

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

Beispielfassung. So sieht der Vertrag aus, den Sie mit Mirwena schließen. Zum Vertragsschluss wird er mit Ihren Angaben ausgefüllt; die verbindliche Fassung erhalten Sie vor der Unterzeichnung.

Verantwortlicher (Auftraggeber) [Name der Praxis], [Anschrift], vertreten durch [Name]

Auftragsverarbeiter (Auftragnehmer) Achim Krämer, Böckemeyerskamp 20, 49479 Ibbenbüren, Deutschland

1. Gegenstand und Dauer

Gegenstand ist die Bereitstellung und der Betrieb der Software **Mirwena** zur digitalen Erfassung von Anamnese- und Befundbögen. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich weisungsgebunden für den Verantwortlichen.

Die Laufzeit entspricht der Laufzeit des zugrunde liegenden Hauptvertrags. Der Vertrag endet automatisch mit dessen Beendigung.

2. Art und Zweck der Verarbeitung

Erhebung, Speicherung, Anzeige, Export und Löschung von Anamnesedaten, die Patientinnen und Patienten über einen personalisierten Zugangslink selbst eingeben, sowie der ergänzenden Behandlerdokumentation.

Zweck ist ausschließlich die Vorbereitung und Dokumentation der Behandlung durch den Verantwortlichen. Eine Nutzung zu eigenen Zwecken des Auftragnehmers, insbesondere zu Analyse-, Trainings- oder Werbezwecken, findet nicht statt.

Zweckbestimmung: Mirwena ist ein Dokumentationswerkzeug. Es trifft keine diagnostischen Aussagen, berechnet keine medizinischen Scores und gibt keine Behandlungsempfehlungen. Es ist kein Medizinprodukt im Sinne der MDR.

3. Art der Daten und Kreis der Betroffenen

Betroffene: Patientinnen und Patienten des Verantwortlichen sowie dessen Beschäftigte, soweit sie Benutzerkonten haben.

Datenarten:

Kategorie	Felder
Stammdaten	Name, Geburtsdatum
Gesundheitsdaten (Art. 9 DSGVO)	Hauptproblem, Ziel, Tagesverlauf, bisherige Versuche, lindernde/verschlimmernde Faktoren, bekannte Erkrankungen, Medikamente, Vorerkrankungen-Checkliste, markierte Schmerzzonen, Angaben zur Lebensqualität, Angaben zum Schlaf, Behandlernetizen
Sonstige	digitale Unterschrift, Zeitstempel, Zugangstoken
Beschäftigtendaten	E-Mail-Adresse, Passwort-Hash, Rolle, 2FA-Geheimnis

Es werden **besondere Kategorien personenbezogener Daten** nach Art. 9 DSGVO verarbeitet. Der Verantwortliche stellt die Rechtsgrundlage sicher (i. d. R. Art. 9 Abs. 2 lit. h DSGVO i. V. m. der Behandlung).

4. Weisungen

Die Verarbeitung erfolgt ausschließlich auf dokumentierte Weisung des Verantwortlichen. Weisungen erfolgen in Textform an **kontakt@mirwena.de**.

Hält der Auftragnehmer eine Weisung für rechtswidrig, informiert er den Verantwortlichen unverzüglich und darf die Ausführung aussetzen.

5. Vertraulichkeit

Der Auftragnehmer setzt zur Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet und über die einschlägigen Datenschutzvorgaben belehrt wurden. Die Verpflichtung wirkt über das Ende der Tätigkeit hinaus.

6. Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Der Auftragnehmer unterhält die in **Anlage 1** beschriebenen Maßnahmen. Er darf sie fortentwickeln, solange das Schutzniveau nicht unterschritten wird.

7. Unterauftragsverarbeiter

Der Verantwortliche stimmt dem Einsatz folgender Unterauftragnehmer zu:

Unterauftragnehmer	Leistung	Ort der Verarbeitung
STRATO GmbH, Berlin	Server-, Datenbank- und Mailbetrieb	Deutschland

Ein gesonderter E-Mail-Versanddienst wird nicht eingesetzt. Die Benachrichtigungen an die Praxis verlässt derselbe Server, auf dem die Anwendung läuft, über den dort eingerichteten

Mailserver. Es kommt damit kein weiterer Unterauftragnehmer hinzu, und die Nachrichten verlassen die Infrastruktur der STRATO GmbH in Deutschland nicht.

