

Datenschutz und Schweigepflicht: zwei Pflichten, ein Vertrag reicht nicht

Der Prüf-Ablauf, damit ein unterschriebener Auftragsverarbeitungsvertrag nicht mit vollständiger Absicherung verwechselt wird.

KI in der Arztpraxis · Baustein 4 von 6 · Stand 15.09.2026



WAS DER VERTRAG ABDECKT

Die datenschutzrechtlichen Anforderungen der DSGVO

Auftragsverarbeitungsvertrag unterschrieben, Thema scheinbar erledigt.



WAS ER NICHT ABDECKT

Die eigenständige, strafbewehrte ärztliche Schweigepflicht nach § 203 StGB

Ein zweites, gesondertes Dokument bleibt nötig, unabhängig vom ersten Vertrag.

≠

Ein Vertrag für die DSGVO. Ein zweiter für die Schweigepflicht. Beide nötig.

Autoren dieses Guides

Dieser Guide entstand in redaktioneller Verantwortung von medivendis und wurde rechtlich durch einen auf Gesundheitsrecht spezialisierten Rechtsanwalt geprüft.



AUTOR

Tobias Boltze

Geschäftsführer, medivendis oHG

Tobias Boltze ist Geschäftsführer der medivendis oHG und verantwortet die Methodik, mit der medizinrechtliche Anforderungen, von Heilmittelwerberecht über Datenschutz bis Barrierefreiheit, in überprüfbare und laufend kontrollierte Systeme übersetzt werden. Sie stammt aus dem Aufbau einer Prüf-Architektur, die Websites regulierter Branchen fortlaufend gegen zwanzig Prüfbereiche misst, von der Erstprüfung bis zur Überwachung nach dem Livegang. Aus über 25 Jahren im Online-Marketing kennt er die Stelle, an der Praxis-Websites regelmäßig auffällig werden: nicht in der Absicht, sondern in Formulierungen und Technik, die nach dem Livegang niemand mehr nachprüft. Die rechtlichen Maßstäbe entstehen in Zusammenarbeit mit Gesundheitsrechtskanzleien wie juravendis; die Bewertung des Einzelfalls bleibt dort.



RECHTLICHE PRÜFUNG

RA Thomas Bruggmann, LL.M.

Inhaber, juravendis Rechtsanwaltskanzlei

Thomas Bruggmann ist Inhaber der Kanzlei juravendis in München. Er berät seit mehr als 20 Jahren Unternehmen schwerpunktmäßig zu Fragen des Lebensmittel- und sonstigen Gesundheitsrechts, insbesondere zu Fragen der Produktabgrenzung und Health Claims. Er ist Autor zahlreicher einschlägiger Veröffentlichungen, Referent der Lebensmittelrechtsakademie an der Universität Marburg und der Behr's Akademie sowie ehemaliger Lehrbeauftragter der Universität Erlangen-Nürnberg.

Übersicht

- 1 Warum ein Auftragsverarbeitungsvertrag nicht reicht
- › Wie Sie weiterlesen: zwei Wege
- 2 Was Art. 9 DSGVO und § 203 StGB unterscheidet
- 3 Die Grundregel: zwei Dokumente, nicht eines
- 4 Die DSFA-Kontroverse
- 5 Drittstaaten-Transfer: warum „DSGVO-konform“ nicht automatisch sicher heißt
- 6 Zero Data Retention: was das Versprechen wert ist
- 7 Ein Fall, der (noch) nicht existiert
- 8 Prüf-Ablauf in fünf Schritten
- 9 Checkliste zum Ausdrucken
- 10 Wo dieser Guide endet

AKTUALITÄTSHINWEIS

Dieser Guide gibt den Stand vom 15.09.2026 wieder. Kapitel 4 und 5 benennen offene, in der Fachwelt umstrittene Rechtsfragen ausdrücklich als solche, statt sie zu verschweigen. Die Fälle in den Kästen „Aus dem AppCore Universum“ sind verdichtete Praxis und keine benannten Kunden.

Wie Sie weiterlesen

Ab hier trennen sich zwei sinnvolle Wege durch diesen Guide. Beide führen durch dieselben Kapitel, nur in anderer Reihenfolge. Es gibt keinen doppelten Inhalt, Sie verpassen also nichts.

WEG A · SOFORT LOSLEGEN

Sie wollen heute noch prüfen, ob Ihre bestehenden KI-Verträge ausreichen.

Kapitel 3: die Grundregel, zwei Dokumente statt eines.

Kapitel 8: der Prüf-Ablauf mit Selbst-Check.

Danach die Kapitel 2, 4 bis 7 zum Verstehen, und Kapitel 10 zum Abschluss.

WEG B · ERST VERSTEHEN

Sie wollen wissen, warum ein einziger Vertrag hier nicht genügt, bevor Sie etwas ändern.

Lesen Sie der Reihe nach weiter ab Kapitel 2. Der Aufbau ist so gedacht: erst die Rechtsgrundlage, dann die Grundregel, dann die offenen Fragen zu Folgenabschätzung, Drittstaaten und Speicherezusagen, dann die Einordnung kursierender Fälle.

Wenn Sie nicht sicher sind, nehmen Sie Weg B. Er dauert eine knappe Stunde und erspart die Rückfragen, die auf Weg A erfahrungsgemäß nach dem ersten Befund kommen.

DAS FRAMEWORK DIESES THEMENPFADS

Alle Guides des Themenpfads KI in der Arztpraxis folgen demselben Vier-Schritte-Vorgehen: **Erfassen · Einordnen · Absichern · Nachweisen**. Dieser Guide konzentriert sich auf Absichern und Nachweisen.

HIER ENDET DIE LESEPROBE

Ab hier steht der eigentliche Inhalt

Was Sie im Hintergrund unscharf sehen, ist die erste von 10 Kapitelseiten dieses Bausteins. Sie ist bewusst nicht lesbar: die Leseprobe zeigt Aufbau und Machart, nicht das Ergebnis.

Der vollständige Baustein führt 10 Kapitel, je mit einem typisierten Fall aus dem AppCore Universum, dazu Prüf-Ablauf, Werkzeug-Übersicht und Checkliste zum Ausdrucken.

Vollständiger Baustein 39 €

medivendis · medivendis.de/audit

Erfassen. Absichern. Bestehen.

Dieser Baustein ist einer von sechs im Thema **KI in der Arztpraxis**. Alle sechs Bausteine zusammen kosten weniger als die Summe der Einzelkäufe, und alle vier Themen zusammen bilden das Kompendium.

KOMPENDIUM

Alle vier Themen, 24 Bausteine

399 €**THEMA**

KI in der Arztpraxis, 6 Bausteine

169 €**EINZELN**

Ein Baustein, frei wählbar

ab 29 €

DIE SECHS BAUSTEINE DES THEMAS KI IN DER ARZTPRAXIS

Grundlagen &
Fristen**29 €**Risiko-
klassifizierung**29 €**Transparenz auf
Website & Telefon**39 €**Datenschutz &
Schweigepflicht**39 €**

✓ Ihrer

Betreiberpflichten
& Governance**29 €**Auswahl & Vertrag
mit Anbietern**29 €**

Zuerst gilt aber: Wie steht es wirklich um Ihre Website?

Dieser Guide erklärt das Verfahren. Messen kann er Ihre Website nicht. Der medivendis Audit prüft sie kostenfrei gegen alle 20 Lösungen in einem Lauf, ohne Vertrag und ohne Kreditkarte.

medivendis.de/audit

* Alle angegebenen Preise sind Nettopreise, zzgl. gesetzl. MwSt.