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

Auftragsverarbeitungsvertrag

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag · Art. 28 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.

zwischen

[Name der Praxis / des MVZ]
[Straße, Hausnummer]
[PLZ, Ort]
vertreten durch [Name, Funktion]

– nachfolgend „Verantwortlicher" –

und

DiggAI GmbH (i. Gr.)
Margarete-Böhme-Str. 3
25813 Husum
vertreten durch den Geschäftsführer Dr. med. Christian Klaproth

– nachfolgend „Auftragsverarbeiter" –

– gemeinsam auch „Parteien" –

> Die Gesellschaft befindet sich in Gründung. Bis zur notariellen Beurkundung des Gesellschaftsvertrags ist Vertragspartner Dr. med. Christian Klaproth persönlich unter der vorstehenden Anschrift; danach die Vorgesellschaft, vertreten durch ihren Geschäftsführer. Eine Eintragung im Handelsregister liegt noch nicht vor; nach der Eintragung sind Registergericht und HRB-Nummer hier nachzutragen. Wortgleich in Impressum, Datenschutzerklärung und AGB — nach der Beurkundung entfällt an allen vier Stellen derselbe Halbsatz.

Präambel

Der Auftragsverarbeiter betreibt unter der Bezeichnung „DiggAI" einen Dienst zur verschlüsselten Übermittlung von Nachrichten und Dokumenten zwischen Patientinnen und Patienten und dem Verantwortlichen (nachfolgend „Dienst"). Grundlage ist der zwischen den Parteien geschlossene Hauptvertrag vom [Datum].

Der Dienst ist so ausgestaltet, dass Inhalte bereits auf dem Endgerät der absendenden Person verschlüsselt werden und ausschließlich mit dem privaten Schlüssel des Verantwortlichen entschlüsselt werden können. Der Auftragsverarbeiter hat zu keinem Zeitpunkt Zugriff auf die Inhalte der übermittelten Daten. Ob das verschlüsselte Datenpaket für den Auftragsverarbeiter ein personenbezogenes Datum ist, wird rechtlich unterschiedlich beurteilt. Die Parteien legen sich darauf nicht fest. Sie schließen diesen Vertrag **vorsorglich** und behandeln Entgegennahme, Zwischenspeicherung, Bereitstellung zur Abholung und Löschung der verschlüsselten Datenpakete sowie die damit verbundenen Verkehrs- und Metadaten wie eine Verarbeitung im Auftrag — unabhängig davon, wie die Rechtsfrage zu beantworten ist. Aus dem Abschluss dieses Vertrags kann kein Anerkenntnis hergeleitet werden.

Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien und ergänzt den Hauptvertrag. Er geht diesem im Konfliktfall in datenschutzrechtlicher Hinsicht vor.

§ 1 Gegenstand, Art, Zweck und Dauer der Verarbeitung

1.1 Gegenstand der Verarbeitung ist die Bereitstellung und der Betrieb des Dienstes zur verschlüsselten Übermittlung von Patientendaten an den Verantwortlichen (Online-Übermittlung).

1.2 Nicht Gegenstand dieses Vertrags ist der weitere vom Dienst angebotene Weg, bei dem Patientinnen und Patienten ihre Angaben als PDF-Dokument ausdrucken und in der Einrichtung des Verantwortlichen vorlegen. Bei diesem Weg werden die Angaben ausschließlich auf dem Endgerät der betroffenen Person erfasst, gespeichert und aufbereitet; eine Übertragung an die Systeme des Auftragsverarbeiters findet nicht statt. Insoweit liegt keine Verarbeitung im Auftrag vor.

1.3 Die Verarbeitung umfasst im Einzelnen:

- die Entgegennahme verschlüsselter Datenpakete von Endgeräten der Patientinnen und Patienten;
- die Vorhaltung dieser Pakete zur Abholung durch den Verantwortlichen. Der Dienst ist ein Abholdienst: Der Verantwortliche ruft die für ihn bestimmten Pakete mit seinem Schlüssel selbst ab. Eine inhaltliche Weiterleitung an ein anderes System findet nicht statt;
- die Benachrichtigung des Verantwortlichen über den Eingang eines Pakets an die von ihm hinterlegte Adresse; die Benachrichtigung enthält keine Inhaltsdaten;
- die Löschung des Datenpakets nach der Abholung, spätestens mit Ablauf der Vorhaltefrist nach § 8;
- die Verwaltung der Registrierungs- und Zugangsdaten des Verantwortlichen sowie des zugehörigen öffentlichen Schlüssels;
- die Protokollierung technischer Vorgänge zum Zweck des Betriebs, der Sicherheit und der Nachvollziehbarkeit der Zustellung.