Mit der STRATO GmbH besteht eine **Vereinbarung zur Auftragsverarbeitung nach Art. 28**

DSGVO: Sie ist Bestandteil deren AGB und kommt mit der Beauftragung zustande, eine gesonderte Unterzeichnung ist nicht erforderlich (<<https://www.strato.de/agb/avv/>>). Damit ist die Weitergabe der Pflichten an den Unterauftragnehmer nach Art. 28 Abs. 4 DSGVO abgedeckt.

Wechsel oder Ergänzungen teilt der Auftragnehmer mindestens **vier Wochen** vorher mit. Der Verantwortliche kann binnen zwei Wochen widersprechen; im Widerspruchsfall steht ihm ein Sonderkündigungsrecht zu.

Eine Verarbeitung außerhalb der EU/des EWR findet nur bei Vorliegen eines Angemessenheitsbeschlusses oder geeigneter Garantien nach Art. 46 DSGVO statt.

8. Unterstützungspflichten

Der Auftragnehmer unterstützt den Verantwortlichen im erforderlichen Umfang bei:

- Anfragen betroffener Personen nach Art. 15–22 DSGVO (Auskunft, Berichtigung, Löschung, Datenübertragbarkeit),
- der Meldung von Datenschutzverletzungen nach Art. 33/34 DSGVO,
- Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO.

Der Auftragnehmer meldet ihm bekannt gewordene Verletzungen des Schutzes personenbezogener Daten **unverzüglich, spätestens innerhalb von 24 Stunden** nach Kenntnis an den Verantwortlichen.

9. Löschung und Rückgabe

Nach Beendigung des Vertrags gibt der Auftragnehmer alle Daten nach Wahl des Verantwortlichen zurück oder löscht sie innerhalb von **30 Tagen**, einschließlich Sicherungskopien, und bestätigt dies in Textform.

Gesetzliche Aufbewahrungspflichten des Verantwortlichen – insbesondere die zehnjährige Aufbewahrungspflicht der Patientenakte nach § 630f Abs. 3 BGB – bleiben unberührt. Der Verantwortliche ist dafür verantwortlich, benötigte Befunde vor der Löschung zu exportieren.

10. Nachweise und Kontrollen

Der Auftragnehmer weist die Einhaltung der Pflichten auf Anfrage nach. Der Verantwortliche kann nach Ankündigung mit angemessener Frist Überprüfungen durchführen oder durch Dritte durchführen lassen.

11. Haftung

11.1 Verhältnis zu Art. 82 DSGVO

Die Haftung gegenüber betroffenen Personen richtet sich nach Art. 82 DSGVO und bleibt von den nachfolgenden Regelungen **unberührt**. Die Ziffern 11.2 bis 11.6 regeln ausschließlich das Verhältnis der Parteien untereinander, einschließlich des Ausgleichs nach Art. 82 Abs. 5 DSGVO.

11.2 Unbeschränkte Haftung

Unbeschränkt haften die Parteien bei Vorsatz und grober Fahrlässigkeit, bei der schuldhaften Verletzung von Leben, Körper oder Gesundheit, bei arglistigem Verschweigen eines Mangels, im Umfang einer übernommenen Garantie sowie in allen Fällen zwingender gesetzlicher Haftung.

11.3 Haftung bei einfacher Fahrlässigkeit

Bei einfacher Fahrlässigkeit haftet eine Partei nur für die Verletzung wesentlicher Vertragspflichten. Wesentlich ist eine Pflicht, deren Erfüllung die ordnungsgemäße Durchführung dieses Vertrags überhaupt erst ermöglicht und auf deren Einhaltung die andere Partei regelmäßig vertrauen darf; dazu gehören insbesondere die in **Anlage 1** beschriebenen Maßnahmen zum Schutz der Daten.

Die Haftung ist in diesen Fällen auf den bei Vertragsschluss vorhersehbaren, vertragstypischen Schaden begrenzt.

Eine weitergehende Haftung bei einfacher Fahrlässigkeit ist ausgeschlossen.

11.4 Versicherung

Der Auftragnehmer erteilt dem Verantwortlichen auf Anfrage in Textform Auskunft darüber, ob und in welcher Höhe eine Haftpflichtversicherung für Vermögensschäden aus der Verarbeitung personenbezogener Daten besteht.

