

Datenschutz-Folgenabschätzung (DSFA)

nach Art. 35 DSGVO — Vorlage für Apotheken, die DoctorBox aTM einsetzen

Dok-ID	DBX-DSFA-001
Fassung	1.0
Stand	06.08.2026
Verantwortliche	(Apotheke — einzutragen)
Erstellt von	DoctorBox Leuchtturm GmbH als Auftragsverarbeiterin (Unterstützung nach Art. 28 Abs. 3 lit. f DSGVO)
Geprüft durch DSB	☐ (Datum, Name — Art. 35 Abs. 2 DSGVO)
Freigegeben durch	☐ (Apothekenleitung)
Nächste Überprüfung	spätestens 12 Monate nach Freigabe oder bei wesentlicher Produktänderung

1. Anlass und Erforderlichkeitsprüfung (Schwellwertanalyse)

(Art. 35 Abs. 1, Abs. 3 lit. b, Abs. 4 DSGVO)

1.1 Zuordnung zur Muss-Liste der Datenschutzkonferenz

Die DSK-Liste der Verarbeitungsvorgänge nach Art. 35 Abs. 4 DSGVO (Version 1.1, Stand 17.10.2018) ist an **vier** Stellen einschlägig:

Nr.	Wortlaut (verkürzt)	Bezug zum Verfahren
16	Verarbeitung von Daten nach Art. 9 Abs. 1 ..., sofern eine nicht einmalige Datenerhebung mittels innovativer Nutzung von Sensoren oder mobiler Anwendungen stattfindet und diese Daten von einer zentralen Stelle empfangen und aufbereitet werden. Typisches Einsatzfeld: Einsatz von Telemedizin-Lösungen zur detaillierten Bearbeitung von Krankheitsdaten.	Volltreffer. Genau der Kern des Verfahrens.
17	Verarbeitung von Daten nach Art. 9 Abs. 1 ..., sofern durch den Anbieter neue Technologien verwendet werden.	Kamerabasierte Vitalwerte-Messung (rPPG).

3	Verarbeitungen, bei denen Daten von Berufsgeheimnisträgern verarbeitet werden.	Apothekerliches Berufsgeheimnis, § 203 Abs. 1 Nr. 1 StGB.
11	Verarbeitungen mit KI-gestützter Interaktion mit betroffenen Personen.	Strukturierte, dialogbasierte Ersteinschätzung.

Negativabgrenzung: Nr. 1 (biometrische Identifizierung) greift **nicht** — die Kameramessung dient der Erhebung von Vitalparametern, nicht der eindeutigen Identifizierung einer Person; es entsteht kein biometrisches Template.

1.2 Gegenprüfung anhand der neun Kriterien der Art.-29-Gruppe (WP 248 rev.01)

#	Kriterium	erfüllt
1	Bewerten oder Einstufen (Scoring/Profiling)	teilweise — Zuordnung zu Dringlichkeitskategorien
2	Automatisierte Entscheidungsfindung mit Rechtswirkung	nein — die ärztliche Entscheidung trifft ausschließlich ein Mensch
3	Systematische Überwachung	nein
4	Vertrauliche bzw. höchst persönliche Daten	ja
5	Datenverarbeitung in großem Umfang	je nach Apotheke; im Verbund über die Plattform: ja
6	Abgleich oder Zusammenführung von Datensätzen	teilweise — Ersteinschätzung + Termindaten + Vitalwerte
7	Daten zu schutzbedürftigen Betroffenen	ja — Patientinnen und Patienten, ggf. Minderjährige ab 12 J. (Impfung)
8	Innovative Nutzung oder Anwendung neuer Technologien	ja
9	Betroffene an der Ausübung eines Rechts gehindert	nein

Ergebnis: Vier bis sechs der neun Kriterien sind erfüllt; bereits zwei begründen regelmäßig die DSFA-Pflicht. Zusammen mit der Muss-Liste steht fest:

Die Verarbeitung ist datenschutz-folgenabschätzungspflichtig.