1.4 Zweck der Verarbeitung ist ausschließlich die Übermittlung der Daten an den Verantwortlichen. Eine Verarbeitung zu eigenen Zwecken des Auftragsverarbeiters, insbesondere zu Zwecken der Werbung, der Profilbildung, der Weitergabe an Dritte oder des Trainings von Systemen künstlicher Intelligenz, findet nicht statt.

1.5 Die Entschlüsselung der Inhalte ist ausschließlich dem Verantwortlichen mittels des ihm zugeordneten privaten Schlüssels möglich. Der Auftragsverarbeiter hat keinen Zugriff auf diesen Schlüssel und ist technisch nicht in der Lage, die Inhalte zur Kenntnis zu nehmen. Einzelheiten der Schlüsselerzeugung und -verwahrung regelt Anlage 1.

1.6 Sprachverarbeitende Funktionen des Dienstes laufen ausschließlich auf dem Endgerät der nutzenden Person oder auf einem Rechner in den Räumen des Verantwortlichen. Eine Übermittlung von Inhalten an einen Anbieter von Sprachmodellen findet nicht statt; ein solcher Anbieter ist nicht eingebunden.

1.7 Die Verarbeitung findet ausschließlich in Rechenzentren innerhalb der Europäischen Union statt. Verarbeitungsorte sind in Anlage 2 im Einzelnen benannt. Eine Übermittlung in ein Drittland oder an eine internationale Organisation erfolgt nicht; sie bedürfte der vorherigen dokumentierten Weisung des Verantwortlichen und der Einhaltung der Art. 44 ff. DSGVO.

1.8 Die Anforderungen des § 393 SGB V an die Verarbeitung von Sozial- und Gesundheitsdaten im Wege des Cloud-Computings setzen voraus, dass ein Cloud-Computing-Dienst im Sinne des § 384 Nr. 5 SGB V vorliegt. Nach der Ausgestaltung des Dienstes nimmt der Auftragsverarbeiter eine verschlüsselte Sendung entgegen, hält sie zur Abholung durch den Verantwortlichen vor und löscht sie nach der Abholung, spätestens nach Ablauf der Frist des § 8. Er verschafft dem Verantwortlichen keinen Zugang zu skalierbaren, elastisch geteilten Rechenressourcen und verarbeitet zu keinem Zeitpunkt lesbare Inhalte.

1.9 Ist der Dienst ganz oder in einzelnen Bestandteilen als Cloud-Computing-Dienst im Sinne des § 384 Nr. 5 SGB V einzuordnen, weist der Auftragsverarbeiter für den betroffenen Bestandteil ein aktuelles C5-Testat oder ein Testat beziehungsweise Zertifikat nach einem Standard mit vergleichbarem oder höherem Sicherheitsniveau nach; § 393 SGB V lässt einen gleichwertigen Standard ausdrücklich zu.

1.10 Für die eingesetzte Infrastruktur liegen die Nachweise bereits vor: Die **Hetzner Online GmbH** verfügt über ein **BSI-C5-Testat Typ 2** sowie über eine Zertifizierung nach **ISO/IEC 27001:2022**; der Geltungsbereich umfasst sämtliche Hosting-Dienste und Rechenzentren einschließlich des Verarbeitungsstandorts **Helsinki**. Der Auftragsverarbeiter legt diese Nachweise auf Verlangen vor. Offen ist allein, ob darüber hinaus die Anwendungsschicht des Auftragsverarbeiters einen eigenen Nachweis erfordert; hierfür ist die Einordnung nach Ziffer 1.8 maßgeblich.

