Prüfleitfaden

Auswahl eines IT-Dienstleisters für Zahnarztpraxen

Umsetzung der IT-Sicherheitsrichtlinie nach § 390 SGB V

Zielgruppe	Niedergelassene zahnärztliche Praxen (alle Fachbereiche)
Rechtsgrundlage	IT-Sicherheitsrichtlinie der KZBV nach § 390 SGB V (Inkrafttreten 02.07.2025, verbindliche Umsetzung ab 02.01.2026)
Zweck des Dokuments	Strukturierte Prüfung, ob ein ortsnahes IT-Systemhaus die erforderlichen Leistungen erbringen kann. Einsetzbar zur Selbstauskunft eines Anbieters oder als Checkliste im Akquise-Gespräch.
Geltungsbereich	Technische und organisatorische Leistungen eines externen IT-Dienstleisters. Nicht abgedeckt: innerbetriebliche Verantwortlichkeiten der Praxis selbst.
Stand	April 2026

1. Vorbemerkung und Nutzungshinweis

Die Umsetzung der IT-Sicherheitsrichtlinie nach § 390 SGB V ist für alle Vertragszahnarztpraxen verpflichtend. Ein wesentlicher Teil der Anforderungen ist technischer Natur (u. a. Firewall, Virenschutz, Backup, Patchmanagement, Netzwerkdokumentation, Berechtigungskonzepte). Kleinere und mittlere Praxen verfügen in der Regel weder über eigenes IT-Personal noch über die fachliche Expertise, diese Anforderungen selbst zu planen, umzusetzen und dauerhaft nachzuweisen.

Die Gesamtverantwortung für die Einhaltung der Anforderungen verbleibt nach der Richtlinie bei der Praxisleitung. Ein externer IT-Dienstleister kann diese operativ umsetzen, die Verantwortung jedoch nicht übernehmen. Aus diesem Grund ist die Auswahl eines fachlich geeigneten Dienstleisters von erheblicher Bedeutung.

Hinweis: Die KBV/KZBV führt ein Verzeichnis freiwillig zertifizierter Dienstleister nach § 390 SGB V. Eine Zertifizierung ist jedoch nicht verpflichtend; auch nicht zertifizierte Anbieter können die Anforderungen kompetent erfüllen. Dieser Leitfaden dient dazu, die tatsächliche Leistungsfähigkeit sachlich zu prüfen.

1.1 Legende – Priorisierung der Leistungen

MUSS	Ohne diese Leistung kann der Dienstleister die Anforderungen der IT-Sicherheitsrichtlinie nicht oder nicht belastbar unterstützen. Eine Bindung ist ohne Erfüllung dieser Punkte nicht zu empfehlen.
SOLL	Leistungen, die für einen professionellen und wirtschaftlich sinnvollen Praxisbetrieb erwartet werden. Fehlen einzelne Punkte, ist dies im Einzelfall abwägbar (z. B. Erbringung durch Kooperationspartner).
KANN	Zusatzleistungen mit Mehrwert. Nicht zwingend erforderlich; sinnvoll bei größeren Praxen, Spezialisierungen (KFO, OC, MKG) oder besonderen Anforderungen.

Hinweis zur Bewertung:

Die nachfolgenden Tabellen sind als Selbstauskunft des Dienstleisters einsetzbar. Jede Anforderung soll mit „Ja“ oder „Nein“ beantwortet werden. Antworten mit „Teilweise“, „durch Partner“, o. Ä. sind schriftlich zu erläutern und dem Dokument beizufügen. Die Feststellung, dass eine Muss-Anforderung nicht erfüllt wird, ist als Ausschlusskriterium zu behandeln – außer die Praxis kann die Lücke anderweitig und belastbar schließen.