1.3 Rechtsfolge für die Apotheke

Weil die Verarbeitung einer DSFA unterliegt, ist die Apotheke nach **§ 38 Abs. 1 Satz 2 BDSG unabhängig von der Zahl ihrer Beschäftigten verpflichtet, eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen**. Auf den Streit, ob eine einzelne Apotheke „umfangreich“ im Sinne des Art. 37 Abs. 1 lit. c DSGVO verarbeitet (Erwägungsgrund 91 nimmt einzelne Apotheker aus), kommt es damit nicht an.

2. Beteiligte und Rollen

Beteiligte	Rolle	Grundlage
Apotheke	Verantwortliche	Art. 4 Nr. 7 DSGVO
DoctorBox Leuchtturm GmbH	Auftragsverarbeiterin	Art. 4 Nr. 8, Art. 28 DSGVO; AVV DBX-AVV-001
Unterauftragsverarbeiter	Hosting, Ersteinschätzung, E-Mail-Versand, Vitalwerte, technische Postfächer, Fernsignatur	Anlage 3 des AVV
Ärztliche Leistungserbringer und deren Dienstleister	eigenständig Verantwortliche	Anlage 6 des AVV
Zahlungsdienstleister	eigenständig Verantwortlicher	Anlage 6 des AVV

Einbindung des DSB (Art. 35 Abs. 2): ☐ Datum, Stellungnahme, ggf. begründete Abweichung eintragen.

Standpunkt der betroffenen Personen (Art. 35 Abs. 9): Eine Befragung betroffener Personen ist ☐ erfolgt am ____ / ☐ unterblieben, weil ____ (Begründung dokumentieren — „gegebenenfalls“ bedeutet nicht „nie“).

3. Systematische Beschreibung der Verarbeitung

(Art. 35 Abs. 7 lit. a DSGVO)

3.1 Zwecke

1. Durchführung und Abrechnung der assistierten Telemedizin nach § 129 Abs. 5h SGB V (strukturierte Ersteinschätzung, Unterstützung während einer Videokonsultation)
2. Vermittlung und Begleitung ärztlicher Videosprechstunden
3. Durchführung und Dokumentation von Schutzimpfungen nach § 20c IfSG
4. Online-Terminvereinbarung für den Apothekenbesuch
5. Optionale Erhebung orientierender Vitalparameter
6. Entgegennahme der Zahlung für Selbstzahlende und Privatversicherte
7. Betrieb, Fehlerbehebung und Nachweisführung

3.2 Ablauf einer Fallbearbeitung

Patient:in am Tablet in der Apotheke

|

└─ 1. Versichertenkarte optisch erfassen (nur auf dem Gerät; das

|

Kamerabild wird nach der Auswertung sofort gelöscht)

└─ 2. Personendaten prüfen und ergänzen

└─ 3. Behandlungsvereinbarung + Einwilligung, handschriftlich unterzeichnet

- └─ 4. [optional] Vitalwerte-Messung (ca. 1 Minute Kamera)
- └─ 5. Strukturierte Ersteinschätzung ───────────▶ Anbieter der
 - | (Symptome, OHNE Identitätsdaten) Ersteinschätzung
- └─ 6. Ergebnis: Videosprechstunde / Selbstbehandlung / Notfall
 - |
- └─ 7a. Terminvermittlung ───────────▶ ärztlicher
 - | (Identität, Versicherung, Beschwerden) Leistungserbringer
 - | (eigenständig
 - | verantwortlich)
- └─ 7b. Videosprechstunde im separaten Raum
- └─ 8. [Selbstzahler/PKV] Kartenzahlung ───────────▶ Zahlungsdienstleister
 - |
- └─ 9. Fallakte Ende-zu-Ende verschlüsseln und übertragen
 - | └─▶ Organisationsspeicher der Apotheke
 - | (lesbar nur mit der PIN der Apotheke)
 - |
- └─ 10. Sitzung beenden → vollständige Löschung aller Falldaten
 - | auf dem Gerät (auch bei Zeitablauf nach 5 Minuten Inaktivität)

3.3 Datenkategorien, Empfänger, Speicherorte, Fristen

Siehe **Anlage 1 des AVV** (DBX-AVV-001). Die dortigen Abschnitte A bis E sind Bestandteil dieser DSFA.

