER kann diesen Vertrag ändern, soweit dies zur Anpassung an geänderte Rechtslage, Rechtsprechung oder aufsichtsbehördliche Vorgaben erforderlich ist. EVER informiert den Verantwortlichen mindestens sechs Wochen vor Wirksamwerden über die Änderung. Widerspricht der Verantwortliche nicht innerhalb von sechs Wochen, gilt die neue Fassung als angenommen. Auf die Bedeutung des Schweigens weist EVER in der Änderungsmitteilung gesondert hin. Im Falle eines Widerspruchs ist jede Partei berechtigt, den Nutzungsvertrag zum Zeitpunkt des Wirksamwerdens der Änderung zu kündigen.

§ 15 Schlussbestimmungen

- (1) Bei Widersprüchen zwischen diesem Vertrag und dem Nutzungsvertrag über den EVER Workspace gehen die Regelungen dieses Vertrages vor, soweit die Verarbeitung personenbezogener Daten der Praxisdokumentation betroffen ist.
- (2) Sollte eine Bestimmung dieses Vertrages unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien ersetzen die unwirksame Bestimmung durch eine wirksame Regelung, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt.
- (3) Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.
- (4) Die Anlagen 1 bis 3 sind Bestandteil dieses Vertrages.

Anlage 1 – Beschreibung der Verarbeitung

1. Gegenstand der Verarbeitung

Speicherung, Strukturierung, Bereitstellung und Löschung der vom Verantwortlichen im EVER Workspace angelegten Praxisdokumentation im Rahmen der Bereitstellung der Softwareleistung.

2. Zweck der Verarbeitung

- Bereitstellung der Funktionen zur Praxis- und Behandlungsdokumentation für den Verantwortlichen
- Vorbereitung der Einladung einer Patientin oder eines Patienten zur eigenen Registrierung bei EVER
- technischer Betrieb, Datensicherung, Fehlerbehebung und Support

3. Art der Verarbeitung

Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Einschränken, Löschen und Vernichten – jeweils im Rahmen der vom Verantwortlichen genutzten Funktionen.

4. Kategorien betroffener Personen

- Patientinnen und Patienten sowie Klientinnen und Klienten des Verantwortlichen
- Beschäftigte des Verantwortlichen, die den EVER Workspace nutzen

5. Art der personenbezogenen Daten

Innerhalb der Praxisdokumentation werden insbesondere folgende Daten verarbeitet:

- Stammdaten: Vorname, Nachname, Geburtsdatum
- Kontaktdaten: E-Mail-Adresse
- Freitextinhalte aus internen Notizen des Verantwortlichen
- vom Verantwortlichen hochgeladene Anamnesebögen und vergleichbare praxisinterne Dokumente
- Metadaten der Verarbeitung: Erstellungs- und Änderungszeitpunkte, Zuordnung zum Konto des Verantwortlichen, Status einer versendeten Einladung

Besondere Kategorien personenbezogener Daten: Die vorgenannten Inhalte können Gesundheitsdaten im Sinne des Art. 9 Abs. 1 DSGVO enthalten. Die Verarbeitung erfolgt unter Beachtung der erhöhten Anforderungen des Art. 9 DSGVO und unter den in Anlage 2 beschriebenen Schutzmaßnahmen.

6. Nicht erfasst

Nicht Gegenstand dieser Verarbeitung im Auftrag sind Nährstoffprotokolle, Laborwerte und alle weiteren Inhalte, die der betroffenen Person in ihrem eigenen EVER-Konto zugänglich sind. Für diese ist EVER eigener Verantwortlicher; siehe Präambel Ziffer (2).

7. Dauer der Verarbeitung

Für die Dauer des Nutzungsvertrages über den EVER Workspace, anschließend Löschung nach Maßgabe des § 10.

8. Kontaktstellen

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

Datenschutzbeauftragte des Auftragsverarbeiters: RPA Datenschutz + Compliance GmbH, Hauser Gasse 19b, 35578 Wetzlar, info@rpa-datenschutz.de

Anlage 2 – Technische und organisatorische Maßnahmen

Die Gliederung folgt Art. 32 Abs. 1 DSGVO. Die Maßnahmen beschreiben den Stand zum Zeitpunkt des Vertragsschlusses.

1. Vertraulichkeit

- Zutrittskontrolle: Die Verarbeitung erfolgt ausschließlich in Rechenzentren der Amazon Web Services in der Region eu-central-1 (Frankfurt am Main). Der physische Zutrittsschutz wird durch AWS gewährleistet und ist über die dortigen Zertifizierungen nachgewiesen.
- Zugangskontrolle: Authentifizierung und Autorisierung erfolgen über Auth0 (EU-Tenant). Die Anmeldung erfolgt über E-Mail und Passwort, für betroffene Personen zusätzlich optional über Google-Anmeldung. Eine Mehrfaktorauthentifizierung wird derzeit nicht angeboten; ihre Einführung für Fachanwenderkonten ist Teil der Sicherheits-Roadmap 2026.
- Zugriffskontrolle: Rollenbasiertes Berechtigungskonzept (RBAC) mit getrennten Rollen für Fachanwender, betroffene Personen und interne Administration. Der administrative Zugriff auf Produktionssysteme erfolgt ausschließlich über einen Jump Host mittels AWS Systems Manager Session Manager und wird protokolliert.
- Netzwerkisolation: Anwendungsdienste und Datenbanken liegen in privaten Subnetzen innerhalb getrennter Virtual Private Clouds. Der eingehende Verkehr wird über einen Application Load Balancer mit vorgeschalteter Web Application Firewall geführt.
- Umgebungstrennung: Entwicklung und Produktion laufen in vollständig getrennten Umgebungen mit getrennten Datenbeständen.
- Mandantentrennung: Die Daten verschiedener Fachanwender werden auf Anwendungsebene logisch getrennt verarbeitet. Ein Fachanwender kann ausschließlich auf die ihm zugeordneten Datensätze zugreifen.
- Verschlüsselung: Verschlüsselung im Transport über TLS und im Ruhezustand über die Verschlüsselungsdienste von AWS. Die Schlüsselverwaltung erfolgt über den AWS Key Management Service nach den Standardvorgaben des Anbieters.
- Trennung von KI-Verarbeitung und Klardaten: Vor jeder Anfrage an ein externes Sprachmodell werden personenbezogene Identifikationsmerkmale innerhalb der EVER-Infrastruktur entfernt. Notizen und Anamnesebögen werden grundsätzlich nicht an externe Sprachmodelle übermittelt.