2. Grundlegende Eignung des Dienstleisters

2.1 Unternehmen und Branchenkompetenz

Kat.	Anforderung / Leistungsbeschreibung	Ja	Nein
MUSS	Nachweisbare Erfahrung im Betrieb von IT in Heilberufspraxen (Zahnarzt, Arzt, Psychotherapie) – mind. 3 Referenzkunden aus dem Gesundheitswesen, davon mindestens einer zahnärztlich.	☐	☐
MUSS	Kenntnis der IT-Sicherheitsrichtlinie nach § 390 SGB V einschließlich Anlagen 1, 2 und 5 (Stand der jeweils gültigen Fassung).	☐	☐
MUSS	Kenntnis der datenschutzrechtlichen Rahmenbedingungen der Verarbeitung von Patientendaten (DSGVO, BDSG, ärztliche Schweigepflicht gem. § 203 StGB).	☐	☐
MUSS	Bereitschaft zum Abschluss eines Vertrags zur Auftragsverarbeitung (AVV) nach Art. 28 DSGVO.	☐	☐
MUSS	Abschluss einer Betriebshaftpflicht- und Vermögensschadenhaftpflichtversicherung mit ausreichender Deckungssumme (Richtwert: mind. 1 Mio. € je Schadensfall). Versicherungsnachweis auf Anforderung.	☐	☐
SOLL	Eintragung im KBV/KZBV-Verzeichnis freiwillig zertifizierter Dienstleister nach § 390 SGB V oder gleichwertige Qualifikation (z. B. BSI-Grundschutz-Praktiker, TÜV-Zertifizierung IT-Sicherheit Arztpraxis).	☐	☐
SOLL	Kooperation oder Erfahrung mit gängigen zahnärztlichen Praxisverwaltungssystemen (PVS) – z. B. DAMPSOFT, CHARLY, ivoris, Z.1 pro	☐	☐
SOLL	Schriftlich dokumentierte Unternehmensprozesse (ISO 9001 oder vergleichbares QM-System).	☐	☐
SOLL	Bestand des Unternehmens seit mindestens 5 Jahren am Markt; nachvollziehbare Eigentümer-/Geschäftsführungsstruktur.	☐	☐
KANN	Zertifizierung nach ISO/IEC 27001 (Informationssicherheits-Managementsystem).	☐	☐
KANN	Mitgliedschaft in Branchenverbänden (z. B. BITMi, Bundesverband IT-Mittelstand) oder dentalspezifischen Arbeitskreisen.	☐	☐

2.2 Ortsnähe und Erreichbarkeit

Für kleine Praxen ist die Fähigkeit des Dienstleisters zu schneller Vor-Ort-Reaktion kritisch, da ein Ausfall der Praxis-IT den Praxisbetrieb in der Regel unmittelbar unterbricht.

Kat.	Anforderung / Leistungsbeschreibung	Ja	Nein
MUSS	Firmensitz oder besetzter Stützpunkt in erreichbarer Entfernung zur Praxis. Richtwert: Anfahrtszeit ≤ 60 Minuten während der üblichen Praxisöffnungs-zeiten.	☐	☐
MUSS	Verbindliche Reaktionszeit bei Totalausfall der Praxis-IT (schriftlich im Service-Level-Agreement fixiert). Richtwert: telefonische Rückmeldung ≤ 1 Stunde, Vor-Ort-Einsatz ≤ 4 Stunden innerhalb der vereinbarten Servicezeit.	☐	☐
MUSS	Erreichbarkeit des Supports während der regulären Praxiszeiten (mindestens Mo – Fr 07:30 Uhr – 18:00 Uhr) über eine zentrale Hotline (keine Mobilnummer eines Einzeltechnikers).	☐	☐
SOLL	Notfallerreichbarkeit außerhalb der regulären Servicezeiten (z. B. Samstagsprechstunde, Kieferchirurgie mit verlängerten Zeiten) gegen Aufpreis.	☐	☐
SOLL	Mindestens zwei Techniker im Unternehmen, die die Praxis-IT kennen (Vertretungsregelung bei Urlaub/Krankheit).	☐	☐
SOLL	Ticketsystem mit schriftlicher Bestätigung, Status- und Lösungsnachverfol-gung. Zugang für die Praxis per Web-Portal oder E-Mail.	☐	☐
KANN	24/7-Bereitschaft (in der Regel nur für MKG-/OC-Praxen mit Klinikanbindung relevant).	☐	☐