3.4 Prägende Architekturentscheidungen

Drei Entscheidungen bestimmen das Risikoprofil maßgeblich und werden deshalb vorangestellt:

1. **Ende-zu-Ende-Verschlüsselung der Fallakte.** Jede Fallakte wird mit einem zufälligen Schlüssel verschlüsselt; dieser Schlüssel wird ausschließlich an das Organisationszertifikat der Apotheke adressiert. Der zugehörige private Schlüssel ist mit einer PIN geschützt, die nur die Apotheke kennt und die nirgends gespeichert wird. Ohne diese PIN sind die Inhalte auch für die Auftragsverarbeiterin nicht lesbar. *(Einschränkung: siehe Risiko R4.)*
2. **Kein Klartext-Patientendatenbestand in der Portal-Datenbank.** Personenbezug entsteht dort nur pseudonym (Hashwerte) oder versiegelt. Statistik- und Abrechnungszahlen sind personenbezugsfrei ausgelegt.
3. **Der Kiosk vergisst.** Falldaten existieren auf dem Tablet nur im Arbeitsspeicher; sie werden beim Fallabschluss und bei Inaktivität nach fünf Minuten vollständig verworfen, einschließlich Zwischenspeichern des Webbrowsers.

4. Notwendigkeit und Verhältnismäßigkeit

(Art. 35 Abs. 7 lit. b DSGVO)

Prüfpunkt	Bewertung
Rechtsgrundlage Art. 6	Art. 6 Abs. 1 lit. b (Behandlungs-/Nutzungsverhältnis) und lit. c i. V. m. § 129 Abs. 5h SGB V, § 300 SGB V (Abrechnung)
Rechtsgrundlage Art. 9	lit. h (Gesundheitsversorgung) i. V. m. § 22 Abs. 1 Nr. 1 lit. b BDSG; für die optionale Vitalwerte-Messung zusätzlich lit. a (ausdrückliche Einwilligung)
Zweckbindung	Verarbeitung ausschließlich zu den in 3.1 genannten Zwecken; vertraglicher Ausschluss der Nutzung für eigene Zwecke der Auftragsverarbeiterin (§ 1 Abs. 4 AVV)
Erforderlichkeit	Die Ersteinschätzung ist gesetzlich vorgesehene Leistung; die erhobenen Identitäts- und Versicherungsdaten sind zur Abrechnung nach § 300 SGB V erforderlich
Datenminimierung	Ersteinschätzung erhält keine Identitätsdaten; Vitalwerte-Anbieter erhält keine Identitätsdaten; Zahlungsdaten ohne Kartennummer; Kamerabild der Versichertenkarte wird nicht gespeichert
Speicherbegrenzung	Gerät: bis Fallabschluss/5 Min. · Terminkontakte: 30 Tage · Impfbuchungen: 90 Tage · Zugangs-Postfächer: 7 Tage · Fallakte: 10 Jahre nach § 630f Abs. 3 BGB, danach Löschung
Verhältnismäßigkeit i. e. S.	Der Eingriff steht in angemessenem Verhältnis: Die Alternative — keine wohnortnahe Versorgung bzw. Papierdokumentation ohne Verschlüsselung — wäre für die Betroffenen nicht milder.
Freiwilligkeit	Die Nutzung ist für Patientinnen und Patienten freiwillig; die Vitalwerte-Messung ist ein optionaler Zusatzschritt, dessen Ablehnung den Ablauf nicht behindert.