2. Integrität

- Weitergabekontrolle: Transportverschlüsselung aller Verbindungen zwischen Clients, API-Diensten und Datenbanken; Auslieferung statischer Inhalte über Amazon CloudFront.
- Eingabekontrolle: Protokollierung von Erstellung, Änderung und Löschung von Inhalten sowie Audit-Trails für Freigaben durch den Fachanwender.
- Infrastructure as Code: Die Infrastruktur wird über Terraform versioniert; Änderungen laufen über automatisierte CI/CD-Pipelines mit GitHub Actions und sind nachvollziehbar.

3. Verfügbarkeit und Belastbarkeit

- Zustandslose, horizontal skalierbare Anwendungsdienste auf Amazon ECS hinter Load Balancern.
- Zentrale Protokollierung, Überwachung und Alarmierung über Amazon CloudWatch.
- Datensicherung: Automatisierte Sicherungen über Amazon RDS innerhalb der Region eu-central-1. Die Aufbewahrungsfrist der Sicherungskopien beträgt 35 Tage.
- Wiederherstellung: Die angestrebte Wiederherstellungszeit nach einem Systemausfall beträgt 24 Stunden.

- Notfallkonzept: Ein dokumentiertes Notfall- und Wiederanlaufkonzept befindet sich in Erarbeitung und ist Teil der Sicherheits-Roadmap 2026.

4. Verfahren zur regelmäßigen Überprüfung

- Ein AWS Security Audit wurde durchgeführt; eine Sicherheits- und Härtings-Roadmap für 2026 ist definiert und in Umsetzung.
- Auftragskontrolle: Unterauftragsverarbeiter werden vor Beauftragung geprüft und vertraglich nach Art. 28 DSGVO gebunden.
- Datenschutz-Management: Die EVER Health GmbH hat mit der RPA Datenschutz + Compliance GmbH eine externe Datenschutzbeauftragte bestellt.
- Zertifizierungen: Die eingesetzte AWS-Infrastruktur unterliegt den Testaten des Anbieters, unter anderem dem BSI-C5-Testat. Eine eigene Zertifizierung der EVER Health GmbH besteht derzeit nicht.
- Löschkonzept: Die Löschung nach § 10 erfolgt in den Produktivsystemen; in Sicherungskopien enthaltene Daten laufen mit deren Aufbewahrungsfrist aus. Ein dokumentiertes Löschkonzept ist Teil der Sicherheits-Roadmap 2026.

Anlage 3 – Unterauftragsverarbeiter und Verarbeitungsstandorte

Unternehmen	Leistung und Verarbeitungsort	Drittlandbezug und Garantie
Amazon Web Services EMEA SARL, Luxemburg	Hosting der gesamten Plattform (ECS, RDS, S3, CloudFront, CloudWatch) einschließlich Datensicherung. Verarbeitung in der Region eu-central-1, Frankfurt am Main.	Verarbeitung innerhalb der EU. Für Support- und Fernzugriffe gelten die AWS-Standardvertragsklauseln.
Auth0 / Okta	Authentifizierung und Autorisierung der Nutzerkonten (Anmeldedaten, Kontokennungen).	EU-Tenant, Verarbeitung innerhalb der EU.
OpenAI Ireland Ltd.	KI-gestützte Funktionen (EVER Guide): Textgenerierung und Zusammenfassung. Erhält keine Klardaten – Identifikationsmerkmale werden zuvor bei EVER entfernt. Notizen und Anamnesebögen werden nicht übermittelt.	Vertragspartnerin ist OpenAI Ireland Ltd. Es besteht ein Auftragsverarbeitungsvertrag einschließlich der EU-Standardvertragsklauseln.
Stripe Payments Europe Ltd., Irland	Abwicklung der Abonnementzahlungen des Fachanwenders.	Verarbeitung innerhalb der EU. Berührt die Praxisdokumentation nicht.
GitHub Inc.	Quellcodeverwaltung und CI/CD-Pipelines.	Kein Zugriff auf Produktionsdaten der Praxisdokumentation.

Nicht als Unterauftragsverarbeitung eingebunden: Der Versand der Einladungs-E-Mails an Patientinnen und Patienten erfolgt durch die EVER-Anwendung selbst unter Verwendung quelloffener Programmbibliotheken auf der eigenen Infrastruktur in der Region eu-central-1. Ein externer E-Mail-Versanddienstleister wird hierfür nicht eingesetzt. HubSpot wird ausschließlich für Marketing-Kommunikation verwendet und erhält keine Daten der Praxisdokumentation.