11.5 Freistellung

Der Verantwortliche stellt den Auftragnehmer von Ansprüchen Dritter und von Bußgeldern frei, die darauf beruhen, dass für die Verarbeitung keine Rechtsgrundlage bestand, die betroffenen Personen nicht ordnungsgemäß informiert wurden oder eine Weisung erteilt wurde, deren Rechtswidrigkeit der Auftragnehmer nicht erkennen musste. Das gilt nicht, soweit der Auftragnehmer die betreffenden Umstände zu vertreten hat.

11.6 Mitwirkung und Mitverschulden

Der Verantwortliche trägt dafür Sorge, dass Zugangsdaten seiner Beschäftigten geheim gehalten, Konten ausgeschiedener Beschäftigter unverzüglich gelöscht und die angebotene Zwei-Faktor-Anmeldung genutzt wird. Verstöße hiergegen sind im Rahmen des § 254 BGB zu berücksichtigen.

12. Zustandekommen und Form

Der Vertrag wird **elektronisch** geschlossen. Art. 28 Abs. 9 DSGVO lässt das ausdrücklich zu; ein Ausdruck ist nicht erforderlich, und ein eingescannter Ausdruck wäre die schwächste der möglichen Formen – er belegt weder Zeitpunkt noch Urheberschaft.

Ablauf:

1. Der Auftragnehmer trägt die Angaben der Praxis ein und **signiert zuerst**.
2. Die Praxis erhält das bereits gegengezeichnete Dokument und signiert elektronisch. Ein Rücklauf genügt.
3. **Erst danach werden Zugänge angelegt**. Vor der Signatur verarbeitet der Auftragnehmer keine Patientendaten des Verantwortlichen – damit kann der Zustand „Praxis arbeitet schon, Vertrag fehlt noch“ nicht entstehen.
4. Beide Seiten erhalten das signierte Dokument samt Prüfprotokoll des Signaturdienstes. Der Verantwortliche bewahrt es zu seiner Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO auf.

Der Signaturdienst verarbeitet dabei Namen und E-Mail-Adressen der Unterzeichnenden – keine Patientendaten. Er ist deshalb **kein** Unterauftragnehmer im Sinne der Ziffer 7.

Unterzeichnet wird elektronisch (Ziffer 12). Ort, Datum und die Unterschriften beider Seiten trägt der Signaturdienst bei; sein Prüfprotokoll gehört zu diesem Vertrag.

Anlage 1 - Technische und organisatorische Maßnahmen

Der folgende Stand entspricht dem tatsächlichen Verhalten der Software (**Stand: 02.09.2026**). **Bei Änderungen an der Anwendung ist diese Anlage nachzuziehen: sie ist eine verbindliche Beschreibung des Stands nach Ziffer 6, keine Absichtserklärung.**

Was dieses Datum trägt und was nicht:

- **Gegen den Quelltext geprüft** sind die Angaben zur Verschlüsselung: die Aufzählung der verschlüsselten und der im Klartext gehaltenen Felder stimmt mit `App\Entity\PatientBefund` überein (29 verschlüsselte Spalten). Ebenso Rollenkonzept, Passwort-Hashing, Einmal-Token samt Gültigkeit und Rate-Limit, UUID-Adressierung und das Löschkonzept.
- **Nicht durch die Software belegbar** und deshalb vom Auftragnehmer eingetragen sind Sicherung, Wiederherstellung und Zutrittskontrolle. Sie stehen unten mit Intervall, Aufbewahrung und Datum;

maßgeblich ist der dort genannte Stand.

Vertraulichkeit

Zutrittskontrolle. Serverbetrieb im Rechenzentrum der STRATO GmbH in Berlin. Maßgeblich sind die Nachweise des Anbieters: „Vereinbarung zur Auftragsverarbeitung – Technische und Organisatorische Sicherheitsmaßnahmen gemäß Art. 32 DSGVO“, Version 1.0, abrufbar unter <https://www.strato.de/agb/tom/> (abgerufen am 18.08.2026). Der Anbieter führt dort unter anderem ein Informationssicherheitsmanagement nach ISO 27001, Brandschutz, Redundanzen und Rechenzentren in Deutschland auf.

Verwiesen statt beigefügt, und zwar mit Version und Abrufdatum: Der Anbieter veröffentlicht diese Maßnahmen als Webseite und entwickelt sie fort. Eine beigelegte Momentaufnahme wäre nach der nächsten Änderung falsch, ohne dass es jemand merkt – festgehalten ist deshalb, welcher Stand galt. Eigene Maßnahmen zur physischen Sicherung trifft der Auftragnehmer nicht und sagt sie auch nicht zu – er hat selbst keinen Zutritt zum Rechenzentrum.