3. Technische Kernleistungen

Die folgenden Leistungen bilden die technische Grundlage zur Umsetzung der Anlagen 1 und 2 der IT-Sicherheitsrichtlinie. Eine kleine oder mittlere Praxis fällt – abhängig von der Zahl ständig mit Datenverarbeitung betrauter Personen – entweder unter die Basisanforderungen (Anlagen 1 + 5) oder zusätzlich unter die Anforderungen der Anlage 2 (ab 6 ständig betrauten Personen).

3.1 Netzwerk und Perimeterschutz

Kat.	Anforderung / Leistungsbeschreibung	Ja	Nein
MUSS	Planung, Installation und Konfiguration einer dedizierten Hardware-Firewall am Übergang zum Internet (A1 der Richtlinie). Keine Nutzung reiner Consumer-Router mit Firewall-Funktion.	☐	☐
MUSS	Erstellung und regelmäßige Aktualisierung eines Netzplans der Praxis (Anforderung aus Anlage 1 der Richtlinie).	☐	☐
MUSS	Segmentierung des Praxisnetzes (getrennte Bereiche für Praxis-IT, medizinische Geräte und Gästenetz/WLAN).	☐	☐
MUSS	Absicherung und eigenes Passwort für Management-Zugriffe auf Netzkomponenten (Router, Switches, Access Points); keine Werkseinstellungen.	☐	☐
MUSS	Gesichertes WLAN (WPA2-Enterprise oder mind. WPA3-Personal mit starkem PSK); getrenntes Gäste-WLAN, falls angeboten.	☐	☐
SOLL	VPN-Einrichtung für Fernzugriff (z. B. externer Befund, Home-Office Abrechnung); IPSec oder WireGuard; keine offenen Remote-Desktop-Ports ins Internet.	☐	☐
SOLL	Monitoring der Firewall (Logauswertung, Alarmierung bei Auffälligkeiten).	☐	☐
KANN	Next-Generation-Firewall mit Intrusion Prevention (IPS), Application Control und SSL-Inspection.	☐	☐
KANN	Redundante Internetanbindung (z. B. LTE-Backup) für ausfallkritische Praxen.	☐	☐

3.2 Endgeräte, Server und Betriebssysteme

Kat.	Anforderung / Leistungsbeschreibung	Ja	Nein
MUSS	Beratung und Beschaffung geeigneter Hardware (Workstations, Server, NAS, ggf. Thin Clients) mit eindeutiger Inventarisierung.	☐	☐
MUSS	Einsatz ausschließlich herstellerseitig unterstützter Betriebssysteme (kein Windows mit abgelaufenem Support, keine End-of-Life-Systeme an Patientendaten).	☐	☐
MUSS	Zentrales Patch- und Updatemanagement für Betriebssysteme und Standardanwendungen (Anlage 1: zeitnahe Installation von Sicherheitsupdates).	☐	☐
MUSS	Schriftlich festgelegte Verantwortlichkeit für Updates (A1-15 der Richtlinie, verbindlich ab 02.01.2026).	☐	☐
MUSS	Identifizierung und Meldung von Hard- und Software, für die keine Sicherheitsupdates mehr bereitstehen (A1-16, verbindlich ab 02.01.2026).	☐	☐
SOLL	Zentrale Geräteverwaltung (z. B. Active Directory, Microsoft Intune, alternative MDM-Lösung) ab 6 Mitarbeitern mit DV-Aufgaben.	☐	☐
SOLL	Standardisierte Arbeitsplatz-Images für schnelle Wiederherstellung bei Hardwaredefekt.	☐	☐
KANN	Hardware-as-a-Service / Mietmodelle mit turnusmäßiger Erneuerung.	☐	☐