> Prüfauftrag an den Rechtsberater. Vor Verwendung ist zu klären, ob DiggAI ein Cloud-Computing-Dienst im Sinne des § 384 Nr. 5 SGB V ist. Die Definition ist wortgleich mit Art. 6 Nr. 30 der NIS-2-Richtlinie (nicht Art. 4 — im Entwurf 6 zunächst falsch zitiert, korrigiert am 01.08.2026) und stellt unter anderem auf Skalierbarkeit, geteilte Nutzung und Elastizität ab; die Auslegung ist bislang nicht gefestigt. Zu prüfen ist getrennt für (1) Entgegennahme, Vorhaltung zur Abholung und Löschung der verschlüsselten Pakete und (2) das Empfängerverzeichnis nebst Kontoverwaltung. **Gegenüber Entwurf 5 hat sich die Tatsachengrundlage geändert:** dort war unterstellt, die Sendung werde unmittelbar weitergeleitet und anschließend gelöscht. Tatsächlich wird sie bis zur Abholung, längstens 30 Tage, vorgehalten. Die Argumentation zu § 384 Nr. 5 SGB V muss auf dieser Grundlage neu bewertet werden. Zu beachten ist dabei, dass die Infrastrukturebene bereits testiert ist (Ziffer 1.10); die Frage verengt sich damit darauf, ob die Anwendungsschicht des Auftragsverarbeiters ein eigenes Cloud-System im Sinne der Norm ist. **Vorarbeit dazu liegt vor:** `docs/recht/PRUEFVERMERK_384-393_SGB-V_2026-08-01.md` trägt Wortlaut, Erwägungsgrund 33 und die Argumente beider Seiten zusammen. Ergebnis in einem Satz: Für das Empfängerverzeichnis ist die Frage nicht entscheidungserheblich, weil dort keine Sozial- oder Gesundheitsdaten liegen; für den Abholdienst sprechen die Merkmale „Rechenressourcen", „Verwaltung auf Abruf" und „Elastizität" gegen eine Einordnung als Cloud-Dienst, die Selbstbezeichnung als Software-as-a-Service in den AGB jedoch dafür. Normadressat ist die Praxis: Ohne Klärung trägt sie das Risiko, nicht der Auftragsverarbeiter.

1.11 Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags. Dieser Vertrag endet automatisch mit dessen Beendigung; § 8 bleibt unberührt.

§ 2 Art der Daten und Kategorien betroffener Personen

2.1 Verschlüsselt übermittelte Inhaltsdaten, die vom Auftragsverarbeiter nicht eingesehen werden können. Diese können nach Angabe des Verantwortlichen insbesondere enthalten: Stammdaten (Name, Geburtsdatum, Anschrift, Kontaktdaten), Versichertendaten, Angaben zu Beschwerden und Anamnese, Befunde, Vorbefunde und Bilddateien, Medikationsangaben sowie sonstige Gesundheitsdaten im Sinne des Art. 9 Abs. 1 DSGVO. Die Aufzählung dient dem Verzeichnis der Verarbeitungstätigkeiten des Verantwortlichen; dem Auftragsverarbeiter ist der Inhalt nicht bekannt.

2.2 Im Klartext verarbeitete Daten: die Verzeichniskennung des Empfängers als kryptografisch abgeleiteter Prüfwert, Zeitpunkt des Eingangs und der Abholung, Größe des Datenpakets, Abhol- und Ablaufstatus, technische Verbindungs- und Protokolldaten einschließlich IP-Adresse sowie die für die Eingangsbenachrichtigung hinterlegte E-Mail-Adresse. Diese Daten können mittelbar einen Personenbezug aufweisen.

2.3 Kein Zugriffsprotokoll des Webservers. Der Auftragsverarbeiter führt kein dauerhaftes Zugriffsprotokoll: Aufgerufene Adressen, Referrer, Browsertyp und Betriebssystem werden nicht gespeichert. IP-Adressen und technische Verbindungsdaten werden beim bloßen Aufruf der Anwendung nur flüchtig verarbeitet, solange die Verbindung besteht. Dauerhaft protokolliert werden ausschließlich die in Ziffer 2.2 genannten Vorgänge im geschützten Bereich — insbesondere Abholung und Löschung durch den Verantwortlichen — samt dessen IP-Adresse. Diese Protokolle enthalten keine Inhaltsdaten und werden nach 90 Tagen automatisch gelöscht (Ziffer 8.4). Wird später ein Zugriffsprotokoll eingerichtet, ist dieser Vertrag vorher zu ändern.

2.4 Die Betriebsstättennummer des Verantwortlichen wird nicht neben dem Datenpaket gespeichert. Der Empfängerbezug wird ausschließlich als kryptografisch abgeleiteter Prüfwert abgelegt, sodass aus dem Datenbestand keine Verbindung zwischen einer bestimmten Einrichtung und einem bestimmten Datenpaket hergestellt werden kann.