Zugangskontrolle. Zugang zum Therapeutenbereich ausschließlich über persönliche Benutzerkonten mit E-Mail und Passwort. Passwörter werden nie im Klartext gespeichert, sondern über den Symphony-Hasher im Modus `auto` (derzeit bcrypt bzw. Argon2id) gehasht. Optional ist eine Zwei-Faktor-Anmeldung per TOTP aktivierbar. Der Login ist gegen Cross-Site-Request-Forgery abgesichert.

Zugriffskontrolle. Rollenkonzept mit zwei Stufen: Therapeutinnen und Therapeuten (`ROLE_USER`) sehen nur die von ihnen selbst erzeugten Befunde, administrative Konten (`ROLE_ADMIN`) haben Zugriff auf Benutzerverwaltung und alle Befunde. Die Prüfung erfolgt serverseitig bei jedem Aufruf.

Verschlüsselung.

- *Transportweg:* ausschließlich HTTPS, HTTP Strict Transport Security aktiv.
- *Ruhende Daten:* Die Gesundheits- und Identifikationsdaten der Befunde werden feldweise mit XSalsa20-Poly1305 (libsodium `secretbox`) verschlüsselt in der Datenbank abgelegt. Das Verfahren ist authentifiziert, Manipulationen am Chifftrat werden beim Lesen erkannt. Der Schlüssel liegt außerhalb der Datenbank in der Serverkonfiguration.

Verschlüsselt sind: Name, Versichertenstatus, Hauptproblem, Ziel, Tagesverlauf, Zeitinvestition, bisherige Versuche, Hinweise an die Therapeutin/den Therapeuten, lindernde und verschlimmernde Faktoren, bekannte Erkrankungen, Medikamente, Vorerkrankungen-Checkliste, markierte Schmerzzonen, Angaben zum Schlaf (Qualität, Dauer, Zustand am Morgen), Unterschrift, Behandlernoteizen sowie die Zusatzangaben des Osteopathie-Bogens: Trinkverhalten und Trinkmenge, umliegende Gelenke, vorhergegangene Operationen, künstliche Gelenke, Schmerzstärke (VAS), körperliche und psychische Belastung, Beruf sowie Sportart und Sportumfang.

Nicht verschlüsselt sind: Geburtsdatum, Angabe zur Lebensqualität, Kennzeichen für vorliegende Arztberichte und Wahrheitsbestätigung, Zeitstempel (einschließlich der Zeitpunkte, zu denen Behandlungsinformationen und Gebührensätze bestätigt wurden), Zugangstoken, die E-Mail-Adresse des ausstellenden Kontos, die Kennung des verwendeten Befundbogens (z. B. „standard“, „osteopathie“) sowie die Nummer des zugestimmten Gebührenverzeichnisses. Diese Felder werden für Betrieb, Sortierung, Ablaufsteuerung des Fragebogens, Zugriffsprüfung und den Nachweis der Zustimmung im Klartext benötigt; Bogenkennung und Gebührenversion sind keine Angaben des Patienten, sondern Festlegungen der Praxis.

Die Gebührenverzeichnisse selbst (Leistungsbezeichnungen und Preise der Praxis) enthalten keine personenbezogenen Daten und werden im Klartext gespeichert. Sie sind unveränderlich versioniert: Eine Preisänderung erzeugt eine neue Version, bestehende bleiben erhalten, damit nachvollziehbar bleibt, welchen Beträgen eine Patientin oder ein Patient tatsächlich zugestimmt hat.

Pseudonymisierung. Befunde werden über zufällige UUIDs adressiert, nicht über fortlaufende Nummern. Rückschlüsse aus der Kennung auf andere Datensätze oder auf die Menge der gespeicherten Befunde sind nicht möglich.

Patientenzugang. Der Zugang zum Fragebogen erfolgt über einen kryptografisch zufälligen Einmal-Token (128 Bit). Er ist **24 Stunden** gültig und verfällt sofort nach dem Absenden. Die Zugriffsroute ist auf **10 Aufrufe pro Minute und IP-Adresse** begrenzt, um das Durchprobieren von Token zu verhindern.

Integrität

Eingabekontrolle. Jeder Befund speichert das ausstellende Benutzerkonto sowie Erstellungszeitpunkt.

Übertragungskontrolle. Datenübertragung ausschließlich über TLS.