3.3 Endpoint-Schutz und Malware-Abwehr

Kat.	Anforderung / Leistungsbeschreibung	Ja	Nein
MUSS	Installation, Konfiguration und laufende Pflege eines zentral verwalteten Virenschutzes auf allen Arbeitsplätzen und Servern.	☐	☐
MUSS	Zentrales Monitoring der Endpoint-Security mit Alarmierung bei Infektionen oder ausgebliebenen Updates.	☐	☐
MUSS	Blockade/Management von Wechseldatenträgern (USB-Sticks) gemäß Praxisrichtlinie.	☐	☐
SOLL	EDR-Lösung (Endpoint Detection and Response) mit verhaltensbasierter Erkennung.	☐	☐
SOLL	Application Whitelisting oder entsprechende Härtungsmaßnahmen an Praxis-PCs.	☐	☐
KANN	Anbindung an ein Security Operations Center (SOC) / Managed Detection and Response.	☐	☐

3.4 Datensicherung und Wiederherstellung

Die Richtlinie fordert regelmäßige Backups und seit 02.01.2026 verbindlich auch dokumentierte Wiederherstellungstests. Unvollständige oder nicht getestete Backups gelten als nicht wirksam.

Kat.	Anforderung / Leistungsbeschreibung	Ja	Nein
MUSS	Konzeption und Einrichtung einer automatisierten Datensicherung (Praxisverwaltungssoftware, Röntgen, DVT, sonstige Patientendaten).	☐	☐
MUSS	3-2-1-Prinzip: mindestens drei Kopien, auf zwei unterschiedlichen Medien, davon eine Kopie extern/offline (Schutz gegen Ransomware).	☐	☐
MUSS	Verschlüsselung der externen/ausgelagerten Sicherungen.	☐	☐
MUSS	Regelmäßige, dokumentierte Wiederherstellungstests (mind. jährlich). Vorlage eines Test-Protokolls an die Praxis.	☐	☐
MUSS	Dokumentierte Wiederanlaufzeit (RTO) und maximal toleriertes Datenverlustfenster (RPO), schriftlich mit der Praxis vereinbart.	☐	☐

Kat.	Anforderung / Leistungsbeschreibung	Ja	Nein
SOLL	Cloud-Backup in einem Rechenzentrum mit Standort in Deutschland oder innerhalb der EU; Vertrag konform zu § 393 SGB V (Cloud-Nutzung im Gesundheitswesen).	☐	☐
SOLL	Unveränderliche Backups (Immutable Storage / Object Lock) gegen gezielte Löschung durch Schadsoftware.	☐	☐
KANN	Replikation auf einen zweiten Standort mit automatischer Umschaltung (Disaster-Recovery-Option).	☐	☐

3.5 Identitäts- und Berechtigungsmanagement

Kat.	Anforderung / Leistungsbeschreibung	Ja	Nein
MUSS	Einrichtung individueller Benutzerkonten für jede mit Datenverarbeitung betraute Person (keine Gruppen- oder Sammelkonten).	☐	☐
MUSS	Durchsetzung einer Passwortrichtlinie und technischer Sperre nach Fehlversuchen.	☐	☐
MUSS	Unterstützung eines dokumentierten Prozesses zum Zugangsentzug beim Ausscheiden von Mitarbeitenden (ab 02.01.2026 verbindlich).	☐	☐
MUSS	Trennung von administrativen und Benutzer-Konten; administrative Zugänge nicht für den Praxisalltag.	☐	☐
SOLL	Mehr-Faktor-Authentifizierung (MFA) für administrative Zugänge sowie für Fernzugriffe.	☐	☐
SOLL	Rollen- und Berechtigungskonzept (Zahnarzt, ZMF/ZMV, Verwaltung, Azubi), schriftlich fixiert und nachvollziehbar umgesetzt.	☐	☐
KANN	Single Sign-On (SSO) zwischen PVS, E-Mail und weiteren Anwendungen.	☐	☐
KANN	Privileged Access Management (PAM) für administrative Tätigkeiten.	☐	☐

