DATENSCHUTZ-INFORMATION · KUNDENFASSUNG · AUGUST 2026

Datenschutz bei Medora

Wie Medora mit den Daten Ihrer Beschäftigten umgeht — Rollen, Schutzmaßnahmen, Dienstleister, Löschung und Ihre Pflichten als Einrichtung.

Art. 28 DSGVO | Art. 9 Gesundheitsdaten | Mandantentrennung | KI transparent

Stand: August 2026 · Medora UG (haftungsbeschränkt) · Kundenfassung zur Weitergabe an Leitung, Betriebsrat und Datenschutzbeauftragte

Worum es in diesem Dokument geht

Wenn eine Pflegeeinrichtung Medora einsetzt, verarbeitet sie damit Daten ihrer Beschäftigten — Dienstpläne, Arbeitszeiten, Nachrichten und, unvermeidlich, auch Krankmeldungen. Krankmeldungen sind Gesundheitsdaten im Sinne des Art. 9 DSGVO und damit die am strengsten geschützte Kategorie überhaupt.

Diese Information beschreibt, **was Medora technisch tatsächlich tut**, wer wofür verantwortlich ist, welche Dienstleister beteiligt sind und was Sie als Einrichtung selbst erledigen müssen. Sie ist so geschrieben, dass Sie sie an Ihre Datenschutzbeauftragte, Ihren Betriebsrat oder Ihre Mitarbeitervertretung weitergeben können.

Ein ausführlicheres internes Konzept, ein Löschkonzept und ein Entwurf der Datenschutz-Folgenabschätzung liegen vor und werden im Rahmen einer Pilotvereinbarung zur Verfügung gestellt. Der **Auftragsverarbeitungsvertrag** nach Art. 28 DSGVO wird auf Anfrage vorgelegt — zur Prüfung durch Ihre Datenschutzbeauftragten, bevor echte Daten eingegeben werden.

> Diese Information ersetzt keine Rechtsberatung. Sie beschreibt den Stand von August 2026 und wird bei wesentlichen Änderungen fortgeschrieben.

1. Wer ist wofür verantwortlich

Das ist die Frage, die in Datenschutzunterlagen am häufigsten durcheinandergerät. Deshalb steht sie hier ganz vorn.

Rolle	Wer	Wofür
Verantwortlicher (Art. 4 Nr. 7 DSGVO)	Ihre Einrichtung	Entscheidet, welche Beschäftigtendaten erhoben werden, zu welchem Zweck und wie lange. Trägt die Rechtsgrundlage.
Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO)	Medora UG (haftungsbeschränkt)	Verarbeitet ausschließlich weisungsgebunden. Stellt Technik, Sicherheit und Löschfunktionen bereit. Entscheidet nicht über Zwecke.

Konkret heißt das: **Sie bleiben Herr der Daten.** Wir betreiben die Technik und dürfen mit den Daten nichts anderes tun, als Sie uns auftragen. Ein **Auftragsverarbeitungsvertrag nach Art. 28 DSGVO** gehört deshalb zwingend zum Vertrag dazu — ohne ihn dürfen wir nicht starten.

Getrennt davon sind wir für unsere *eigenen* Daten Verantwortlicher: Vertrags- und Rechnungsdaten, Ansprechpartner, Support-Vorgänge, Besucher dieser Website. Dafür gilt Art. 28 gerade nicht.

Anbieter

Firmierung	Medora UG (haftungsbeschränkt)
Sitz	Ammerland, Niedersachsen — vollständige Anschrift im Impressum
Geschäftsführung	Fynn Hobbje
Kontakt in Datenschutzfragen	datenschutz@medora.software

2. Was verarbeitet wird

2.1 Zweck

Medora dient der Organisation des Betriebsalltags: Dienst- und Einsatzplanung, Arbeitszeiten, Ausfall- und Einspringen-Management, Urlaub und Wunschfrei, interne Kommunikation, Dateiablage, Benachrichtigungen.

