

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag (AVV)

nach Art. 28 Abs. 3 DSGVO

Dok-ID: DBX-AVV-001 · Fassung: 2.1 · Stand: 06.08.2026 Ergänzt die AGB für die Nutzung des DoctorBox aTM-Portals (§ 14 AGB)

Präambel

Zwischen

der Apotheke (nachfolgend „**Verantwortliche**“) — Name, Anschrift, Betriebserlaubnis-Nr./IK gemäß Anlage 3 —

und

DoctorBox Leuchtturm GmbH, Taubenstraße 26, 10117 Berlin (nachfolgend „**Auftragsverarbeiterin**“)

wird der nachfolgende Vertrag geschlossen.

Die Verantwortliche nutzt die Plattform „DoctorBox aTM“ (Portal, Tablet-Anwendung und zugehörige Schnittstellen) zur Erbringung apothekerlicher Leistungen, insbesondere der assistierten Telemedizin nach § 129 Abs. 5h SGB V. Dabei verarbeitet die Auftragsverarbeiterin personenbezogene Daten im Auftrag der Verantwortlichen. Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien.

Rangfolge: Dieser Vertrag geht den AGB und dem sonstigen Hauptvertrag vor, soweit sich Widersprüche in datenschutzrechtlichen Fragen ergeben (§ 14 Abs. 2 AGB). Ohne wirksamen Abschluss dieses Vertrages dürfen über die Plattform keine personenbezogenen Daten von Patientinnen und Patienten verarbeitet werden.

§ 1 Gegenstand, Art, Zweck und Dauer der Verarbeitung

(Art. 28 Abs. 3 S. 1 DSGVO)

(1) Gegenstand, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten sowie die Kategorien betroffener Personen ergeben sich abschließend aus **Anlage 1**. Anlage 1 bildet zugleich die Grundlage für das Verzeichnis der Verantwortlichen nach Art. 30 Abs. 1 DSGVO und für dasjenige der Auftragsverarbeiterin nach Art. 30 Abs. 2 DSGVO.

(2) Die Verarbeitung findet ausschließlich im Gebiet der Europäischen Union oder des Europäischen Wirtschaftsraums statt, soweit in Anlage 2 nicht ausdrücklich etwas anderes bestimmt und dort abgesichert ist.

(3) Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages. Für die Zeit nach Vertragsende gilt § 11.

(4) Die Auftragsverarbeiterin verarbeitet die Daten ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen. Eine Verarbeitung zu eigenen Zwecken — insbesondere zur Produktverbesserung,

zum Training von KI-Modellen oder zu Analyse Zwecken — findet nicht statt. Statistische Auswertungen erfolgen ausschließlich auf Grundlage von Daten ohne Personenbezug (Anlage 1 Abschnitt E).

§ 2 Rechte und Pflichten der Verantwortlichen

(Art. 28 Abs. 3 S. 1, Art. 24, Art. 5 Abs. 2 DSGVO)

(1) Die Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Rechte betroffener Personen allein verantwortlich. Sie stellt insbesondere sicher, dass für jede Verarbeitung eine Rechtsgrundlage nach Art. 6 und — soweit Gesundheitsdaten betroffen sind — nach Art. 9 Abs. 2 DSGVO besteht.

(2) Die Verantwortliche informiert die Betroffenen entsprechend Art. 13, 14 DSGVO. Die Auftragsverarbeiterin stellt hierfür Textbausteine und die technische Beschreibung der Verarbeitung zur Verfügung (§ 8 Abs. 3).

(3) Die Verantwortliche führt die nach Art. 35 DSGVO erforderliche Datenschutz-Folgenabschätzung durch. Die Auftragsverarbeiterin stellt hierfür eine vorausgefüllte Vorlage sowie die technischen Angaben bereit (§ 8 Abs. 2). Die Verantwortliche wird darauf hingewiesen, dass sie aufgrund dieser DSFA-Pflicht nach **§ 38 Abs. 1 S. 2 BDSG unabhängig von der Zahl ihrer Beschäftigten eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen hat**.

(4) Die Verantwortliche erfüllt die in **Anlage 5** genannten Mitwirkungspflichten. Diese sind Voraussetzung dafür, dass das vereinbarte Schutzniveau erreicht wird; sie ergeben sich überwiegend aus den Vorgaben der ABDA zur assistierten Telemedizin und liegen außerhalb des Einflussbereichs der Auftragsverarbeiterin.

§ 3 Weisungsrecht und Weisungsbindung

(Art. 28 Abs. 3 lit. a und UAbs. 2, Art. 29 DSGVO)

(1) Die Auftragsverarbeiterin verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung der Verantwortlichen. Dies gilt auch für die Übermittlung in Drittländer. Besteht ausnahmsweise eine gesetzliche Verpflichtung zur Verarbeitung, teilt die Auftragsverarbeiterin dies der Verantwortlichen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Konfiguration der Plattform durch die Verantwortliche (Einstellungen im Portal, Freischaltung von Funktionsmodulen, Geräteeinstellungen am Tablet) gilt als Weisung im Sinne dieses Vertrages.

