DiggAI GmbH (i. Gr.)
Margarete-Böhme-Str. 3 · 25813 Husum
diggai.de

Technische und organisatorische Maßnahmen

Anlage zum Auftragsverarbeitungsvertrag · Art. 32 DSGVO

> Vorabfassung zur Prüfung. Dieses Dokument gibt den Stand vom 1. August 2026 wieder und ist für die Prüfung durch Ihre Datenschutzbeauftragten bestimmt. Die anwaltliche Prüfung ist noch nicht abgeschlossen; die verbindliche Fassung zur Unterzeichnung erhalten Sie vor der Freischaltung Ihrer Praxis. Angaben in eckigen Klammern werden dabei durch Ihre Daten ersetzt.

> **Grundsatz dieses Dokuments: Es steht nichts darin, was nicht belegt ist.** Angaben, die am 01.08.2026 im Quellcode oder in der Betriebsdokumentation geprüft wurden, stehen ohne Vorbehalt. Alles Übrige ist als offen gekennzeichnet. Eine TOM-Beschreibung, die mehr verspricht als das System leistet, ist im Prüfungsfall schlechter als eine knappe.

Auftraggeber:

[Einrichtung] · [Vorname, Nachname] · [Straße] · [PLZ/Ort] · [Telefon] · [E-Mail]

Auftragnehmer:

DiggAI GmbH (i. Gr.), Margarete-Böhme-Str. 3, 25813 Husum
Geschäftsführer: Dr. med. Christian Klaproth

> Die Gesellschaft befindet sich in Gründung. Bis zur notariellen Beurkundung des Gesellschaftsvertrags handelt Dr. med. Christian Klaproth persönlich unter der vorstehenden Anschrift; danach die Vorgesellschaft, vertreten durch ihren Geschäftsführer.

0. Was DiggAI überhaupt speichert

> **Zur Rolle.** Ob das verschlüsselte Paket für den Auftragnehmer ein personenbezogenes Datum ist, wird rechtlich unterschiedlich beurteilt. Der Auftragnehmer legt sich darauf nicht fest und behandelt die Verarbeitung **vorsorglich** als Auftragsverarbeitung — diese Beschreibung gilt unabhängig davon, wie die Frage beantwortet wird.

Diese Übersicht steht bewusst am Anfang: Das Schutzniveau der folgenden Abschnitte ergibt sich vor allem daraus, wie wenig lesbare Daten überhaupt vorhanden sind.

Datenbestand	Form	Aufbewahrung
Inhalt einer Sendung an die Einrichtung (Anliegen, Vorgeschichte, Dokumente)	ausschließlich verschlüsselt; für den Auftragnehmer nicht zu öffnen	bis zur Abholung, längstens 30 Tage
Begleitdaten der Sendung: abgeleiteter Empfängerprüfwert, Eingangszeitpunkt, Größe, Abhol- und Ablaufstatus	Klartext, ohne Personenbezug zum Inhalt	mit der Sendung
Verzeichniseintrag der Einrichtung: Name, Anschrift, öffentlicher Schlüssel, Benachrichtigungs-E-Mail, Rufnummer	Klartext	bis Vertragsende oder Schlüsselaustausch

Datenbestand	Form	Aufbewahrung
Kunden- und Vertragsdaten der Einrichtung (Name, Rechtsform, BSNR bzw. IK, Vertragsstatus)	Klartext	Vertragslaufzeit, danach gesetzliche Fristen
Sicherheitsprotokolle über Vorgänge im geschützten Bereich (Abholung, Löschung, administrative Änderungen) mit IP-Adresse, Gerätekennung, Zeitpunkt und Aktion — **ein Zugriffsprotokoll des Webservers wird nicht geführt**	Klartext	90 Tage, danach automatische Löschung
Inhaltsleerer Nachweiseintrag über die Zustellung	Klartext, ohne Inhalt	30 Tage
Verschlüsselter Schlüsselaustausch zwischen Geräten der Einrichtung	verschlüsselt	abgeholt 30 Tage, sonst 90 Tage
Lokale Gesundheitsakte, Notfallpass, private Schlüssel der nutzenden Person	liegen ausschließlich auf deren Gerät	keine Speicherung beim Auftragnehmer