2.2 Wessen Daten

Kategorie	Umfang
Beschäftigte der Einrichtung	Kern der Verarbeitung — Pflegekräfte, Leitungen, Verwaltung
Bewohnerinnen, Bewohner, Klienten	Nur mittelbar und nur, soweit Beschäftigte sie in Freitextfelder eintragen
Bewerberinnen und Bewerber	Nur wenn der Website-Baukasten aktiv ist
Externe Gesprächsteilnehmer	Nur bei Gastzugang zu Videoanrufen

2.3 Welche Daten

Kategorie	Beispiele
Stammdaten	Name, E-Mail, Telefon, Anschrift, Geburtsdatum, Personalnummer, Notfallkontakt
Beschäftigungsdaten	Qualifikation, Fachkraftstatus, Beschäftigungsumfang, Wochenstunden
Planungs- und Arbeitszeitdaten	Dienste, Ist-Zeiten, Arbeitszeitkonten, Urlaub, Wunschfrei
Gesundheitsdaten	Krankmeldungen, Abwesenheitsgründe, Krankheitstage — siehe Abschnitt 4
Kommunikationsdaten	Nachrichten, Anhänge, Sprachnachrichten, Anrufe, News-Beiträge

Kategorie	Beispiele
Anmeldedaten	Passwort-Prüfwert, Passkeys, Sitzungs- und Gerätekennungen — nie im Klartext
Protokolldaten	Änderungsprotokoll, Anmeldeversuche, Dateizugriffe

3. Getrennte Umgebungen: der stärkste Punkt der Architektur

Die Trennung zwischen Kunden ist **physisch, nicht logisch**. Es gibt keine gemeinsame Tabelle mit einer Kundenkennung, in der ein Programmierfehler Daten vermischen könnte.

- **Eine eigene Datenbank je Einrichtung**, angelegt mit eigenem Datenbankbenutzer und eigenem Zufallspasswort. Die Rechte sind auf genau diese eine Datenbank beschränkt.
- **Ein eigener Dateibaum je Einrichtung**, gegen direkten Abruf gesperrt. Dateien werden ausschließlich über rechteprüfende Programmteile ausgeliefert.
- **Auflösung über die Domain.** Welche Datenbank gilt, ergibt sich aus dem aufgerufenen Hostnamen.
- **Fail-Closed.** Lässt sich die Datenbank einer Einrichtung nicht verbinden, endet die Anfrage mit einem Fehler. Es gibt keinen Rückfall auf eine andere Datenbank.
- **Sitzungsbindung.** Eine Anmeldung gilt nur in der Umgebung, in der sie entstanden ist.
- **Zugriffe des Anbieters auf Kundendaten werden protokolliert.**

> Der praktische Nutzen: Selbst ein Fehler in der Rechteprüfung kann keine Daten einer anderen Einrichtung offenlegen, weil die Verbindung sie gar nicht erreicht.

4. Gesundheitsdaten

4.1 Wo sie anfallen

Krankmeldungen sind im Pflegebetrieb unvermeidlich. In Medora entstehen Gesundheitsdaten beim Krankheitsfall selbst (Beginn, voraussichtliches Ende, Rückkehr, Status, ein auf 250 Zeichen begrenzter Freitextgrund), in der Krankheitshistorie einer Person, im Ereignisverlauf des Ausfalls, in den Krankheitstagen des Arbeitszeitkontos und im Dienstplan selbst, wo der Dienst „Krank" steht.

4.2 Was ausdrücklich nicht erhoben wird

Diese Abgrenzung ist für Ihre Risikobewertung wichtig:

- **Kein Upload von Arbeitsunfähigkeitsbescheinigungen.** Es gibt keine Attest-Funktion.
- **Keine Felder** für Schwangerschaft, Mutterschutz, Schwerbehinderung, Betriebsarzt oder arbeitsmedizinische Untersuchungen.
- **Keine Diagnosen** als strukturiertes Feld.
- **Keine Angaben** zu Religion, Gewerkschaftszugehörigkeit oder Herkunft.

> **Bitte weisen Sie Ihr Team darauf hin, dass in das Grundfeld der Krankmeldung keine Diagnose gehört.** Als Arbeitgeber dürfen Sie die Diagnose regelmäßig nicht kennen. Steht sie doch im Freitext, entsteht ein vermeidbares Risiko, das technisch nicht verhinderbar ist.

4.3 Daten von Pflegebedürftigen

Medora hat kein Feld für Diagnosen, Medikation oder Pflegeberichte und ist für die pflegerische Dokumentation nicht vorgesehen — die gehört in Ihr Fachprogramm. In Freitextfelder wie Nachrichten, Dokumente oder den Kommentar an einem Ausfall können Beschäftigte gleichwohl Angaben über betreute Personen eintragen. Verantwortlich bleiben Sie auch dafür. Wir empfehlen, im Pilot ausdrücklich festzuhalten, dass dort keine Gesundheitsdaten Dritter hineingehören, und das den Beschäftigten so zu sagen.