2.5 Kategorien betroffener Personen sind Patientinnen und Patienten des Verantwortlichen, deren gesetzliche Vertreter, Betreuer und Angehörige, soweit diese den Dienst nutzen, Bewohnerinnen und Bewohner sowie Pflegekräfte einer angebundenen Einrichtung sowie Beschäftigte des Verantwortlichen, soweit sie den Dienst bedienen.

§ 3 Weisungsrecht des Verantwortlichen

3.1 Der Auftragsverarbeiter verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Dieser Vertrag einschließlich seiner Anlagen stellt die Grunddokumentation der Weisungen dar. Einzelweisungen bedürfen der Textform und sind vom Auftragsverarbeiter zu dokumentieren.

3.2 Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, hat er den Verantwortlichen unverzüglich darauf hinzuweisen. Er ist berechtigt, die Ausführung der Weisung bis zu deren Bestätigung oder Änderung auszusetzen (Art. 28 Abs. 3 Satz 3 DSGVO).

3.3 Die Parteien sind sich einig, dass Weisungen, die sich auf die Inhalte der verschlüsselten Datenpakete beziehen – etwa deren Berichtigung, Einsichtnahme, Auswertung oder inhaltsbezogene Sortierung –, vom Auftragsverarbeiter technisch nicht ausgeführt werden können. Der Verantwortliche wird solche Weisungen nicht erteilen. Eine Weisung zur vorzeitigen Löschung eines Datenpakets kann der Auftragsverarbeiter dagegen ausführen.

3.4 Ansprechpartner für Weisungen sind auf Seiten des Verantwortlichen [Name, Funktion, Kontakt], auf Seiten des Auftragsverarbeiters [Name, Funktion, Kontakt].

3.5 Im Rahmen der Störungsbearbeitung greift der Auftragsverarbeiter nur auf technische Protokoll- und Zustelldaten zu. Ein Zugriff auf Inhalte, eine Fernwartung von Systemen des Verantwortlichen und die Anforderung von Bildschirmaufnahmen mit Patientenbezug finden nicht statt. Übermittelt der Verantwortliche gleichwohl personenbezogene Daten im Rahmen einer Supportanfrage, werden diese nach Abschluss des Vorgangs, spätestens nach [XX] Tagen gelöscht.

§ 4 Vertraulichkeit und ärztliche Schweigepflicht

4.1 Der Auftragsverarbeiter setzt zur Verarbeitung ausschließlich Personen ein, die zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Die Verpflichtung besteht auch nach Beendigung der Tätigkeit fort.

4.2 Der Auftragsverarbeiter und alle bei ihm tätigen Personen werden ausdrücklich als sonstige mitwirkende Personen im Sinne des § 203 Abs. 3 Satz 2 StGB zur Wahrung fremder Geheimnisse verpflichtet. Die Verpflichtungserklärung ist diesem Vertrag als Anlage 3 beigefügt und wird für jede eingesetzte Person gesondert unterzeichnet. Der Auftragsverarbeiter weist die Verpflichtungen auf Verlangen nach.

4.3 Der Auftragsverarbeiter verpflichtet auch von ihm eingesetzte Unterauftragsverarbeiter nach § 203 Abs. 4 Satz 2 Nr. 1 StGB in gleicher Weise.

4.4 Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn Dritte – insbesondere Strafverfolgungs- oder sonstige Behörden – Zugriff auf die verarbeiteten Daten verlangen, soweit dem keine gesetzliche Verpflichtung entgegensteht. Er weist die verlangende Stelle darauf hin, dass er die Inhalte nicht entschlüsseln kann und über keinen Schlüssel verfügt.

§ 5 Technische und organisatorische Maßnahmen

5.1 Der Auftragsverarbeiter trifft die zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus erforderlichen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. Der Stand dieser Maßnahmen zum Zeitpunkt des Vertragsschlusses ist in Anlage 1 dokumentiert.

5.2 Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragsverarbeiter darf sie anpassen, sofern das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren und

dem Verantwortlichen mitzuteilen.

5.3 Der Auftragsverarbeiter überprüft die Wirksamkeit der Maßnahmen regelmäßig, mindestens jährlich, sowie anlassbezogen bei wesentlichen Änderungen der Verarbeitung.