> **Klarstellung zu einer verbreiteten Annahme.** Es trifft nicht zu, dass beim Auftragnehmer nur Kundendaten zur Abwicklung des Zahlungsverkehrs gespeichert würden. Gespeichert werden zusätzlich die verschlüsselten Sendungen bis zur Abholung, die Verzeichnis- und Vertragsdaten der Einrichtung sowie Sicherheitsprotokolle mit IP-Adressen. Umgekehrt ist die Zahlungsabwicklung derzeit der am wenigsten aktive Teil: die entsprechende Funktion steht hinter einem Schalter, der standardmäßig aus ist. **Vor Verwendung ist zu prüfen, ob im Produktivbetrieb Zahlungsdaten verarbeitet werden;** ist das der Fall, gehört der Zahlungsdienstleister in Anlage 2 des AVV.

> **Offener Bereinigungspunkt.** Das Datenmodell enthält aus der Zeit vor der Umstellung auf Zero-Knowledge weitere Tabellen für Patientenkonten und serverseitig entschlüsselte Vorgänge. Sie werden vom heutigen Betrieb nicht mehr gefüllt; die Entscheidung, die Altbestände zu löschen, ist am 23.07.2026 getroffen, aber noch nicht vollzogen. Bis dahin ist diese Beschreibung insoweit unvollständig. Beim Entfernen ist zu beachten, dass der Produktivcontainer das Schema beim Start abgleicht und ein entferntes Modell seine Daten mitnimmt.

1. Vertraulichkeit

Maßnahmen, um Unbefugten den Zugang zu Daten und Systemen zu verwehren und unberechtigte Datennutzung zu verhindern.

1.1 Zutrittskontrolle

Die Serverinfrastruktur wird in einem Rechenzentrum des Hosting-Partners Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, betrieben. Für dieses liegen ein **BSI-C5-Testat Typ 2** und eine Zertifizierung nach **ISO/IEC 27001:2022** vor; der Geltungsbereich umfasst sämtliche Hosting-Dienste und Rechenzentren einschließlich des Verarbeitungsstandorts Helsinki. Die Nachweise werden auf Verlangen vorgelegt. Verarbeitungsort ist der Standort Helsinki, Finnland; die Verarbeitung findet damit vollständig innerhalb der Europäischen Union statt. Das Rechenzentrum verfügt über mehrstufige elektronische Zutrittskontrolle, Videoüberwachung, durchgehende Bewachung und alarmgesicherte Zugangsbereiche.

Eigene Serverräume unterhält der Auftragnehmer nicht. Arbeitsplatzrechner, über die administrative Zugänge möglich sind, sind mit Festplattenverschlüsselung und Bildschirmsperre gesichert. [Weitere Angaben zu den Geschäftsräumen vor Verwendung ergänzen.]

1.2 Zugangskontrolle

Der Zugriff auf interne Systeme erfordert individuelle Benutzerkonten; gemeinsam genutzte Konten werden nicht verwendet. Administrative Zugänge zur Serverinfrastruktur erfolgen über Schlüsselpaare, nicht über Kennwörter,

und sind auf einen festgelegten Personenkreis begrenzt. Für Zugänge zu Dienstleisterkonten ist Zwei-Faktor-Authentisierung eingerichtet.

Der Auftraggeber selbst authentisiert sich nicht über ein Kennwort. Die Einrichtung weist sich durch den Besitz ihres privaten Schlüssels aus: Der Server stellt eine Aufgabe, die nur mit dem passenden Schlüssel gelöst werden kann. Es gibt daher weder ein Praxiskennwort, das gestohlen werden könnte, noch eine Kennwortdatenbank beim Auftragnehmer.

[Kennwortrichtlinie, Sperre nach Fehlversuchen und Sitzungsablauf für interne Konten sind vor Verwendung zu dokumentieren.]

1.3 Zugriffskontrolle

Es gilt ein rollenbasiertes Berechtigungskonzept nach dem Grundsatz der geringsten Rechte. Die Zahl der Personen mit administrativem Zugriff ist auf das Notwendige begrenzt; administrative Vorgänge werden protokolliert.