(3) Weisungen sind grundsätzlich in Textform zu erteilen. Mündlich erteilte Weisungen sind unverzüglich in Textform zu bestätigen. Weisungsberechtigte und Weisungsempfänger sind in **Anlage 3** benannt.

(4) Beide Parteien dokumentieren Weisungen und bewahren die Dokumentation für die Dauer des Vertrages und drei Jahre darüber hinaus auf.

(5) Ist die Auftragsverarbeiterin der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, teilt sie dies der Verantwortlichen unverzüglich mit. Sie ist berechtigt, die Ausführung der betreffenden Weisung auszusetzen, bis die Verantwortliche sie schriftlich bestätigt oder ändert.

(6) Für Aufwände, die durch Weisungen außerhalb des vertraglich vereinbarten Leistungsumfangs entstehen, kann die Auftragsverarbeiterin eine angemessene Vergütung nach ihrer jeweils gültigen Preisliste verlangen. Sie weist vor Ausführung auf die Vergütungspflicht hin.

§ 4 Vertraulichkeit

(Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO)

(1) Die Auftragsverarbeiterin setzt zur Verarbeitung ausschließlich Personen ein, die zur Vertraulichkeit verpflichtet und über die einschlägigen datenschutzrechtlichen Vorgaben unterwiesen wurden.

(2) Die Verpflichtung erfolgt vor Aufnahme der Tätigkeit in Textform und wirkt über das Ende des jeweiligen Beschäftigungs- oder Auftragsverhältnisses hinaus fort. Ein Muster der Verpflichtungserklärung ist als **Anlage 4** beigelegt.

(3) Die Auftragsverarbeiterin weist die Verpflichtungen auf Anforderung nach.

§ 5 Berufsgeheimnis — Verpflichtung nach § 203 StGB

(§ 203 Abs. 3 S. 2, Abs. 4 StGB; § 53a, § 97 Abs. 2 StPO)

(1) **Feststellung.** Die Parteien sind sich einig, dass die Verantwortliche als Apothekerin bzw. Apotheker zu den in § 203 Abs. 1 Nr. 1 StGB genannten Berufsgeheimnisträgern gehört und dass die Auftragsverarbeiterin im Rahmen dieses Vertrages Zugang zu Geheimnissen im Sinne dieser Vorschrift erhalten kann. Die Auftragsverarbeiterin wird als „sonstige mitwirkende Person“ im Sinne des § 203 Abs. 3 S. 2 StGB tätig; die Offenbarung ihr gegenüber ist zur Inanspruchnahme ihrer Tätigkeit erforderlich und damit befugt.

(2) **Stillschweigen.** Die Auftragsverarbeiterin verpflichtet sich, über alle ihr im Rahmen der Tätigkeit bekannt gewordenen Geheimnisse Stillschweigen zu bewahren. Sie nimmt von Geheimnissen nur Kenntnis, soweit dies zur Leistungserbringung erforderlich ist.

(3) **Belehrung.** Die Auftragsverarbeiterin ist darüber belehrt worden, dass sie und die für sie tätigen Personen sich nach § 203 Abs. 4 S. 1 StGB strafbar machen, wenn sie ein solches Geheimnis unbefugt offenbaren.

(4) **Weitergabe der Verpflichtung.** Die Auftragsverarbeiterin stellt sicher, dass alle mit der Leistungserbringung befassten Beschäftigten sowie alle weiteren für sie tätigen Personen — insbesondere Unterauftragsverarbeiter nach § 6 — vor Aufnahme der Tätigkeit in Textform zur Geheimhaltung verpflichtet und über die Strafbarkeit nach § 203 Abs. 4 StGB belehrt wurden.

(5) **Zeugnisverweigerungsrecht.** Die Auftragsverarbeiterin und die für sie tätigen Personen sind Berufshelfer im Sinne des § 53a StPO. Sie machen von einem Zeugnisverweigerungsrecht Gebrauch, soweit dieses besteht und die Verantwortliche sie nicht von der Schweigepflicht entbunden hat.

(6) **Beschlagnahme und behördliche Zugriffe.** Die Auftragsverarbeiterin weist bei behördlichen Auskunftersuchen, Durchsuchungen oder Beschlagnahmeversuchen unverzüglich auf das Beschlagnahmeverbot nach § 97 Abs. 2 StPO hin, widerspricht der Maßnahme, verlangt die Versiegelung der betroffenen Datenträger und informiert die Verantwortliche unverzüglich, soweit ihr dies rechtlich nicht untersagt ist. Sie unterhält hierfür einen dokumentierten internen Eskalationsprozess.

(7) **Fortwirkung.** Die Verpflichtungen dieses Paragraphen gelten über das Ende dieses Vertrages hinaus zeitlich unbegrenzt fort.