3.6 E-Mail, Kommunikation, KIM und Internetdienste

Kat.	Anforderung / Leistungsbeschreibung	Ja	Nein
MUSS	Bereitstellung/Betrieb einer geschäftlichen E-Mail-Lösung mit Spam- und Malware-Filter sowie TLS-Transportverschlüsselung.	☐	☐
MUSS	Unterstützung von KIM (Kommunikation im Medizinwesen) im Zusammenspiel mit dem TI-Konnektor und dem PVS-Hersteller (Ersteinrichtung, Fehleranalyse an der praxisseitigen Infrastruktur).	☐	☐
SOLL	Hosting der E-Mail in einem Rechenzentrum in Deutschland/EU; DSGVO-konformer AVV.	☐	☐
SOLL	Technische Absicherung eingehender E-Mail (SPF, DKIM, DMARC) und Schutz vor gefälschten Absendern (Phishing-Schutz).	☐	☐
KANN	Ende-zu-Ende-verschlüsselte E-Mail für nicht-KIM-Versandwege (S/MIME, PGP).	☐	☐
KANN	Sicherer Dateiaustausch mit Laboren, Überweiser-Kliniken u. Ä. über dedizierte Portale.	☐	☐

3.7 Telematikinfrastruktur (TI) – Schnittstelle zum PVS-Hersteller

Betrieb und Support von TI-Konnektor, eHBA, SMC-B sowie ePA- und eRezept-Anbindung liegen in der Regel beim PVS-Hersteller bzw. beim TI-Fachdienstleister. Der lokale IT-Dienstleister muss hier nicht die Führung übernehmen, jedoch an der Schnittstelle sauber zusammenarbeiten können.

Kat.	Anforderung / Leistungsbeschreibung	Ja	Nein
MUSS	Sicherstellung der netzwerkseitigen Voraussetzungen für den TI-Konnektor (korrekte IP-Adressierung, Firewall-Freischaltungen, Routing).	☐	☐
MUSS	Unterstützung im Fehlerfall an der Schnittstelle Praxisnetz – TI (Abgrenzung gegenüber dem PVS-/TI-Support; gemeinsame Fehleranalyse).	☐	☐
SOLL	Kenntnis der Migration auf TI 2.0 / TI-Gateway (Rechenzentrumskonnektor) einschließlich der Anforderung eines VPN-Tunnels zwischen Praxis und ausgelagertem Konnektor.	☐	☐
SOLL	Schriftlich dokumentierte Zuständigkeitsabgrenzung zwischen PVS-Hersteller und IT-Dienstleister.	☐	☐
KANN	Direkter Vertrag als TI-Fachdienstleister (eher bei Systemhäusern mit Heilberufe-Schwerpunkt).	☐	☐

3.8 Besondere Geräte zahnmedizinischer Praxen

Zahnärztliche, kieferorthopädische und chirurgisch arbeitende Praxen betreiben zahlreiche Spezialgeräte, die netzwerkseitig integriert werden müssen. Der Dienstleister muss nicht die Geräte selbst warten (das übernimmt der Medizintechnik-Hersteller), aber ihre Netzwerk- und Datensicht beherrschen.

Kat.	Anforderung / Leistungsbeschreibung	Ja	Nein
MUSS	Netzwerkseitige Integration digitaler Röntgengeräte und der zugehörigen Datenverarbeitungsgeräte.	☐	☐
MUSS	Backup der Bilddatenbank abgestimmt mit dem Bildgebungssystem (vollständige, konsistente Sicherung inkl. Datenbank).	☐	☐
MUSS	Netzwerktechnische Trennung von Medizingeräten mit unsicheren oder nicht mehr gepflegten Betriebssystemen (eigenes VLAN).	☐	☐
SOLL	Erfahrung mit DVT-Geräten (hohes Datenvolumen, große Datenbanken) – relevant bei Oralchirurgie, KFO und MKG.	☐	☐