4.4 Rechtsgrundlage

Für Gesundheitsdaten von Beschäftigten kommt **Art. 9 Abs. 2 lit. b DSGVO** in Verbindung mit **§ 26 Abs. 3 BDSG** in Betracht — Verarbeitung zur Ausübung von Rechten und Pflichten aus dem Arbeitsrecht. Die Rechtsgrundlage sicherzustellen ist Ihre Aufgabe als Verantwortliche; wir stellen die technischen Schutzmaßnahmen nach § 22 Abs. 2 BDSG bereit.

5. Mitbestimmung: bitte früh einplanen

Medora enthält Funktionen, die zur Überwachung von Leistung und Verhalten **objektiv geeignet** sind. Auf die Absicht kommt es nach ständiger Rechtsprechung nicht an. Dazu zählen Zeiterfassung, Ist-Arbeitszeiten und Arbeitszeitkonten, die Anwesenheitsanzeige, das Änderungsprotokoll im Dienstplan, Zugriffsprotokolle der Dateiablage und angezeigte Lesezeitpunkte im Messenger.

> **Wenn es bei Ihnen einen Betriebsrat oder eine Mitarbeitervertretung gibt, ist die Einführung nach § 87 Abs. 1 Nr. 6 BetrVG mitbestimmungspflichtig.** Ohne Beteiligung droht ein Unterlassungsanspruch — im schlimmsten Fall müssten Sie die Software wieder abschalten.

Wir liefern dafür eine **Muster-Betriebsvereinbarung** als Anlage mit. Sie nimmt die aufwendigste Hürde weitgehend ab und beschleunigt die Einführung erheblich.

6. Schutzmaßnahmen (Art. 32 DSGVO)

6.1 Zugang und Zugriff

Maßnahme	Umsetzung
Passwörter	Als bcrypt-Prüfwert gespeichert, nie im Klartext, auch nicht in Protokollen
Zwei-Faktor	Passkeys nach WebAuthn (Face ID, Touch ID, Sicherheitsschlüssel). Drei Stufen: aus, Abfrage beim Anmelden, verpflichtend
Verwaltungszugang des Anbieters	Passkey **verpflichtend** auf allen Anmeldewegen
Anmeldeschutz	Sperre nach 5 Fehlversuchen in 15 Minuten, ansteigend bis 60 Minuten
Speicherung der Fehlversuche	Nur ein Prüfwert aus Benutzername und IP — weder Name noch IP im Klartext
Sitzungsdauer	10 Minuten ohne Aktivität; 14 Tage bei ausdrücklich langer Sitzung

Maßnahme	Umsetzung
Rollenmodell	Abgestufte Rollen von Mitarbeitenden bis Administration, dazu frei benennbare Zusatzrollen und eine Rechte-Feinsteuerung
Zusätzliche Schranke	Rang allein genügt nicht — für den Zugriff ist zusätzlich die Zuständigkeit für den jeweiligen Bereich erforderlich

6.2 Übertragung

Durchgehend HTTPS mit vorgelagertem Schutzdienst, HSTS aktiv, strenge Inhaltsrichtlinie (Content Security Policy) mit Einmalkennung je Seitenaufruf, kein MIME-Raten, Einbettung nur aus eigener Herkunft, Standortbestimmung und Bezahlschnittstellen abgeschaltet.

6.3 Verschlüsselung gespeicherter Daten

Bereich	Stand
Nachrichteninhalte	Verschlüsselt gespeichert
Messenger-Medien und Dokumente	Verschlüsselt gespeichert
Ende-zu-Ende (optional)	Für Ordner der Dateiablage und Nachrichten zuschaltbar; der private Schlüssel verlässt das Gerät nie
Sicherungen	AES-256-GCM
Stammdaten in der Datenbank	Unverschlüsselt gespeichert, geschützt durch Zugriffsrechte auf Server und Datenbank — wie bei Fachanwendungen üblich
Hochgeladene Dateien	Abgelegt außerhalb des direkten Abrufwegs, Auslieferung nur nach Rechteprüfung

6.4 Nachvollziehbarkeit

Ein Änderungsprotokoll erfasst Konto, Aktion, betroffenen Datensatz und Zeitpunkt — unter anderem für Rollenänderungen, Bereichs- und Dienstartänderungen sowie Löschungen. Einsichtnahmen des Anbieters in Kundendaten werden gesondert vermerkt.