§ 6 Unterauftragsverarbeiter

(Art. 28 Abs. 2 und 4 DSGVO)

(1) Die Verantwortliche erteilt hiermit die **allgemeine schriftliche Genehmigung** zur Hinzuziehung der in **Anlage 2** aufgeführten Unterauftragsverarbeiter.

(2) Beabsichtigt die Auftragsverarbeiterin, einen weiteren Unterauftragsverarbeiter hinzuzuziehen oder einen bestehenden zu ersetzen, informiert sie die Verantwortliche mindestens **30 Tage** vorher in Textform unter Angabe von Name, Anschrift, Leistung, Datenkategorien und Verarbeitungsort.

(3) Die Verantwortliche kann der Änderung innerhalb von **14 Tagen** nach Zugang der Information aus einem wichtigen datenschutzrechtlichen Grund in Textform widersprechen. Kann der Einwand nicht innerhalb angemessener Frist ausgeräumt werden, steht der Verantwortlichen ein außerordentliches Kündigungsrecht hinsichtlich der betroffenen Leistung ohne zusätzliche Kosten zu.

(4) Die Auftragsverarbeiterin verpflichtet jeden Unterauftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten, die ihr aus diesem Vertrag obliegen, einschließlich der Verpflichtung nach § 5, soweit der Unterauftragsverarbeiter Zugang zu Berufsgeheimnissen erhält. Kommt der Unterauftragsverarbeiter seinen Pflichten nicht nach, haftet die Auftragsverarbeiterin gegenüber der Verantwortlichen für dessen Verhalten wie für eigenes.

(5) Nicht als Unterauftragsverarbeitung gelten Nebenleistungen ohne Verarbeitung personenbezogener Daten der Verantwortlichen (z. B. Telekommunikation, Reinigung, Bewachung) sowie die in Anlage 2 Abschnitt C bezeichneten Empfänger, die keine identifizierbaren personenbezogenen Daten erhalten.

(6) **Abgrenzung.** Empfänger, die im Rahmen der Leistungserbringung als eigenständig Verantwortliche tätig werden — insbesondere die ärztlichen Leistungserbringer und die von ihnen eingesetzten Terminvermittlungs- und Videodienstanbieter sowie der Zahlungsdienstleister — sind keine Unterauftragsverarbeiter. Die Rollenverteilung ergibt sich aus **Anlage 6**.

§ 7 Technische und organisatorische Maßnahmen

(Art. 28 Abs. 3 lit. c, Art. 32 DSGVO)

(1) Die Auftragsverarbeiterin trifft technische und organisatorische Maßnahmen, die ein dem Risiko angemessenes Schutzniveau gewährleisten. Sie umfassen insbesondere:

- a) **Verschlüsselung der Beratungsinhalte (Ende-zu-Ende).** Jede Fallakte wird mit einem je Vorgang neu erzeugten Schlüssel AES-256-verschlüsselt; dieser Schlüssel wird ausschließlich an das Organisationszertifikat der Verantwortlichen adressiert. Der zugehörige private Schlüssel ist mit einer nur der Verantwortlichen bekannten PIN geschützt und wird nirgends im Klartext gespeichert. **Die Auftragsverarbeiterin kann die Fallinhalte ohne diese PIN nicht lesen;** sie werden nur dann und nur so lange entschlüsselt, wie die Verantwortliche selbst durch PIN-Eingabe im Portal die Anzeige veranlasst.
- b) **Verschlüsselte Übertragung.** Sämtliche Datenübertragungen erfolgen transportverschlüsselt (TLS). Ausstehende Zustellungen liegen auf dem Tablet ausschließlich verschlüsselt vor.