Für die Inhalte der übermittelten Sendungen ist eine Zugriffskontrolle im herkömmlichen Sinne nicht erforderlich und auch nicht wirksam: **Ein Zugriff auf Inhalte ist technisch ausgeschlossen, nicht bloß organisatorisch untersagt.** Die Inhalte liegen ausschließlich verschlüsselt vor, und der zugehörige private Schlüssel befindet sich nicht im Verfügungsbereich des Auftragnehmers. Auch eine Person mit vollständigen Administratorrechten auf dem Server kann die Inhalte nicht lesen.

Alle für den Auftragnehmer tätigen Personen sind auf Vertraulichkeit und als sonstige mitwirkende Personen nach § 203 Abs. 3 Satz 2 StGB verpflichtet.

1.4 Trennungskontrolle

Die Anwendung ist mandantenfähig; Daten werden je Betriebsstätte bzw. Einrichtung getrennt geführt und sind für andere Mandanten nicht einsehbar. Eine Auswertung über Mandanten hinweg findet nicht statt.

Die Mandantentrennung wird in jedem Zugriffspfad ausdrücklich geprüft; eine automatische Filterung durch die Datenbankschicht besteht nicht und wird bewusst nicht vorausgesetzt. Entwicklungs-, Test- und Produktivumgebung sind getrennt; Echtdaten werden in nicht-produktiven Umgebungen nicht verwendet.

1.5 Pseudonymisierung und Verschlüsselung

Dies ist die tragende Maßnahme des gesamten Konzepts.

- **Ende-zu-Ende-Verschlüsselung der Inhalte.** Der Inhalt wird auf dem Gerät der absendenden Person mit AES-256-GCM verschlüsselt; der einmalige Sitzungsschlüssel wird über X25519 an den öffentlichen Schlüssel der empfangenden Einrichtung gebunden. Klartext entsteht erst wieder auf dem Gerät der Einrichtung.
- **Lokale Schlüsselerzeugung.** Das Schlüsselpaar der Einrichtung entsteht auf deren Gerät. Übertragen wird ausschließlich der öffentliche Schlüssel. Der private Schlüssel ist auf dem Gerät so abgelegt, dass die Anwendung ihn nicht auslesen kann.
- **Empfängerbezug nur als abgeleiteter Prüfwert.** Die Betriebsstättennummer wird nicht neben der Sendung gespeichert. Aus dem Datenbestand lässt sich daher nicht ableiten, welche Einrichtung eine bestimmte Sendung erhält.
- **Keine Klartext-Kennungen in Protokollen.** Protokolle enthalten technische Vorgangskennungen, keine Inhalte.
- **Verschlüsselte Sicherungen.** Sicherungskopien enthalten Inhalte ausschließlich in der bereits verschlüsselten Form.
- **Prüfung des Empfängers vor dem Versand.** Der absendenden Person wird der Fingerabdruck des öffentlichen Schlüssels angezeigt; ein Wechsel des Schlüssels muss erneut bestätigt werden. Einrichtungen werden vor der Freischaltung im Verzeichnis auf ihre Identität geprüft.

2. Integrität

2.1 Weitergabekontrolle

Sämtliche Verbindungen sind transportverschlüsselt (TLS, aktuelle Versionen mit starken Chiffren); unverschlüsselte Zugriffe werden abgewiesen oder umgeleitet. Zusätzlich zur Transportverschlüsselung sind die Inhalte bereits auf dem Endgerät verschlüsselt, sodass die Vertraulichkeit nicht allein von der Transportsicherung abhängt.

In der Weboberfläche greifen eine restriktive Content-Security-Policy, eine eingeschränkte Freigabe fremder Ursprünge sowie die üblichen Sicherheits-Header. Serverseitig bestehen Eingabeprüfung, Schutz gegen websiteübergreifende Anfragefälschung und Begrenzung der Aufrufhäufigkeit je Endpunkt. Ein externer Penetrationstest wurde durchgeführt; die bestätigten Befunde wurden behoben. [Datum und Prüfer vor Verwendung eintragen.]