Kat.	Anforderung / Leistungsbeschreibung	Ja	Nein
SOLL	Anbindung von Intraoralscannern (z. B. 3Shape TRIOS, iTero, CEREC Primescan) und CAD/CAM-Workstations – relevant bei restaurativ-zahnärztlichen und KFO-Praxen.	☐	☐
SOLL	Kenntnis des DICOM-Standards und des Datenaustauschs mit Fremdbefundern / Großgeräte-Zentren (insb. MKG-Praxen mit Klinikanbindung).	☐	☐
KANN	Anbindung von digitalen KFO-Planungstools und STL-Workflows.	☐	☐
KANN	OP-Dokumentationssysteme und Schnittstellen zu ambulanten OP-Zentren (MKG, Oralchirurgie).	☐	☐

3.9 Cloud-Dienste (§ 393 SGB V)

Die aktuelle Richtlinie regelt erstmals ausdrücklich den Einsatz von Cloud-Diensten. Der Dienstleister muss die Einhaltung dieser Vorgaben nachweisen können, wenn er Cloud-Komponenten einsetzt oder empfiehlt.

Kat.	Anforderung / Leistungsbeschreibung	Ja	Nein
MUSS	Einsatz ausschließlich solcher Cloud-Dienste, die die Anforderungen aus § 393 SGB V erfüllen (Rechenzentrum innerhalb EU, geeignetes Sicherheitsniveau, C5-Testat oder gleichwertig).	☐	☐
MUSS	Schriftlicher AVV mit jedem Cloud-Anbieter; Transparenz über Sub-Auftragsverarbeiter.	☐	☐
SOLL	BSI-C5-Testat des genutzten Cloud-Anbieters.	☐	☐
KANN	Angebot einer dedizierten Praxis-Cloud / Virtual-Desktop-Infrastruktur (VDI) für ortsunabhängigen Zugriff.	☐	☐

4. Organisatorische Leistungen und Dokumentation

4.1 Dokumentation und Nachweisführung

Ein wesentlicher Teil der Richtlinienerfüllung ist die nachweisbare Dokumentation. Der Dienstleister soll die Praxis aktiv dabei unterstützen, die geforderten Unterlagen zu erstellen und aktuell zu halten.

Kat.	Anforderung / Leistungsbeschreibung	Ja	Nein
MUSS	Erstellung und Pflege eines aktuellen Netzplans der Praxis.	☐	☐
MUSS	Führung eines Inventarverzeichnisses der IT-Komponenten (Hard- und Software) mit Stand- und Ablaufdaten.	☐	☐
MUSS	Dokumentation der Administrations-Passwörter und -Zugänge in einem für die Praxis (z. B. im Notfall) zugänglichen, verschlüsselten Tresor.	☐	☐
MUSS	Bereitstellung von Mustern und Vorlagen (z. B. IT-Notfallkarte nach BSI-/KZBV-Vorlage, Richtlinien-Umsetzungscheckliste).	☐	☐
MUSS	Jährlicher schriftlicher Prüfbericht zum Stand der Umsetzung der IT-Sicherheitsrichtlinie.	☐	☐
SOLL	Unterstützung beim Verzeichnis der Verarbeitungstätigkeiten (VVT) nach Art. 30 DSGVO, soweit es IT-Systeme betrifft.	☐	☐
SOLL	Übergabedokumentation beim Dienstleisterwechsel (Exit-Dokumentation).	☐	☐
KANN	Elektronische Praxis-Akte mit allen IT-Dokumenten und Prüfprotokollen.	☐	☐

4.2 Notfall- und IT-Sicherheitsvorfallmanagement

Kat.	Anforderung / Leistungsbeschreibung	Ja	Nein
MUSS	Erarbeitung eines schriftlichen IT-Notfallplans (u. a. Ausfall PVS, Ransomware, Datenverlust, Telefonausfall).	☐	☐
MUSS	Klar definierter Notfallkontakt (Telefon, E-Mail), Erreichbarkeit im Notfallplan ausgewiesen.	☐	☐
MUSS	Unterstützung der Praxis bei der Erfüllung der Meldepflichten nach DSGVO (Art. 33/34) im Falle einer Datenpanne – der Dienstleister meldet nicht selbst, liefert aber die technischen Fakten.	☐	☐
SOLL	Regelmäßige Notfallübung / Tabletop-Test mit der Praxisleitung (mind. alle 24 Monate).	☐	☐
SOLL	Bereitstellung von Ersatzhardware (Leihgerät) bei kritischen Defekten.	☐	☐
KANN	Cyber-Versicherungsbegleitung (Unterstützung bei Meldungen, Forensik-Ansprechpartner).	☐	☐