- c) **Datensparsamkeit an den Schnittstellen.** An das Verfahren der strukturierten Ersteinschätzung und an den Anbieter der Vitalwerte-Messung werden keine Identitätsdaten übermittelt; an den Zahlungsdienstleister keine Kartennummern; Statistik- und Abrechnungszählungen enthalten keine personenbezogenen Daten.
- d) **Zugangs- und Zugriffskontrolle.** Der Portalzugang erfolgt über einen zentralen Identitätsanbieter mit gehashten Zugangsdaten. Die Anzeige von Klartext-Personendaten erfordert eine zusätzliche PIN-Eingabe, die nach 15 Minuten Untätigkeit verfällt und nach fünf Fehlversuchen für fünf Minuten gesperrt wird. Jedes Tablet authentisiert sich mit einem eigenen, widerrufbaren Zugangsschlüssel. Mandantentrennung stellt sicher, dass jede Apotheke ausschließlich auf ihre eigenen Daten zugreift.
- e) **Gerätesicherheit.** Die Tablet-Anwendung wird im Kiosk-Betrieb geführt; sicherheitsrelevante Konfiguration ist passwortgeschützt. Personenbezogene Falldaten werden nach Fallabschluss sowie nach fünf Minuten Untätigkeit vollständig vom Gerät gelöscht.
- f) **Löschung.** Termin- und Kontaktdaten im Portal werden nach den in Anlage 1 Abschnitt D genannten Fristen automatisch gelöscht bzw. pseudonymisiert.
- g) **Verfügbarkeit und Belastbarkeit.** Eine ausfallsichere Zustellwarteschlange verhindert Datenverlust bei Netzausfällen. Die Datenbank wird täglich verschlüsselt gesichert; die Sicherungen werden über mehrere Verfügbarkeitszonen verteilt vorgehalten.
- h) **Protokollierung mit Datenminimierung.** Fehler- und Betriebstelemetrie enthält keine Anfrageinhalte, keine Kopf- oder Cookie-Daten und keine Klartext-Personendaten, sondern ausschließlich Fehlerklassen und zufällige Vorgangskennungen.
- i) **Regelmäßige Überprüfung.** Die Wirksamkeit der Maßnahmen wird durch automatisierte Tests, statische Codeanalyse als verbindliches Auslieferungstor sowie laufende Auswertung der Betriebstelemetrie überprüft (Art. 32 Abs. 1 lit. d DSGVO).
- (2) Die Maßnahmen unterliegen dem technischen Fortschritt. Die Auftragsverarbeiterin darf sie anpassen, sofern das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen dokumentiert sie und teilt sie der Verantwortlichen in Textform mit.

§ 8 Unterstützungspflichten

(Art. 28 Abs. 3 lit. e und f DSGVO)

- (1) **Betroffenenrechte.** Die Auftragsverarbeiterin unterstützt die Verantwortliche mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Anträgen betroffener Personen nach Art. 12 bis 23 DSGVO. Wendet sich eine betroffene Person unmittelbar an die Auftragsverarbeiterin, leitet diese den Antrag unverzüglich an die Verantwortliche weiter und beantwortet ihn nicht selbst.
- (2) **Datenschutz-Folgenabschätzung.** Die Auftragsverarbeiterin unterstützt die Verantwortliche bei der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und einer etwaigen vorherigen Konsultation nach Art. 36 DSGVO. Sie stellt hierfür eine produktbezogene DSFA-Vorlage bereit und aktualisiert diese bei wesentlichen Produktänderungen.
- (3) **Informationspflichten.** Die Auftragsverarbeiterin stellt Textbausteine und technische Angaben zur Verfügung, die die Verantwortliche zur Erfüllung ihrer Informationspflichten nach Art. 13, 14 DSGVO benötigt.

(4) Für Unterstützungsleistungen, die über den vertraglich geschuldeten Umfang hinausgehen und nicht auf einem Umstand beruhen, den die Auftragsverarbeiterin zu vertreten hat, gilt § 3 Abs. 6 entsprechend.

§ 9 Meldung von Verletzungen des Schutzes personenbezogener Daten

(Art. 28 Abs. 3 lit. f, Art. 33 Abs. 2, Art. 34 DSGVO)

(1) Die Auftragsverarbeiterin meldet der Verantwortlichen jede ihr bekannt gewordene Verletzung des Schutzes personenbezogener Daten **unverzüglich, spätestens jedoch innerhalb von 24 Stunden** nach Kenntniserlangung in Textform an die in Anlage 3 benannte Stelle.

(2) Die Meldung enthält, soweit verfügbar: Beschreibung der Art der Verletzung, Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, wahrscheinliche Folgen, ergriffene und vorgeschlagene Maßnahmen sowie einen Ansprechpartner. Sind nicht alle Angaben verfügbar, erfolgt eine Erstmeldung mit den bekannten Informationen und eine Nachmeldung.

(3) Die Auftragsverarbeiterin unterstützt die Verantwortliche bei der Erfüllung von deren Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO. Die Meldung an die Aufsichtsbehörde obliegt der Verantwortlichen.

(4) Die Auftragsverarbeiterin ergreift unverzüglich angemessene Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen.

§ 10 Nachweise und Überprüfungen

(Art. 28 Abs. 3 lit. h DSGVO)

(1) Die Auftragsverarbeiterin stellt der Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO erforderlich sind.

(2) Der Nachweis erfolgt abgestuft:

- **Stufe 1 — Selbstauskunft.** Vorlage einer Maßnahmenbeschreibung und eines ausgefüllten TOM-Fragebogens auf Anforderung, höchstens einmal jährlich.
- **Stufe 2 — Nachweise Dritter.** Vorlage vorhandener Testate, Zertifizierungen oder Prüfberichte, soweit solche existieren.
- **Stufe 3 — Vor-Ort-Prüfung.** Bei konkretem Anlass — insbesondere nach einer Datenschutzverletzung, bei begründeten Zweifeln an der Einhaltung dieses Vertrages oder auf Anordnung einer Aufsichtsbehörde — kann die Verantwortliche eine Überprüfung in den Geschäftsräumen der Auftragsverarbeiterin durchführen oder durch eine zur Verschwiegenheit verpflichtete, nicht mit der Auftragsverarbeiterin im Wettbewerb stehende Prüferin durchführen lassen. Die Prüfung ist mit 14 Tagen Frist anzukündigen, auf die Geschäftszeiten zu beschränken und so durchzuführen, dass der Betriebsablauf nicht unangemessen beeinträchtigt wird.