6.5 Datensparsamkeit ab Erhebung

Belege für Privacy by Design nach Art. 25 DSGVO:

- Anmeldeversuche speichern keine Klartext-Kennungen.
- Einwilligungen speichern die IP-Adresse nur als Prüfwert.
- Nutzungsstatistiken sind reine Tages- und Stundenzähler **ohne** Kontobezug.
- Das Protokoll der KI-Nutzung erfasst Zweck, Modell und Umfang, aber **keine Inhalte**.
- Einladungs-E-Mails enthalten keine Zählpixel; QR-Codes werden lokal erzeugt.
- Nachrichten werden nach 30 Tagen automatisch gelöscht.

7. Beteiligte Dienstleister

7.1 Unterauftragsverarbeiter

Dienstleister	Leistung	Daten	Ort
Hetzner Online GmbH	Serverbetrieb	Alle Daten	Deutschland
Cloudflare	Vorgelagerter Schutz, Verbindungsverschlüsselung, DNS	IP-Adressen, Verbindungsdaten	Weltweit, Sitz USA
Apple	Push-Benachrichtigungen an iPhones	Gerätekennung, Absendername in der Benachrichtigung	USA
Microsoft 365	E-Mail-Versand (Einladungen, Rechnungen)	E-Mail-Adresse, Name	EU/USA
Google (Gemini)	KI-Auswertung — **nur wenn zugebucht**	Pseudonymisierte Plandaten, siehe Abschnitt 8	Weltweit, Sitz USA
OpenAI	Sprachausgabe des Assistenten — **nur wenn zugebucht und ausdrücklich aktiviert**	Nur unkritische Kurzsätze	USA

Für Anbieter mit Sitz in den USA bestehen jeweils ein Auftragsverarbeitungsvertrag, eine Grundlage nach Kapitel V DSGVO (Angemessenheitsbeschluss oder Standardvertragsklauseln) und eine dokumentierte Abwägung. Die jeweils gültige Liste ist Anlage zum Auftragsverarbeitungsvertrag; Änderungen werden Ihnen vorab angezeigt.

7.2 Was nachweislich nicht eingesetzt wird

Keine Webanalyse. Kein Tracking-Pixel. Keine Werbekennungen. Keine externe Fehlerüberwachung. Keine Kartendienste. Kein Zahlungsdienstleister in der Anwendung. Kein Firebase.

Videokonferenz und Telefonie laufen auf eigener Infrastruktur. Die Sprachausgabe kann vollständig lokal erfolgen. Schriftarten werden vom eigenen Server ausgeliefert, nicht von Google. Die Anwendung setzt fünf eigene Cookies, alle rein funktional, jeweils mit den Schutzattributen `HttpOnly`, `Secure` und `SameSite=Lax`.

> Das ist ein Punkt, den Betriebsräte regelmäßig zuerst prüfen: Medora hat kein wirtschaftliches Interesse an Nutzungsdaten und keine Kette externer Beobachter.

8. Künstliche Intelligenz — was wirklich passiert

Die KI-Funktionen sind **zubuchbar und vollständig abschaltbar**. Ohne Zugangsschlüssel findet kein einziger externer Aufruf statt. Wo sie eingesetzt werden, gilt Folgendes.

8.1 Pseudonymisierung vor jeder Übermittlung

Vor jedem Aufruf ersetzt ein serverseitiger Baustein die Namen aller Personen aus dem Zuständigkeitsbereich der anfragenden Person durch Platzhalter (`Person_1`, `Person_2`, …). Die Zuordnung bleibt auf dem Server und wird weder an die KI noch an den Browser übermittelt.

8.2 Dienstplanprüfung

Zunächst läuft eine rein rechnerische Prüfung ohne KI. Nur wenn der Plan vollständig ist, folgt genau ein Aufruf. Übermittelt werden ausschließlich Platzhalter, Dienstkürzel und Tageszahlen — **keine Namen, keine Personalnummern, kein Freitext**.

8.3 Planungsvorschlag

Übermittelt werden je Platzhalter Qualifikation, Zielstunden, Höchstzahl aufeinanderfolgender Tage, bevorzugte und gemiedene Dienste, Wochenend- und Nachtneigung, Stundensaldo sowie historische Nacht- und Wochenendzahlen.