Verfügbarkeit und Belastbarkeit

Sicherung. Gesichert wird auf zwei Wegen:

Sicherung	Zeitpunkt	Aufbewahrung
täglich	03:15 Uhr	5 Tage
wöchentlich	-	4 Wochen

Beide liegen auf dem Server selbst. **Zusätzlich wird der virtuelle Server als Ganzes beim Anbieter gesichert;** damit besteht eine Kopie außerhalb der Maschine.

Die Aufteilung ist beabsichtigt und deckt drei verschiedene Fälle ab: Die tägliche Sicherung holt zurück, was versehentlich gelöscht oder fehlerhaft geändert wurde. Die wöchentliche erweitert den

Zeitraum, in dem ein Fehler noch auffallen darf – bei einer Aufbewahrungspflicht von zehn Jahren ist das der Unterschied zwischen „vorige Woche bemerkt“ und „nicht mehr herstellbar“. Die Sicherung des Servers beim Anbieter deckt dessen Verlust ab.

Zum Verschlüsselungsschlüssel: Der APP_ENCRYPTION_KEY wird **zusätzlich an einem von den Sicherungen getrennten Ort aufbewahrt**. Das ist keine Förmlichkeit: Ohne ihn lässt sich keine Sicherung wiederherstellen – eine Datensicherung allein ist wertlos, und ginge der Schlüssel mit dem Server verloren, wären auch alle Sicherungen unlesbar. Auf dem Server selbst liegt er notwendigerweise, sonst könnte die Anwendung die Daten nicht lesen. Die Feldverschlüsselung schützt deshalb gegen die Preisgabe der **Datenbank** – einen kopierten Abzug, eine abhanden gekommene Sicherung, einen Zugriff allein auf die Datenbank. Gegen die vollständige Übernahme des Servers schützt sie nicht; diesen Fall decken Zugangs- und Zugriffskontrolle ab. Das ist die Reichweite der Maßnahme, und sie steht hier statt eines Satzes, der mehr verspricht.

Wiederherstellung. Eine Wiederherstellung aus der Sicherung ist **jederzeit möglich** und wird auf Anforderung des Verantwortlichen oder bei Bedarf durch den Auftragnehmer durchgeführt. Zuletzt erprobt am **18.08.2026**.

Der Test gehört wiederholt, wenn sich an Datenbank, Verschlüsselungsschlüssel oder Hosting etwas ändert. Ob eine Sicherung sich zurückspielen lässt, weiß man erst, wenn man es getan hat, und eine Angabe, die auf einem alten Versuch beruht, trägt im Ernstfall nicht.

Verfahren zur regelmäßigen Überprüfung

Datenschutz durch Voreinstellung. Der Fragebogen erhebt ausschließlich die für die Behandlung erforderlichen Angaben. Ein anonymer Zugang zum Formular ist nicht möglich.

Löschkonzept. Der Befehl `app:befunde:cleanup` läuft täglich und löscht Befunde, deren Zugangslink abgelaufen ist und die nie abgeschickt wurden, nach einer Karenzzeit von 7 Tagen. Für abgeschlossene Befunde ist eine Aufbewahrungsfrist konfigurierbar; sie ist im Auslieferungszustand deaktiviert, damit die Aufbewahrungspflicht nach § 630f BGB nicht unterlaufen wird. Vereinbarte Frist: `[... Tage / keine]`.

Trennungskontrolle. Für jede Praxis wird eine eigene Datenbank angelegt. Jede Praxis erhält eine eigene Installation mit eigener Datenbank und eigenem Verschlüsselungsschlüssel. Eine gemeinsame Datenhaltung mehrerer Praxen findet nicht statt – auch dann nicht, wenn mehrere Installationen als Sub-Domains derselben Adresse erreichbar sind (`muster-physio.mirwena.de`). Die gemeinsame Adresse ist eine Frage der Erreichbarkeit, nicht der Datenhaltung.

Aus der eigenen Datenbank folgt der eigene Schlüssel: `APP_ENCRYPTION_KEY` gilt je Installation, und ein Schlüssel, der zwei Datenbanken öffnet, hebt die Trennung wieder auf. Beides wird beim Anlegen einer Praxis zusammen erzeugt.

„Eigene Installation“ heißt eigener Webbereich, eigene Datenbank und eigener Schlüssel - nicht notwendigerweise ein eigener Server. Mehrere Installationen können auf derselben gemieteten Maschine laufen. Getrennt sind Datenhaltung und Schlüssel; das Blech ist es nicht, und dieser Vertrag sagt es auch nicht zu.