(3) Prüfungen nach Stufe 3, die die Verantwortliche ohne von der Auftragsverarbeiterin zu vertretenden Anlass veranlasst, kann die Auftragsverarbeiterin nach Aufwand vergüten lassen.

(4) Die Auftragsverarbeiterin duldet Kontrollen der zuständigen Aufsichtsbehörden und wirkt daran mit.

§ 11 Löschung und Rückgabe nach Beendigung

(Art. 28 Abs. 3 lit. g DSGVO)

(1) Nach Beendigung der Verarbeitungsleistungen wählt die Verantwortliche innerhalb von **30 Tagen** in Textform, ob die personenbezogenen Daten gelöscht oder zurückgegeben werden sollen. Trifft sie keine Wahl, werden die Daten gelöscht.

(2) Die Rückgabe erfolgt in einem gängigen, maschinenlesbaren Format. Daten, die mit dem Organisationszertifikat der Verantwortlichen verschlüsselt sind, werden im verschlüsselten Zustand übergeben; die Verantwortliche verfügt über den zur Entschlüsselung erforderlichen privaten Schlüssel und die zugehörige PIN. Die Auftragsverarbeiterin weist ausdrücklich darauf hin, dass ein Verlust dieser PIN zur endgültigen Unlesbarkeit der Daten führt und die Auftragsverarbeiterin sie nicht wiederherstellen kann.

(3) Die Löschung erfolgt nach Rückgabe, spätestens **30 Tage** nach Ablauf der Frist nach Absatz 1. Sie umfasst auch Kopien bei Unterauftragsverarbeitern.

(4) Ausgenommen sind Daten, für die eine gesetzliche Aufbewahrungspflicht besteht — insbesondere die Behandlungsdokumentation nach § 630f Abs. 3 BGB (zehn Jahre); diese werden gesperrt und nach Fristablauf gelöscht. Ebenfalls ausgenommen sind Sicherungskopien bis zum Ablauf des regulären Rotationszyklus (7 Tage für Tages-, 4 Wochen für Wochensicherungen).

(5) Die Auftragsverarbeiterin bestätigt die Löschung auf Anforderung in Textform.

§ 12 Haftung

(1) Für die Haftung der Parteien untereinander gelten die Regelungen des Hauptvertrages (§ 12 AGB), soweit dieser Vertrag nichts anderes bestimmt.

(2) Art. 82 DSGVO bleibt unberührt. Im Innenverhältnis tragen die Parteien den Schaden entsprechend ihrem jeweiligen Verantwortungsanteil.

(3) Die Haftungsbeschränkungen des Hauptvertrages gelten nicht für Schäden aus der Verletzung von Leben, Körper oder Gesundheit, für Vorsatz und grobe Fahrlässigkeit sowie für Bußgelder, die gegen die Verantwortliche wegen eines von der Auftragsverarbeiterin zu vertretenden Verstoßes verhängt werden.

§ 13 Datenschutzbeauftragte und Kontakt

(1) Datenschutzbeauftragte(r) beider Parteien: siehe Anlage 3.

(2) Die Verantwortliche bestätigt, auf die Benennungspflicht nach § 38 Abs. 1 S. 2 BDSG hingewiesen worden zu sein (§ 2 Abs. 3).

§ 14 Vertragsdauer, Änderungen, Schlussbestimmungen

(1) Dieser Vertrag beginnt mit der Zustimmung der Verantwortlichen und endet mit dem Hauptvertrag. § 5 Abs. 7 und § 11 gelten darüber hinaus fort.

(2) Änderungen bedürfen der Textform. Das gilt auch für die Abbedingung dieses Formerfordernisses. Aktualisierungen der Anlage 2 erfolgen nach dem in § 6 Abs. 2 geregelten Verfahren.

(3) Sollte eine Bestimmung dieses Vertrages unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien ersetzen die unwirksame Bestimmung durch eine wirksame, die dem wirtschaftlichen Zweck am nächsten kommt.

(4) Es gilt deutsches Recht. Gerichtsstand ist, soweit zulässig, Berlin.