§ 6 Unterauftragsverarbeiter

6.1 Der Verantwortliche erteilt die allgemeine Genehmigung zur Beauftragung der in Anlage 2 aufgeführten Unterauftragsverarbeiter.

6.2 Der Auftragsverarbeiter informiert den Verantwortlichen mindestens vier Wochen vor der Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters in Textform. Der Verantwortliche kann innerhalb von zwei Wochen ab Zugang aus wichtigem, datenschutzrechtlich begründetem Anlass widersprechen. Im Fall eines berechtigten Widerspruchs, dem nicht abgeholfen werden kann, steht dem Verantwortlichen ein Sonderkündigungsrecht des Hauptvertrags zu.

6.3 Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die den Pflichten aus diesem Vertrag entsprechen, und haftet für dessen Verhalten wie für eigenes.

6.4 Nebenleistungen ohne unmittelbaren Bezug zur Verarbeitung – etwa Telekommunikationsdienste, Post- und Transportdienste, Reinigung, Bewachung oder die Entsorgung von Datenträgern – gelten nicht als Unterauftragsverarbeitung. Der Auftragsverarbeiter stellt auch insoweit angemessenen Schutz sicher.

§ 7 Unterstützung des Verantwortlichen

7.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten Maßnahmen bei der Erfüllung von Betroffenenrechten nach Kapitel III DSGVO. Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, leitet dieser das Anliegen unverzüglich an den Verantwortlichen weiter und beantwortet es nicht selbst.

7.2 Die Parteien stellen klar, dass Auskunfts-, Berichtigungs- und Löschungsverlangen, die sich auf die verschlüsselten Inhalte beziehen, nur vom Verantwortlichen erfüllt werden können, da nur dieser über den zur Entschlüsselung erforderlichen Schlüssel verfügt.

7.3 Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntniserlangung, damit der Verantwortliche die Frist des Art. 33 Abs. 1 DSGVO einhalten kann. Die Meldung enthält die nach Art. 33 Abs. 3 DSGVO erforderlichen Angaben, soweit dem Auftragsverarbeiter bekannt. Als meldepflichtiges Ereignis gilt ausdrücklich auch der Verlust der Verfügbarkeit noch nicht abgeholter Datenpakete.

7.4 Der Auftragsverarbeiter unterstützt den Verantwortlichen bei Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO und einer etwaigen vorherigen Konsultation nach Art. 36 DSGVO, insbesondere durch Bereitstellung der erforderlichen Informationen über den Dienst.

7.5 Ansprechpartner für den Datenschutz beim Auftragsverarbeiter ist [Name, Anschrift, E-Mail].

> Prüfauftrag an den Rechtsberater. Ob der Auftragsverarbeiter einen Datenschutzbeauftragten zu bestellen hat, 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. Entwurf 5 sagte an dieser Stelle einen bestellten Datenschutzbeauftragten zu; das trifft derzeit nicht zu und wurde deshalb auf einen Ansprechpartner zurückgenommen.

§ 8 Löschung

8.1 Ein Datenpaket wird zur Abholung durch den Verantwortlichen vorgehalten. Mit der Abholung und der Bestätigung des Empfangs wird der Inhalt auf den Systemen des Auftragsverarbeiters gelöscht.

8.2 Wird ein Datenpaket nicht abgeholt, wird es spätestens 30 Tage nach Eingang automatisch und ohne weiteres Zutun gelöscht. Diese Frist ist Teil der Systemauslegung und kann durch Weisung weder verlängert noch verkürzt werden. Nach Fristablauf ist der Inhalt endgültig verloren; eine Wiederherstellung ist auch dem Auftragsverarbeiter nicht möglich.

8.3 Für den verschlüsselten Schlüsselaustausch zwischen Geräten des Verantwortlichen gilt eine Frist von 30 Tagen nach Abholung, längstens 90 Tage.

8.4 Protokoll- und Verkehrsdaten nach § 2 Abs. 2 werden nach 90 Tagen gelöscht, soweit sie nicht zur Abwehr konkreter Angriffe auf die Systeme oder zur Erfüllung gesetzlicher Aufbewahrungspflichten benötigt werden. Ein inhaltsleerer Nachweiseintrag über die Zustellung wird nach 30 Tagen vollständig gelöscht.

8.5 Nach Beendigung des Vertrags löscht der Auftragsverarbeiter sämtliche im Auftrag verarbeiteten Daten einschließlich vorhandener Kopien innerhalb von 30 Tagen, sofern nicht nach Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung besteht. Die Löschung ist dem Verantwortlichen auf Verlangen in Textform zu bestätigen.