> Das ist **pseudonymisiert, nicht anonym**. Datenschutzrechtlich bleiben es personenbezogene Daten. Die Übermittlung braucht daher eine Rechtsgrundlage und gehört in Ihr Verarbeitungsverzeichnis.

8.4 Sprachausgabe

Zwei serverseitige Schranken, beide voreingestellt sicher: Vorgelesen wird nur ein kurzer, allgemeiner Satz, während Einzelheiten am Bildschirm bleiben. Zusätzlich prüft eine Erkennung auf Namen aus der Zuständigkeitsliste und rund fünfzig Stichwörter (krank, Diagnose, Attest, schwanger, Pflegegrad, Medikament, Bewohner, Patient, Gehalt, Geburtsdatum …). Erkannter empfindlicher Text wird **lokal** gesprochen. Die Sprachausgabe über einen externen Anbieter ist zudem **standardmäßig ausgeschaltet**.

8.5 Unsere Empfehlung für den Pilot

> **KI-Assistent und KI-Planung im Pilot abgeschaltet lassen, die Dienstplanprüfung freigeben.** Die Dienstplanprüfung liefert den sichtbaren Nutzen und ist datenschutzrechtlich sauber, weil sie ausschließlich Platzhalter und Dienstkürzel überträgt. Assistent und Planer bringen den größten Teil des Erklärungs- und Prüfaufwands, ohne im Pilot entscheidend zu sein. Beide lassen sich später als eigene, gesondert vereinbarte Änderung zuschalten.

9. Löschung und Aufbewahrung

Die Einzelheiten stehen in einem eigenen Löschkonzept, das Teil der Pilotunterlagen ist. Die Grundsätze:

1. **Beim Ausscheiden einer Person wird anonymisiert, nicht kaskadierend gelöscht.** Stammdaten werden überschrieben und die Anmeldung unmöglich gemacht. Dienstplanhistorie, geteilte Nachrichten und Protokolle bleiben als anonymisierter Platzhalter erhalten — das schützt die Nachvollziehbarkeit von Arbeitszeiten, die auch im Interesse der betroffenen Person liegt.
2. **Beim Vertragsende wird vollständig gelöscht:** Datenbank, Dateien, Registry-Eintrag und die Sicherungen über den Rotationszyklus.
3. **Vor jeder Löschung steht das Auskunftsrecht.** Ein maschinenlesbarer Export ist eingebaut.
4. **Nachrichten werden nach 30 Tagen automatisch gelöscht.**

Die konkreten Fristen der übrigen Datenkategorien stimmen wir mit Ihnen ab, weil sie von Ihren arbeits- und steuerrechtlichen Aufbewahrungspflichten abhängen.

10. Rechte der Beschäftigten

Recht	Umsetzung
Auskunft (Art. 15)	Eingebauter Export sämtlicher Datensätze mit Personenbezug als maschinenlesbare Datei — ohne Passwort-Prüfwerte und Passkey-Geheimnisse
Datenübertragbarkeit (Art. 20)	Derselbe Export
Berichtigung (Art. 16)	Über die Verwaltungsoberfläche
Löschung (Art. 17)	Anonymisierung des Kontos, siehe Abschnitt 9
Einschränkung (Art. 18)	Konto deaktivieren
Widerspruch (Art. 21)	Abschaltung freiwilliger Funktionen

Zuständig sind Sie. Anfragen richten Beschäftigte an ihren Arbeitgeber als Verantwortlichen. Erreicht eine Anfrage uns unmittelbar, beantworten wir sie **nicht selbst**, sondern leiten sie unverzüglich an Sie weiter und unterstützen technisch.

11. Datenpannen

Bei einem Vorfall melden wir **unverzüglich an Sie** — nicht an die Aufsichtsbehörde. Die Meldepflicht nach Art. 33 DSGVO trifft Sie als Verantwortliche, und Ihre 72-Stunden-Frist beginnt mit Ihrer Kenntnis. Jede Verzögerung bei uns würde Ihre Frist verkürzen, deshalb ist die Erstmeldung an Sie fest terminiert und im Auftragsverarbeitungsvertrag geregelt.

Die Meldung enthält Art des Vorfalls, betroffene Kategorien und ungefähre Zahl, wahrscheinliche Folgen und die ergriffenen Maßnahmen. Jeder Vorfall wird dokumentiert, auch der nicht meldepflichtige.