Anlage 1 — Gegenstand, Art und Zweck der Verarbeitung, Datenkategorien und betroffene Personen

A. Kategorien betroffener Personen

Kategorie	Erläuterung
Patientinnen und Patienten der Apotheke	Personen, die eine Leistung nach § 129 Abs. 5h SGB V, eine Schutzimpfung, einen Gesundheitstest oder eine Terminvereinbarung in Anspruch nehmen
Beschäftigte der Apotheke	Pharmazeutisches Personal, Inhaberin/Inhaber (Stammdaten, Unterschrift, Portalzugang)
Ärztliche Leistungserbringer	Nur im Modul „DoctorBox-Netz“: Name, Fachrichtung, Verfügbarkeiten, Organisationszertifikat

B. Art der personenbezogenen Daten

Datenart	Beispiele	Art. 9 DSGVO
Identitäts- und Kontaktdaten	Vor-/Nachname, Geburtsdatum, Anschrift, E-Mail, Telefon	nein
Versicherungsdaten	Krankenversichertennummer, Kostenträger-IK, Kassenname, Versichertenstatus/-art, GKV/PKV/Selbstzahler	nein ¹
Strukturierte Ersteinschätzung	Symptomangaben und Antworten im Anamnese-Verfahren, Ergebniskategorie	ja
Impfdokumentation	Anamnese- und Einwilligungsangaben, Impfstoffbezeichnung, Chargennummer, Impfarm, impfende Person	ja
Vitalparameter	Puls, Atemfrequenz, Herzratenvariabilität, Blutdruck	ja

	(kamerabasierte Schätzung), Stressindex	
Behandlungsvereinbarung und Einwilligungen	Handschriftliche Unterschrift, Einwilligungszeitpunkt, Textversion	ja ²
Terminaten	Zeitpunkt, Fachrichtung, Praxis, Terminstatus	ja ²
Zahlungsdaten	Kartenmarke, letzte vier Ziffern, Betrag, Zahlungsreferenz — keine vollständige Kartennummer	nein
Abrechnungsdaten	Sonderkennzeichen, Pauschale, Leistungsdatum	nein ¹
Technische Daten	Geräte-Kennung, App-Version, Zeitstempel, Fehlerdiagnosedaten ohne Personenbezug	nein

¹ Für sich genommen keine Gesundheitsdaten; im Verarbeitungskontext (Inanspruchnahme einer medizinischen Leistung) mittelbar aussagekräftig und deshalb wie Art.-9-Daten geschützt. · ² Aus dem Kontext ergibt sich ein Gesundheitsbezug.

C. Verarbeitungstätigkeiten und Zwecke

- **V1 — Assistierte Telemedizin:** Durchführung der strukturierten Ersteinschätzung, Unterstützung bei der Videokonsultation, Abrechnung nach § 129 Abs. 5h SGB V. Die Fallakte wird Ende-zu-Ende verschlüsselt an das Organisationszertifikat der Verantwortlichen adressiert und ist ohne deren PIN nicht lesbar.
- **V2 — Terminvermittlung** an ärztliche Leistungserbringer (Übermittlung an eigenständig Verantwortliche, Anlage 6).
- **V3 — Impfservice:** Terminvereinbarung, Anamnese, Dokumentation und Abrechnung von Schutzimpfungen nach § 20c IfSG. Rechtsgrundlage (durch Verantwortliche zu prüfen): Art. 9 Abs. 2 lit. h DSGVO i. V. m. § 22 BDSG, zusätzlich ausdrückliche Einwilligung.
- **V4 — Online-Terminvereinbarung:** Reservierung eines Ankunftszeitfensters; Name und E-Mail werden unmittelbar mit dem Organisationszertifikat versiegelt.
- **V5 — Vitalwerte-Messung:** optionale Erhebung orientierender Vitalparameter; gespeichert und übermittelt werden nur abgeleitete Messwerte, keine Bilder. Rechtsgrundlage (durch Verantwortliche zu prüfen): ausdrückliche Einwilligung, Art. 9 Abs. 2 lit. a DSGVO.
- **V6 — Kartenzahlung:** Bezahlung der Pauschale durch Selbstzahlende und Privatversicherte; Kartendaten verarbeitet ausschließlich der Zahlungsdienstleister.
- **V7 — Fehler- und Betriebstelemetrie:** Betrieb, Fehlerbehebung und Verfügbarkeit; personenbezugsfrei.

D. Speicherorte und Löschfristen

Ort / Bestand	Inhalt	Region	Löschung
Tablet in der Apotheke	Fallbearbeitung im Arbeitsspeicher; verschlüsselte Zustellwarteschlange	Betriebsstätte	Fallabschluss / 5 Min. Untätigkeit

Webportal-Datenbank (Scalingo)	Stammdaten, versiegelte Terminkontakte, pseudonyme Zähl­daten — keine Gesundheitsdaten im Klartext	Frankreich	Terminbuchung 30 Tage; Impfbuchung 90 Tage; Benachrichtigungen 7 Tage
Organisationsspeicher (DoctorBox-Infrastruktur)	Ende-zu-Ende verschlüsselte Fallakten — sämtliche Gesundheitsdaten liegen ausschließlich hier und ausschließlich verschlüsselt	Deutschland (Rechenzentrum Noris Network AG, Nürnberg)	Aufbewahrung nach § 630f Abs. 3 BGB (10 Jahre), danach Löschung
Fehlertelemetrie (DoctorBox-Infrastruktur)	Diagnosedaten ohne Personenbezug	Deutschland	90 Tage

E. Verarbeitungen ohne Personenbezug

Zähl- und Statistikdatensätze (Durchläufe der Ersteinschätzung, Vitalwert- und Zahlungszählung, Netzanfragen) enthalten ausschließlich zufällige Kennungen, Zeitstempel und Kategorien. Ein Rückschluss auf betroffene Personen ist ohne die verschlüsselte Fallakte nicht möglich.