8.6 Eine Rückgabe von Inhaltsdaten bei Vertragsende kommt nicht in Betracht: Der Verantwortliche kann alle für ihn bestimmten Pakete jederzeit selbst abholen, und der Auftragsverarbeiter könnte sie nur als Chiffrat herausgeben. Der Verantwortliche wird darauf hingewiesen, noch nicht abgeholte Pakete vor Vertragsende abzurufen.

8.7 Sicherungskopien enthalten Inhalte ausschließlich in verschlüsselter Form und werden nach dem in Anlage 1 beschriebenen Verfahren überschrieben.

§ 9 Nachweise und Kontrollrechte

9.1 Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO erforderlich sind, und ermöglicht Überprüfungen einschließlich Inspektionen.

9.2 Der Nachweis kann geführt werden durch aktuelle Testate, Zertifikate oder Berichte unabhängiger Stellen, durch eine geeignete Zertifizierung nach Art. 42 DSGVO oder durch die Beantwortung eines schriftlichen Prüfkatalogs. Der Auftragsverarbeiter hält hierfür eine aktuelle Dokumentation der Maßnahmen nach Anlage 1 bereit.

9.3 Reicht dies im Einzelfall nicht aus, ist der Verantwortliche berechtigt, nach rechtzeitiger Ankündigung von mindestens zwei Wochen während der üblichen Geschäftszeiten eine Prüfung vor Ort durchzuführen oder durch einen zur Verschwiegenheit verpflichteten, nicht mit dem Auftragsverarbeiter im Wettbewerb stehenden Prüfer durchführen zu lassen. Die Prüfung darf den Betriebsablauf nicht unangemessen beeinträchtigen.

9.4 Der Auftragsverarbeiter führt ein Verzeichnis der im Auftrag durchgeführten Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und legt es dem Verantwortlichen auf Verlangen vor.

§ 10 Haftung und Schlussbestimmungen

10.1 Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO. Im Innenverhältnis haften die Parteien nach den Regelungen des Hauptvertrags.

10.2 Für Schäden, die aus dem Verlust des privaten Schlüssels des Verantwortlichen oder aus dem Umgang mit bereits entschlüsselten Inhalten auf dessen Systemen entstehen, haftet der Auftragsverarbeiter nicht.

10.3 Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform; dies gilt auch für die Abbedingung dieser Klausel. Der Vertrag kann nach Art. 28 Abs. 9 DSGVO in elektronischem Format geschlossen werden.

10.4 Sollte eine Bestimmung dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien werden die unwirksame Bestimmung durch eine wirksame ersetzen, die dem wirtschaftlichen Zweck am nächsten kommt.

10.5 Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist, soweit zulässig, der Sitz des Auftragsverarbeiters.

10.6 Bestandteil dieses Vertrags sind die Anlagen 1 bis 3.

[Ort], den [Datum]

Verantwortlicher – [Praxis / MVZ]

Auftragsverarbeiter – DiggAI GmbH (i. Gr.)

Anlage 1 – Technische und organisatorische Maßnahmen

Stand: 01.08.2026 · Diese Anlage wird bei wesentlichen Änderungen fortgeschrieben.

> Hinweis zum Entwurfsstand: Die mit eckigen Klammern gekennzeichneten Stellen sind noch offen. Die übrigen Angaben entsprechen dem am 01.08.2026 im Quellcode geprüften Stand.

1. Grundprinzip

Inhalte werden auf dem Endgerät der absendenden Person hybrid verschlüsselt: AES-256-GCM für die Inhalte, X25519 für die Kapselung des Sitzungsschlüssels. Auf der Infrastruktur des Auftragsverarbeiters liegen zu keinem Zeitpunkt lesbare Patientendaten.

Das Schlüsselpaar des Verantwortlichen wird lokal auf dessen System erzeugt; ausschließlich der öffentliche Schlüssel wird übertragen und im Verzeichnis veröffentlicht. Der private Schlüssel verlässt das System des Verantwortlichen nicht und ist dort so abgelegt, dass er durch die Anwendung nicht ausgelesen werden kann.

Der Empfängerbezug wird nicht im Klartext gespeichert, sondern als kryptografisch abgeleiteter Prüfwert. Die Datenbank enthält daher keine Verbindung zwischen einer bestimmten Einrichtung und einem bestimmten Datenpaket.