2.2 Eingabekontrolle

Eingang, Abholung und Löschung jeder Sendung werden mit Zeitstempel protokolliert; administrative Vorgänge werden mit Benutzerkennung, Aktion, Ressource, IP-Adresse und Zeitpunkt aufgezeichnet. Die Protokolle enthalten keine Inhaltsdaten. Sie werden nach 90 Tagen automatisch gelöscht. **Ein dauerhaftes Zugriffsprotokoll des Webservers wird nicht geführt** — aufgerufene Adressen, Referrer, Browsertyp und Betriebssystem werden nicht gespeichert (am 01.08.2026 auf dem Produktivsystem geprüft: keine `log`-Direktive im Caddyfile, null Zugriffszeilen im Containerlog).

Über die Zustellung wird ein inhaltsleerer Nachweiseintrag geführt, der der Einrichtung belegt, wann eine Sendung eingegangen und abgeholt wurde.

3. Verfügbarkeit

Die Datenbank wird regelmäßig gesichert; die Sicherungen sind verschlüsselt und verbleiben innerhalb der Europäischen Union. Das Rechenzentrum stellt unterbrechungsfreie Stromversorgung, Netzersatz, Klimatisierung sowie Brandmelde- und Löschtechnik bereit.

Die Systeme werden auf Erreichbarkeit überwacht; bei Störungen erfolgt eine Alarmierung.

> Offen und vor Verwendung zu ergänzen: Sicherungsrhythmus, Aufbewahrungsdauer der Sicherungen, Zeitpunkt des letzten Wiederherstellungstests sowie Zielwerte für Wiederanlaufzeit und tolerierten Datenverlust. Ein Backup- und Wiederanlaufkonzept liegt vor; die Zahlen sind vor Verwendung gegen den tatsächlichen Betrieb zu prüfen.

Besonderheit der Architektur. Ein Ausfall des Auftragnehmers führt nicht zum Verlust bereits abgeholter Daten: Diese liegen entschlüsselt in der Einrichtung. Umgekehrt kann der Auftragnehmer noch nicht abgeholte Sendungen bei einem Verlust der Datenbank nicht aus einem Klartextbestand rekonstruieren — auch die Sicherung enthält sie nur verschlüsselt. Der Verlust der Verfügbarkeit noch nicht abgeholter Sendungen gilt ausdrücklich als meldepflichtiges Ereignis.

4. Belastbarkeit

Server und Anwendung werden gepflegt und aktualisiert; nicht benötigte Dienste und Anschlüsse sind abgeschaltet. Die Abhängigkeiten der Anwendung werden auf bekannte Schwachstellen überwacht.

Die Aufrufhäufigkeit ist je Endpunkt begrenzt, wodurch massenhafte automatisierte Anfragen und das systematische Durchprobieren von Zugangsdaten begrenzt werden. Schutz gegen Überlastangriffe besteht netzseitig beim Rechenzentrumsbetreiber.

Der Betrieb läuft auf einem einzelnen Serversystem. Eine redundante Auslegung mit automatischer Übernahme durch ein zweites System besteht derzeit nicht; im Störungsfall erfolgt die Wiederherstellung aus der Sicherung. Diese Angabe ist bewusst so formuliert, weil eine Hochverfügbarkeitszusage nicht eingelöst werden könnte.

5. Weitere organisatorische Maßnahmen

5.1 Zuständigkeit für den Datenschutz

Ansprechpartner für den Datenschutz ist [Name, E-Mail]. Ob ein Datenschutzbeauftragter zu bestellen ist, ist offen: Die Zahl der ständig mit der Verarbeitung beschäftigten Personen liegt unter zwanzig, § 38 Abs. 1 Satz 2 BDSG knüpft die Pflicht jedoch auch an Verarbeitungen, die einer Datenschutz-Folgenabschätzung unterliegen. Die Frage ist vor dem ersten Vertragsschluss zu klären.

5.2 Verpflichtung und Sensibilisierung

Alle für den Auftragnehmer tätigen Personen werden vor Aufnahme der Tätigkeit auf Vertraulichkeit und auf die Wahrung fremder Geheimnisse nach § 203 StGB verpflichtet; die Verpflichtung gilt unbefristet über das Ende der Tätigkeit hinaus. Das Muster ist Anlage 3 des Auftragsverarbeitungsvertrags. Eine Auffrischung erfolgt mindestens jährlich oder anlassbezogen.