Anlage 2 — Unterauftragsverarbeiter

Stand: 06.08.2026

A. Genehmigte Unterauftragsverarbeiter

Unternehmen	Leistung	Datenkategorien	Ort
Noris Network AG, Nürnberg	Rechenzentrumsbetrieb der DoctorBox-Infrastruktur (Organisationsspeicher der Fallakten, Identitätsdienst)	Gesundheitsdaten ausschließlich in Ende-zu-Ende-verschlüsselter Form ; Anmeldedaten des Apothekenpersonals	DE
Scalingo SAS, Straßburg	Hosting des Webportals (Anwendung, Datenbank, Zwischenspeicher)	Apotheken-Stammdaten, versiegelte Terminkontakte, pseudonyme Zähl­daten — keine Gesundheitsdaten im Klartext	FR
XUND Solutions GmbH, Wien	Strukturierte medizinische Ersteinschätzung	Symptom- und Anamnesedaten ohne Identitätsdaten	AT

Sendinblue SAS (Brevo), Paris	Versand von Bestätigungs-, Erinnerungs- und Zugangs-E-Mails	Name, E-Mail-Adresse, Terminzeitpunkt, Leistungsart	FR
Mediwave (Shen.AI)	Kamerabasierte Vitalwerte-Messung (nur bei freigeschaltetem Modul)	Kamerabild zur Verarbeitung, pseudonyme Laufkennung; Rückgabe nur abgeleiteter Messwerte	EU

Sämtliche Unterauftragsverarbeiter verarbeiten in der Europäischen Union bzw. im Europäischen Wirtschaftsraum. Alle Unterauftragsverarbeiter mit möglichem Zugang zu Berufsgeheimnissen sind nach § 6 Abs. 4 i. V. m. § 5 auf Vertraulichkeit und Berufsgeheimnis verpflichtet.

B. Zusätzlich eingesetzte Dienste der Auftragsverarbeiterin

Der Identitätsdienst (Anmeldung von Personal und Tablets), der Organisationsspeicher (Ablage der ausschließlich verschlüsselten Fallakten) und die Fehlertelemetrie werden von der Auftragsverarbeiterin bzw. mit ihr verbundenen Unternehmen auf eigener Infrastruktur betrieben; sie läuft im Rechenzentrum der Noris Network AG, Nürnberg (Anlage 2 Abschnitt A). Das Webportal bei Scalingo hält keine Gesundheitsdaten im Klartext. Sämtliche Dienste unterliegen den Maßnahmen nach § 7.

C. Empfänger ohne Auftragsverarbeitung

Adressvervollständigung. Zur Vervollständigung der Anschriftseingabe wird die eingegebene Zeichenfolge an einen quelloffenen Ortsverzeichnisdienst gesendet. Übertragen werden ausschließlich diese Zeichenfolge sowie Sprache und Trefferzahl — kein Name, kein Geburtsdatum, keine Versichertennummer, keine Fall- oder Sitzungskennung. Die Anfrage geht vom Tablet der Apotheke aus. Für den Empfänger ist eine Ortsangabe ohne Zuordnungsmerkmal keiner identifizierbaren natürlichen Person zuzuordnen (Maßstab EuGH, Rs. C-582/14 — Breyer); eine Auftragsverarbeitung nach Art. 28 DSGVO liegt nicht vor.

Anlage 3 — Ansprechpartner und Weisungsberechtigte

Verantwortliche (Apotheke)

Rolle	Name	Kontakt
Apothekenleitung	_____	_____
Weisungsberechtigt	_____	_____
Datenschutzbeauftragte(r)	_____	_____
Empfänger von Meldungen nach § 9	_____	_____

Betriebsstätte / IK	_____	_____
---------------------	-------	-------

Auftragsverarbeiterin (DoctorBox Leuchtturm GmbH)

Rolle	Name	Kontakt
Weisungsempfänger und Meldestelle	_____	datenschutz@doctorbox.de
Datenschutzbeauftragte(r)	_____	_____

Anlage 4 — Muster einer Verpflichtungserklärung

(zu § 4 Abs. 2 und § 5 Abs. 4)

Verpflichtung auf Vertraulichkeit und auf das Berufsgeheimnis

Frau/Herr _____ wird im Rahmen ihrer/seiner Tätigkeit für die DoctorBox Leuchtturm GmbH mit personenbezogenen Daten befasst, die dem Berufsgeheimnis von Apothekerinnen und Apothekern (§ 203 Abs. 1 Nr. 1 StGB) unterliegen.