5. Risiken für die Rechte und Freiheiten der betroffenen Personen

(Art. 35 Abs. 7 lit. c DSGVO)

5.1 Bewertungsmaßstab

Angelehnt an die Orientierungshilfe des Bayerischen Landesbeauftragten für den Datenschutz, Ausbaustufe L (wegen Gesundheitsdaten):

Eintrittswahrscheinlichkeit (E): 1 geringfügig · 2 überschaubar · 3 substanziell · 4 groß **Schwere (S):** 1 geringfügig · 2 überschaubar · 3 substanziell · 4 groß

Risikoindex = E × S → 1–3 gering · 4–7 mittel · 8–11 hoch · 12–16 sehr hoch

Bewertet wird zuerst das **Ausgangsrisiko ohne Maßnahmen**, dann das **Restrisiko** nach Umsetzung der Maßnahmen aus Abschnitt 6. (Der häufigste Prüfungsmangel ist, nur das Restrisiko zu dokumentieren.)

Gliederung nach den sieben Gewährleistungszielen des Standard-Datenschutzmodells (SDM 3.0).

5.2 Risikokatalog

ID	Gewährleistungsziel	Risikoszenario	E	S	Ausgangsindex	Rest-index
R1	Vertraulichkeit	Dritte im Offizinbereich hören oder sehen die Eingaben bzw. die Videosprechstunde mit	4	4	16	4
R2	Vertraulichkeit	Verlust oder Diebstahl des Tablets mit noch nicht zugestellten Falldaten	2	4	8	2
R3	Vertraulichkeit	Unbefugter Zugriff auf ein Portalkonto (Phishing, schwaches Passwort)	3	4	12	6
R4	Vertraulichkeit	Zugriff auf Fallinhalte über die Verschlüsselungskomponente, die die Inhaltsschlüssel transient verarbeitet	2	4	8	4
R5	Vertraulichkeit	Übermittlung der vollständigen Falldaten an das teilnehmende MVZ bzw. die Praxis erfolgt ohne wirksame Einwilligung oder an den falschen Empfänger	2	4	8	4
R6	Vertraulichkeit	Ortsanfrage der Adressvervollständigung an einen externen Dienst (<i>Bewertung: keine identifizierenden Merkmale, siehe 5.4</i>)	4	1	4	2
R7	Vertraulichkeit	Drittlandtransfer (USA) über technische Postfächer mit Terminbezug	3	3	9	6
R8	Vertraulichkeit	Kamerastrom der Vitalwerte-Messung verlässt unbemerkt das Gerät	2	4	8	4
R9	Vertraulichkeit	Unbefugter Zugriff auf die Datenbank ermöglicht über den dort im Klartext gespeicherten Geräte-Zugangsschlüssel die Nutzung von Schnittstellen (u. a. E-Mail-Versand)	2	3	6	4
R10	Verkettbarkeit	Pseudonyme Verknüpfungsdaten erlauben das Wiedererkennen einer Person, solange sie vorgehalten werden	3	3	9	6
R11	Verkettbarkeit	Terminbuchungen bleiben über einen stabilen Kontakt-Hashwert auch nach Entfernen des Klarnamens wiedererkennbar	2	2	4	2
R12	Datenminimierung	Aufbewahrung der Fallakten im Organisationsspeicher über die gesetzliche Frist hinaus	4	3	12	6
R1	Datenminimierung	Nicht zustellbare Falldatensätze verbleiben unbefristet	3	3	9	4