5.3 Regelmäßige Überprüfung

Die Wirksamkeit der Maßnahmen wird mindestens jährlich sowie anlassbezogen überprüft, insbesondere bei wesentlichen Änderungen der Verarbeitung. Sicherheitsrelevante Änderungen an der Anwendung werden dokumentiert. Ein externer Penetrationstest wurde durchgeführt und die bestätigten Befunde behoben; Wiederholungen erfolgen anlassbezogen.

5.4 Umgang mit Sicherheitsvorfällen

Es besteht ein festgelegter Meldeweg. Anzeichen eines Vorfalls sind unverzüglich der Geschäftsführung anzuzeigen; diese bewertet den Vorfall, leitet Gegenmaßnahmen ein und dokumentiert ihn.

Bestätigt sich ein Vorfall mit Risiko für die Rechte und Freiheiten betroffener Personen, wird der betroffene Auftraggeber **unverzüglich, spätestens binnen 24 Stunden** nach Kenntnis unterrichtet — damit ihm für seine eigene Meldung nach Art. 33 DSGVO die volle Frist bleibt. Die Unterrichtung enthält die nach Art. 33 Abs. 3 DSGVO erforderlichen Angaben, soweit bekannt.

Bei der Bewertung ist zu berücksichtigen, dass beim Auftragnehmer gespeicherte Inhalte ausschließlich verschlüsselt vorliegen und die zugehörigen Schlüssel sich nicht in seinem Verfügungsbereich befinden.

5.5 Datenschutz durch Technikgestaltung und Voreinstellungen

- **Datenminimierung als Bauprinzip.** Der Auftragnehmer erhebt keine Inhalte, sondern befördert sie verschlossen. Was nicht lesbar vorliegt, kann weder ausgewertet noch weitergegeben noch versehentlich offengelegt werden.
- **Löschung ohne Zutun.** Die Fristen aus Abschnitt 0 laufen automatisch ab. Eine Verlängerung durch Weisung ist nicht vorgesehen.
- **Keine Übermittlung an Anbieter von Sprachmodellen.** Sprachverarbeitende Funktionen laufen auf dem Gerät der nutzenden Person oder auf einem Rechner in den Räumen der Einrichtung. Inhalte werden nicht an OpenAI, Google, Microsoft oder vergleichbare Anbieter übertragen. Ein Training mit Daten des Auftraggebers oder seiner Patientinnen und Patienten findet nicht statt.
- **Keine automatisierte Entscheidung.** Die Anwendung trifft keine Entscheidungen mit rechtlicher oder ähnlich erheblicher Wirkung für betroffene Personen im Sinne des Art. 22 DSGVO. Sie ordnet Anliegen zu und bereitet sie strukturiert auf; jede Entscheidung trifft die Einrichtung.
- **Keine Werbung, kein Verkauf, keine Profilbildung.** Eine Verarbeitung zu eigenen Zwecken des Auftragnehmers findet nicht statt.

5.6 Auftragskontrolle und Unterstützung des Verantwortlichen

Der Auftragnehmer verarbeitet ausschließlich zu den vertraglich vereinbarten Zwecken und nach Weisung. Weisungen, die auf die Kenntnisnahme oder Änderung von Inhalten gerichtet sind, kann er nicht ausführen; eine Löschweisung kann er ausführen.

Er unterstützt den Auftraggeber bei Betroffenenanfragen, bei der Datenschutz-Folgenabschätzung und bei einer Konsultation der Aufsichtsbehörde. Anfragen betroffener Personen, die ihn unmittelbar erreichen, leitet er weiter und beantwortet sie nicht selbst.

Weitere Auftragsverarbeiter werden nur auf Grundlage der im Auftragsverarbeitungsvertrag erteilten allgemeinen Genehmigung eingesetzt, vertraglich auf ein gleichwertiges Schutzniveau verpflichtet und in einer aktuellen Übersicht geführt. Eingesetzt sind derzeit ausschließlich die Hetzner Online GmbH (Server und Datenbank) und die Brevo GmbH (Versand der inhaltsfreien Eingangsbenachrichtigung). Eine Übermittlung in Drittländer findet nicht statt.

[Ort], den [Datum]

Unterschrift / Stempel Auftraggeber

DiggAI GmbH (i. Gr.) · Margarete-Böhme-Str. 3 · 25813 Husum · Geschäftsführer: Dr. med. Christian Klaproth