12. Datenschutz-Folgenabschätzung

Eine Folgenabschätzung nach Art. 35 DSGVO ist für diesen Einsatz **aller Voraussicht nach verpflichtend**. Es treffen mehrere Kriterien der Liste der deutschen Aufsichtsbehörden zusammen: umfangreiche Verarbeitung von Gesundheitsdaten, Beschäftigtendaten mit Funktionen, die zur Verhaltens- und Leistungskontrolle geeignet sind, der Einsatz innovativer Technik und ein Abhängigkeitsverhältnis der Betroffenen.

Geschuldet ist sie formal von **Ihnen**. Wir stellen einen vorbereiteten Entwurf zur Verfügung, der den größten Teil der Arbeit abnimmt und nur noch an Ihre Verhältnisse anzupassen ist.

13. Was wir vor dem Start eines Pilotbetriebs zusichern

Bevor die erste echte Krankmeldung in Medora steht, sind folgende Punkte erfüllt und werden Ihnen gegenüber schriftlich bestätigt:

	Zusage
1	Auftragsverarbeitungsvertrag geschlossen, mit vollständiger Liste der Unterauftragsverarbeiter
2	Verträge und Drittlandgrundlagen mit allen eigenen Dienstleistern liegen vor und sind dokumentiert

	Zusage
3	Sicherungen bestehen zusätzlich außerhalb des Servers; die Wiederherstellung ist erprobt und protokolliert
4	Die Verschlüsselung von Nachrichten, Medien und Sicherungen ist vor Freigabe geprüft
5	Löschfristen laufen zeitgesteuert und sind nachweisbar
6	Verpflichtung auf Vertraulichkeit für jede Person mit Zugriff auf Ihre Daten liegt unterschrieben vor
7	Meldeweg und Erreichbarkeit für Datenpannen sind festgelegt, auch außerhalb der Geschäftszeiten
8	Verarbeitungsverzeichnis, Löschkonzept und Entwurf der Folgenabschätzung liegen Ihnen vor
9	Datenschutzhinweis für Ihre Beschäftigten und Muster-Betriebsvereinbarung sind Teil des Lieferumfangs

Empfohlener Zuschnitt

Das Risiko sinkt erheblich, wenn der Pilot bewusst kleiner geschnitten wird als der spätere Funktionsumfang. Unsere Empfehlung: **KI-Assistent und KI-Planung abgeschaltet** (Dienstplanprüfung bleibt), **Website-Baukasten zunächst abgeschaltet** (sonst kommen Bewerberdaten und Lebenslauf-Uploads hinzu) und die **schriftliche Festlegung, dass in Freitextfelder keine Gesundheitsdaten betreuter Personen gehören**. Damit beschränkt sich der Pilot auf Beschäftigtendaten und Krankmeldungen — beherrschbar, erklärbar und mit den vorliegenden Unterlagen vollständig abgedeckt.

14. Was Sie selbst erledigen müssen

Damit nichts liegen bleibt, hier die Punkte, die rechtlich bei Ihnen liegen und die wir Ihnen nicht abnehmen können:

1. **Auftragsverarbeitungsvertrag** unterzeichnen, bevor echte Daten eingegeben werden.
2. **Rechtsgrundlage** für die Verarbeitung der Beschäftigtendaten sicherstellen, in der Regel § 26 BDSG.
3. **Datenschutzhinweis nach Art. 13 DSGVO** an Ihre Beschäftigten ausgeben — eine Vorlage liefern wir mit.
4. **Betriebsrat oder Mitarbeitervertretung beteiligen**, falls vorhanden — Muster-Betriebsvereinbarung liefern wir mit.
5. **Folgenabschätzung** abschließen — Entwurf liefern wir mit.
6. **Aufbewahrungsfristen** für Ihre Einrichtung festlegen und mit uns abstimmen.
7. **Verarbeitungsverzeichnis** um Medora ergänzen.
8. **Intern klarstellen**, dass in die Krankmeldung keine Diagnose gehört.

15. Fragen

Fragen zum Datenschutz beantworten wir direkt und ohne Umweg über eine Hotline.

Medora UG (haftungsbeschränkt) Fynn Hobbje · Geschäftsführer datenschutz@medora.software · medora.software

Stand: August 2026. Diese Information wird bei wesentlichen Änderungen der Software, bei Aufnahme neuer Dienstleister und mindestens jährlich überprüft. Sie ersetzt keine Rechtsberatung.