3	ng	verschlüsselt auf dem Gerät				
R1 4	Verfügbarkeit	Verlust der PIN führt zum endgültigen Verlust der Behandlungsdokumentation (§ 630f BGB)	3	4	12	6
R1 5	Integrität	Fehlerhafte Zuordnung von Falldaten (z. B. Karten-Fehlerkennung) führt zu falscher Dokumentation	2	4	8	4
R1 6	Integrität	Fehleinschätzung der Dringlichkeit; Patient:in versäumt notwendige Notfallversorgung	2	4	8	4
R1 7	Transparenz	Betroffene erkennen nicht, welche Daten an welchen Empfänger fließen (mehrere eigenständig Verantwortliche)	3	2	6	2
R1 8	Intervenierbarkeit	Auskunfts- oder Löschbegehren kann nicht erfüllt werden, weil die Apotheke ihre Daten ohne PIN nicht lesen kann	2	3	6	4
R1 9	Vertraulichkeit	Beschlagnahme oder behördlicher Zugriff auf Server mit Berufsgeheimnisdaten	1	4	4	2
R2 0	Verfügbarkeit	Ausfall der Plattform während einer laufenden Versorgung	3	2	6	4

5.3 Risiken mit besonderem Handlungsbedarf

Fünf Risiken tragen ein Restrisiko von 6 und sind vor dem Produktivbetrieb zu behandeln: **R3, R7, R10, R12, R14**. Sie sind in Abschnitt 7 gesondert bewertet.

5.4 Geprüfte, aber nicht als Risiko gewertete Sachverhalte

(Dokumentiert, weil die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO auch die begründete Negativentscheidung verlangt.)

Adressvervollständigung (R6). An den Dienst werden ausschließlich die eingegebene Zeichenfolge sowie Sprache und Trefferzahl übertragen — kein Name, kein Geburtsdatum, keine Versichertennummer, keine Fall- oder Sitzungskennung. Die Anfrage geht vom Tablet der Apotheke aus; die Absender-IP ist die der Apotheke, nicht die einer betroffenen Person. Für den Empfänger ist eine Ortsangabe ohne Zuordnungsmerkmal keiner identifizierbaren natürlichen Person zuzuordnen; Mittel, die vernünftigerweise zur Identifizierung eingesetzt werden könnten, stehen ihm nicht zur Verfügung (Maßstab EuGH, Rs. C-582/14 — Breyer). Eine Auftragsverarbeitung nach Art. 28 DSGVO liegt nicht vor. Der Dienst kommt ohne Schlüssel, Konto und Wiedererkennungsmerkmale aus. Verbleibender Punkt: Der Betreiber dokumentiert Protokollierung und Aufbewahrung nicht; eine optionale Härtung besteht im Eigenbetrieb der quelloffenen Software.

Optische Erfassung der Versichertenkarte. Die Auswertung erfolgt vollständig auf dem Gerät; das Kamerabild wird unmittelbar nach der Auswertung gelöscht und verlässt das Tablet nie.

Automatisierte Entscheidungen (Art. 22 DSGVO). Die Ersteinschätzung kategorisiert die Dringlichkeit, trifft aber keine Entscheidung mit rechtlicher Wirkung; die ärztliche Entscheidung bleibt ausnahmslos

einem Menschen vorbehalten.

6. Abhilfemaßnahmen

(Art. 35 Abs. 7 lit. d DSGVO)

6.1 Maßnahmen der Auftragsverarbeiterin

Die Maßnahmen sind in **§ 7 des AVV** (DBX-AVV-001) geregelt. Zuordnung zu den Risiken:

Risiko	Maßnahme
R1	Kiosk-Betriebsmodus ohne Verlassen der Anwendung; automatische Sitzungsbeendigung nach 5 Minuten; Vorgabe eines uneinsehbaren Raums (Mitwirkungspflicht, Abschnitt 8)
R2	Gerätespeicher verschlüsselt; ausstehende Zustellungen ausschließlich verschlüsselt abgelegt; Administrationsbereich passwortgeschützt; Fernlöschung über die Geräteverwaltung
R3	Passwörter nur als Hashwert gespeichert; Anmeldeversuche begrenzt; Klartext-Patientendaten zusätzlich erst nach separater PIN-Eingabe sichtbar, die nach 15 Minuten Untätigkeit verfällt und nach fünf Fehlversuchen sperrt
R4	Inhaltsschlüssel werden nur transient verarbeitet und nicht gespeichert; die Fallakte ist ohne die PIN der Verantwortlichen nicht lesbar
R5	Übermittlung an das MVZ bzw. die Praxis nur nach dokumentierter Einwilligung der betroffenen Person; Empfänger als eigenständig Verantwortliche (Anlage 6 AVV)
R6	An den Adressdienst gehen keine identifizierenden Merkmale; die Anfrage erfolgt von der Apotheken-IP (Abschnitt 5.4)
R7	Standardvertragsklauseln und Transfer-Folgenabschätzung; Postfächer werden nach 7 Tagen gelöscht; übermittelt werden nur Terminbestätigungen ohne Klarnamen des Postfachs
R8	Übermittlung nur einer zufälligen Laufkennung, keine Identitätsdaten; keine Speicherung von Bildern oder Rohsignal; Aktivierung des Moduls nur nach Freischaltung durch die Verantwortliche
R9	Zugangsschlüssel je Gerät einzeln widerrufbar; Schnittstellen mit Nutzungsbegrenzung; Datenbank nicht aus dem Internet erreichbar
R10	Pseudonyme Verknüpfungsdaten werden turnusmäßig bereinigt; kein Klarname enthalten
R11	Hashwert mit geheimem Schlüssel gebildet; dient allein der Missbrauchsbegrenzung
R12	Aufbewahrung nach § 630f Abs. 3 BGB (10 Jahre), anschließend Löschung; Löschweg festgelegt
R13	Nicht zustellbare Datensätze liegen verschlüsselt vor und werden nach einer Höchstaufbewahrung gelöscht

R14	Ausdruckbares PIN-Dokument bei der Einrichtung; Bestätigungspflicht der Apothekenleitung; Hinweis auf Unwiederbringlichkeit; getrennte Verwahrung als Mitwirkungspflicht
R15	Erfasste Kartendaten werden dem Personal zur Prüfung angezeigt und sind korrigierbar; Unterschrift bestätigt die Richtigkeit
R16	Ergebnis der Ersteinschätzung führt bei Notfallverdacht zu einem eindeutigen Hinweis; die ärztliche Entscheidung bleibt einem Menschen vorbehalten; keine automatisierte Entscheidung im Sinne des Art. 22 DSGVO
R17	Einwilligungen werden je Empfänger einzeln, mit Zeitpunkt und Textfassung erhoben; Informationsblatt für Betroffene
R18	Fallakten sind über das Portal nach PIN-Eingabe im Klartext einsehbar und exportierbar
R19	Vertragliche Verpflichtung nach § 203 StGB, Hinweis auf das Beschlagnahmeverbot nach § 97 Abs. 2 StPO, dokumentierter Eskalationsprozess (§ 5 Abs. 6 AVV)
R20	Warteschlange mit automatischer Wiederholung; kein Datenverlust bei Ausfall; Überwachung mit Alarmierung

6.2 Mitwirkungspflichten der Verantwortlichen

Siehe Abschnitt 8. Ohne sie wird das in Abschnitt 7 angenommene Restrisiko **nicht** erreicht.

7. Bewertung des Restrisikos und Entscheidung nach Art. 36 DSGVO

7.1 Gesamtbewertung

Nach Umsetzung der Maßnahmen aus Abschnitt 6 und der Mitwirkungspflichten aus Abschnitt 8 liegt das Restrisiko für alle 20 betrachteten Szenarien im **geringen bis mittleren** Bereich. Kein Szenario erreicht nach Umsetzung der Maßnahmen den Bereich „hoch“.

7.2 Entscheidung über die vorherige Konsultation

Art. 36 Abs. 1 DSGVO verlangt die Konsultation der Aufsichtsbehörde nur dann, wenn das **Restrisiko** nach Umsetzung aller Maßnahmen weiterhin **hoch** ist. Ein hohes Ausgangsrisiko allein löst die Konsultationspflicht nicht aus.