1. Ich verpflichte mich, über alle mir bekannt werdenden personenbezogenen Daten und Geheimnisse Stillschweigen zu bewahren und sie ausschließlich zu den Zwecken zu verarbeiten, zu denen ich beauftragt bin.
2. Ich nehme von solchen Daten nur Kenntnis, soweit dies zur Erfüllung meiner Aufgaben erforderlich ist.
3. **Ich bin darüber belehrt worden, dass ich mich nach § 203 Abs. 4 Satz 1 StGB strafbar mache, wenn ich ein fremdes Geheimnis unbefugt offenbare, das mir bei der Ausübung meiner Tätigkeit bekannt geworden ist.** Der Strafrahmen beträgt Freiheitsstrafe bis zu einem Jahr oder Geldstrafe.
4. Ich bin darüber belehrt worden, dass Verstöße gegen datenschutzrechtliche Vorschriften zudem nach Art. 83, 84 DSGVO und §§ 42, 43 BDSG geahndet werden können und arbeitsrechtliche Konsequenzen nach sich ziehen können.
5. Diese Verpflichtung gilt über das Ende meines Beschäftigungs- bzw. Auftragsverhältnisses hinaus zeitlich unbegrenzt fort.

Ort, Datum _____ Unterschrift _____

Anlage 5 — Mitwirkungspflichten der Verantwortlichen

(zu § 2 Abs. 4; überwiegend aus den Vorgaben der ABDA zur assistierten Telemedizin. Voraussetzung des vereinbarten Schutzniveaus.)

#	Pflicht
M1	Bereitstellung eines Raumes, in dem weder Mithören noch Einsehen möglich ist
M2	Nutzung des Gerätes ausschließlich für die Videosprechstunde bzw. die aTM-Anwendung
M3	Betrieb außerhalb des regulären Apothekennetzes (separates WLAN oder Netzsegmentierung)
M4	Beschränkung auf die erforderlichen Funktionen; automatische Sperrung nicht benötigter Websites
M5	USB-Anschlüsse deaktiviert oder gesperrt
M6	Aktueller Virenschutz und aktive Firewall
M7	Betriebssystem- und Sicherheitseinstellungen für Patientinnen und Patienten nicht änderbar
M8	Während der Konsultation ist die versicherte Person allein im Raum und bedient das Gerät selbst
M9	Kiosk-Modus auf Android-Geräten über die eigene Geräteverwaltung erzwingen; auf iOS geführten Zugriff aktiv halten
M10	Vergabe eines starken Tablet-Administrationspassworts bei Inbetriebnahme; sichere Verwahrung der DoctorBox-PIN, getrennt von der Betriebsstätte
M11	Benennung einer/eines Datenschutzbeauftragten (§ 38 Abs. 1 S. 2 BDSG)
M12	Information der Betroffenen nach Art. 13 DSGVO
M13	Führung personenbezogener Benutzerkonten je Beschäftigtem; keine Sammelkonten
M14	Verpflichtung des eigenen Personals auf Vertraulichkeit und Berufsgeheimnis; unverzügliche Sperrung verlorener Geräte über den Wiederverbindungscode

Anlage 6 — Rollenabgrenzung

Nicht jede Datenübermittlung im Rahmen der Leistung ist eine Auftragsverarbeitung. Für die folgenden Empfänger ist die Auftragsverarbeiterin nicht verantwortlich; sie handeln als eigenständig Verantwortliche.

Empfänger	Rolle	Begründung
Ärztliche Leistungserbringer (Videosprechstunde)	Eigenständig Verantwortliche	Die ärztliche Behandlung erfolgt in eigener fachlicher und rechtlicher Verantwortung; die Apotheke stellt Raum, Technik und Begleitung. Für die Videosprechstunde werden die vollständigen Falldaten an das teilnehmende MVZ bzw. die

		Praxis übermittelt.
Terminvermittlungs- und Videodienstanbieter der Ärzteseite	Auftragsverarbeiter der Arztseite	Vertragsbeziehung besteht zwischen Arzt/MVZ und Anbieter
Praxis-Terminportal (Buchung im Formular der Praxis)	Auftragsverarbeiter der Praxis	Die Patientin gibt ihre Daten unmittelbar im Formular der Praxis ein; die Anwendung befüllt lediglich Felder vor
Zahlungsdienstleister	Eigenständig Verantwortlicher	Zahlungsdiensteaufsichtsrechtliche Eigenverantwortung; Vertragsbeziehung besteht zwischen Apotheke und Zahlungsdienstleister

Wichtig für die Verantwortliche: Für die Übermittlung an eigenständig Verantwortliche benötigt sie eine eigene Rechtsgrundlage. Die Anwendung holt hierfür die Einwilligung der betroffenen Person ein und dokumentiert sie mit Zeitpunkt und Textfassung.

Unterschriften

Ort, Datum _____

Für die Verantwortliche _____

Für die Auftragsverarbeiterin _____