Registrierung und Schlüsseländerungen werden über einen vom Verantwortlichen unabhängigen Kanal bestätigt; dabei wird der Fingerabdruck des öffentlichen Schlüssels abgeglichen. Die absendende Person erhält den Fingerabdruck vor dem Versand angezeigt. Freigaben und Schlüsseländerungen werden protokolliert.

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Bereich	Maßnahme
Zutrittskontrolle	Betrieb in einem zertifizierten Rechenzentrum der Hetzner Online GmbH, Standort Helsinki, Finnland; Zutritt nur für autorisiertes Personal des Rechenzentrumsbetreibers; Vereinzelungsanlage, Videoüberwachung, Protokollierung.
Zugangskontrolle	Individuelle Benutzerkonten ohne gemeinsam genutzte Zugänge; Zwei-Faktor-Authentifizierung für sämtliche administrativen Zugriffe; automatische Sperrung nach Fehlversuchen. Der Verantwortliche selbst authentisiert sich nicht über ein Kennwort, sondern über den Besitz seines Schlüssels.
Zugriffskontrolle	Rollenbasiertes Berechtigungskonzept nach dem Prinzip der geringsten Rechte; administrative Zugriffe werden protokolliert; ein Zugriff auf Inhaltsdaten ist technisch ausgeschlossen, da diese ausschließlich verschlüsselt vorliegen. Schutz des Schlüsselverzeichnisses durch ein dokumentiertes Freigabeverfahren.
Trennungskontrolle	Mandantentrennung je Verantwortlichem auf Anwendungs- und Datenbankebene; getrennte Umgebungen für Entwicklung, Test und Produktion; keine Verwendung von Echtdaten in Test- und Entwicklungsumgebungen.

Bereich	Maßnahme
Pseudonymisierung	Verzicht auf Klartext-Identifikatoren betroffener Personen in Protokolldaten; Verwendung technischer Vorgangskennungen; Empfängerbezug ausschließlich als abgeleiteter Prüfwert.

3. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Bereich	Maßnahme
Weitergabekontrolle	Transportverschlüsselung nach TLS [Version] für sämtliche Verbindungen; Ende-zu-Ende-Verschlüsselung der Inhalte mit AES-256-GCM und X25519; Vorhaltung und Herausgabe ausschließlich als Chiffrat; Zertifikatsverwaltung und Schlüsselrotation nach dokumentiertem Verfahren.
Eingabekontrolle	Protokollierung aller Eingangs-, Abhol- und Löschvorgänge mit Zeitstempel; Protokolle sind gegen nachträgliche Veränderung geschützt und enthalten keine Inhaltsdaten. Ein Zugriffsprotokoll des Webservers wird nicht geführt (Ziffer 2.3).
Authentizität	Auslieferung des clientseitigen Programmcodes über HTTPS mit restriktiver Content-Security-Policy; Subresource Integrity und Veröffentlichung von Prüfsummen der ausgelieferten Codeversionen [geplant / umgesetzt — vor Verwendung prüfen].

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

Bereich	Maßnahme
Verfügbarkeit	Unterbrechungsfreie Stromversorgung und Netzersatzanlage im Rechenzentrum; Monitoring mit Alarmierung; Schutz gegen Überlastangriffe.
Datensicherung	Verschlüsselte Sicherung [Rhythmus]; getrennte Aufbewahrung der Sicherungen; regelmäßige Wiederherstellungstests mindestens [jährlich].
Nicht abgeholte Pakete	Ein Datenpaket bleibt bis zur Abholung, längstens 30 Tage, vorgehalten und wird danach automatisch gelöscht. Automatische Zustellversuche an ein System des Verantwortlichen finden nicht statt; der Verantwortliche wird über den Eingang benachrichtigt und ruft das Paket selbst ab.
Schlüsselverlust	Verliert der Verantwortliche seinen privaten Schlüssel, ist eine Entschlüsselung noch nicht abgeholter Sendungen endgültig nicht mehr möglich. Der Auftragsverarbeiter kann den Schlüssel nicht wiederherstellen. Der Verantwortliche ist zur sicheren Verwahrung verpflichtet und erhält hierzu bei der Registrierung Hinweise sowie die Möglichkeit, eine Sicherung anzulegen.

5. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

Bereich	Maßnahme
Datenschutzmanagement	Benannter Ansprechpartner für den Datenschutz; Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO; dokumentiertes Löschkonzept mit automatischer Ausführung; Verfahren zur Behandlung von Datenschutzverletzungen mit definierten Meldewegen.
Auftragskontrolle	Schriftliche Verträge mit allen Unterauftragsverarbeitern; Prüfung vor Beauftragung; Führung einer Übersicht nach Anlage 2.
Überprüfung	Interne Überprüfung der Maßnahmen mindestens jährlich sowie anlassbezogen; Schwachstellen- und Patchmanagement; ein externer Penetrationstest wurde durchgeführt, die bestätigten Befunde wurden behoben [Datum und Prüfer vor Verwendung eintragen]; C5-Testat oder gleichwertiger Nachweis, soweit § 393 SGB V nach der Einordnung des Dienstes gemäß § 384 Nr. 5 SGB V anwendbar ist [Typ und Geltungsbereich: _____].

Bereich	Maßnahme
Sensibilisierung	Verpflichtung aller Beschäftigten auf Vertraulichkeit und § 203 StGB vor Aufnahme der Tätigkeit; Schulung mindestens jährlich.

Anlage 2 – Unterauftragsverarbeiter

Stand: 01.08.2026. Änderungen werden dem Verantwortlichen nach § 6 Abs. 2 dieses Vertrags mitgeteilt.

Unternehmen	Anschrift / Sitz	Leistung	Ort der Verarbeitung	Zugang zu Inhalten
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen	Server- und Rechenzentrumsleistungen, Speicher, Datenbank	Helsinki, Finnland	nein – ausschließlich Chiffrat
Brevo GmbH (vormals Sendinblue)	Köpenicker Str. 126, 10179 Berlin	Versand der Eingangsbenachrichtigung per E-Mail	Europäische Union	nein – die Benachrichtigung enthält keine Inhaltsdaten

Weitere Unterauftragsverarbeiter werden nicht eingesetzt. Insbesondere ist kein Dienstleister für den Versand von SMS, für Namensauflösung, für Erreichbarkeitsüberwachung oder für die Zahlungsabwicklung eingebunden. Antworten an Patientinnen und Patienten versendet der Verantwortliche über ein eigenes Gerät.

Sämtliche vorstehenden Unternehmen verarbeiten ausschließlich innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums. Mit jedem Unternehmen besteht ein Vertrag nach Art. 28 DSGVO sowie eine Verpflichtung nach § 203 Abs. 4 Satz 2 Nr. 1 StGB, soweit ein Zugriff auf Daten technisch nicht ausgeschlossen ist.

Anlage 3 – Verpflichtung auf die Geheimhaltung nach § 203 StGB

Muster – für jede eingesetzte Person gesondert zu unterzeichnen

Frau / Herr [Vorname, Name], tätig für die DiggAI GmbH (i. Gr.) als [Funktion], wird hiermit als sonstige mitwirkende Person im Sinne des § 203 Abs. 3 Satz 2 StGB zur Geheimhaltung verpflichtet.

Belehrung

Im Rahmen meiner Tätigkeit kann ich Kenntnis von fremden Geheimnissen erlangen, die einem Angehörigen eines Heilberufs anvertraut oder sonst bekannt geworden sind. Dazu gehören insbesondere Angaben über Erkrankungen, Behandlungen, persönliche Verhältnisse sowie bereits die Tatsache, dass eine bestimmte Person Patientin oder Patient einer bestimmten Praxis ist.

Ich bin darüber belehrt worden, dass die unbefugte Offenbarung solcher Geheimnisse nach § 203 Abs. 4 StGB mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft werden kann. Die Verpflichtung gilt gegenüber jedermann, auch gegenüber Familienangehörigen, und besteht nach dem Ende meiner Tätigkeit unbefristet fort.

Erklärung

Ich verpflichte mich, fremde Geheimnisse im Sinne des § 203 StGB nicht unbefugt zu offenbaren oder zu verwerten. Ich werde Daten, zu denen ich Zugang erhalte, ausschließlich im Rahmen meiner dienstlichen Aufgaben und nur auf Weisung verarbeiten. Ich habe eine Ausfertigung dieser Verpflichtung erhalten.

[Ort], den [Datum]

Verpflichtete Person

Für die DiggAI GmbH (i. Gr.)