Szenario	Ergebnis
Alle Maßnahmen aus Abschnitt 6 und alle Mitwirkungspflichten aus Abschnitt 8 sind umgesetzt	Kein Restrisiko im Bereich „hoch“ (≥ 8) → Konsultation nach Art. 36 nicht erforderlich
Die offenen Punkte zu R5 (Klartextspeicher) und R12 (fehlende Löschfrist) sind nicht behoben	Restrisiko R5 verbleibt bei 8 = „hoch“ → Konsultation erforderlich oder Modul nicht einsetzen
Die Mitwirkungspflichten (insbesondere separater	Restrisiko R1 verbleibt bei 16 = „sehr hoch“ →

Raum und Netztrennung) werden **nicht** eingehalten

Einsatz unzulässig

Ergebnis dieser Vorlage: Die Konsultation nach Art. 36 DSGVO ist **nicht erforderlich**, sofern die offenen Punkte vor dem Produktivbetrieb geschlossen und die Mitwirkungspflichten eingehalten werden. Andernfalls ist mit einem Vorlauf von bis zu **14 Wochen** zu rechnen (acht Wochen Regelfrist, verlängerbar um sechs Wochen).

7.3 Überprüfung

Die DSFA ist zu überprüfen bei: neuem Funktionsmodul, neuem Unterauftragsverarbeiter, neuem Verarbeitungsort oder Drittlandbezug, neuer Datenkategorie, sicherheitsrelevantem Vorfall — spätestens jedoch nach zwölf Monaten.

8. Mitwirkungspflichten der Apotheke

(Diese Anforderungen ergeben sich überwiegend aus den Vorgaben der ABDA zur assistierten Telemedizin und liegen außerhalb des Einflussbereichs der Auftragsverarbeiterin. Sie sind Voraussetzung des in Abschnitt 7 angenommenen Restrisikos.)

#	Pflicht	Risiko- Bezug
M1	Bereitstellung eines Raumes, in dem weder Mithören noch Einsehen möglich ist	R1
M2	Nutzung des Gerätes ausschließlich für die Videosprechstunde bzw. die aTM-Anwendung	R1, R2
M3	Betrieb außerhalb des regulären Apothekennetzes (separates WLAN oder Netzsegmentierung)	R2, R9
M4	Beschränkung auf die erforderlichen Funktionen; automatische Sperrung nicht benötigter Websites	R2
M5	USB-Anschlüsse deaktiviert oder gesperrt	R2
M6	Aktueller Virenschutz und aktive Firewall	R2
M7	Betriebssystem- und Sicherheitseinstellungen für Patientinnen und Patienten nicht änderbar	R1, R2
M8	Während der Konsultation ist die versicherte Person allein im Raum und bedient das Gerät selbst	R1
M9	Sichere Verwahrung des PIN-Dokuments; getrennte Aufbewahrung von der Betriebsstätte empfohlen	R14
M10	Benennung einer/eines Datenschutzbeauftragten (§ 38 Abs. 1 S. 2 BDSG)	—

M1 1	Information der Betroffenen nach Art. 13 DSGVO (Aushang und mündlicher Hinweis)	R17
M1 2	Festlegung der Aufbewahrungsfrist für die Behandlungsdokumentation und regelmäßige Löschung	R12
M1 3	Verpflichtung des eigenen Personals auf Vertraulichkeit und Berufsgeheimnis	R1, R19

9. Freigabe

	Name	Datum	Unterschrift
Erstellt (Vorlage)	DoctorBox Leuchtturm GmbH	06.08.2026	—
Stellungnahme DSB	☐	☐	☐
Geprüft	☐	☐	☐
Freigegeben (Apothekenleitung)	☐	☐	☐

Änderungshistorie

Fassung	Datum	Änderung
1.0	06.08.2026	Ersterstellung