4.3 Schulung und Security Awareness

Die aktualisierte Richtlinie fordert ausdrücklich Sensibilisierungsmaßnahmen (Security Awareness) für Praxispersonal. Diese können vom Dienstleister erbracht oder zugeliefert werden.

Kat.	Anforderung / Leistungsbeschreibung	Ja	Nein
MUSS	Bereitstellung von Schulungsmaterial für das Praxisteam (z. B. KBV-Basis- und Phishing-Schulung) sowie Unterstützung bei deren Organisation.	☐	☐
MUSS	Strukturierte technische Einarbeitung neuer Mitarbeitender (Kontenanlage, Rechtevergabe, kurze IT-Sicherheits-Unterweisung) – verbindlich ab 02.01.2026.	☐	☐
SOLL	Eigene Präsenz- oder Online-Schulung zur IT-Sicherheit für Praxisteams, mindestens einmal jährlich.	☐	☐
SOLL	Phishing-Simulationen (z. B. 1–2 × jährlich) mit Auswertung.	☐	☐
KANN	Learning-Management-System mit individuellen Nachweisen pro Mitarbeitendem.	☐	☐

4.4 Datenschutz-Schnittstelle

Kat.	Anforderung / Leistungsbeschreibung	Ja	Nein
MUSS	Benennung eines festen Ansprechpartners für den Datenschutzbeauftragten der Praxis.	☐	☐
MUSS	Unterstützung bei technischer Umsetzung von Betroffenenrechten (z. B. Auskunft, Löschung) im Rahmen der eingesetzten Systeme.	☐	☐
SOLL	Kooperation mit dem externen Datenschutzbeauftragten der Praxis; ggf. Empfehlung geeigneter Anbieter, wenn die Praxis (noch) keinen DSB bestellt hat.	☐	☐
KANN	Angebot eigener Datenschutzberatung (nur durch qualifiziertes Personal; strikt von der IT-Rolle trennbar).	☐	☐

5. Vertragliche Rahmenbedingungen

Kat.	Anforderung / Leistungsbeschreibung	Ja	Nein
MUSS	Schriftlicher Service-Vertrag mit klarem Leistungsumfang, Leistungsabgrenzung, Preisen und Kündigungsfristen.	☐	☐
MUSS	Service-Level-Agreement (SLA) mit definierten Reaktions- und Wiederherstellungszeiten.	☐	☐
MUSS	Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO.	☐	☐
MUSS	Verschwiegenheitsverpflichtung aller eingesetzten Mitarbeitenden, mit ausdrücklichem Bezug auf § 203 StGB (berufsmäßige Schweigepflicht).	☐	☐
MUSS	Schriftliche Regelung zur Herausgabe von Daten, Zugangsdaten und Dokumentation bei Vertragsende (Exit-Klausel).	☐	☐
SOLL	Transparente Preisstruktur: monatliche Pauschale für Betreuung, klare Stundensätze für Projekte, keine versteckten Kosten.	☐	☐
SOLL	Regelung zum Umgang mit Sub-Dienstleistern (z. B. Rechenzentrumsbe-treiber, Hersteller-Fernwartung).	☐	☐
SOLL	Jährlicher Jour-fixe mit der Praxisleitung zur Bewertung der Servicequalität und des IT-Sicherheitsstandes.	☐	☐
KANN	Vertragsstrafe / Pönale bei Nichteinhaltung zugesagter Reaktionszeiten.	☐	☐

6. Zusammenfassung der Prüfung

Nach Durchsicht der obigen Anforderungen kann eine zusammenfassende Bewertung vorgenommen werden.

Kategorie	Anzahl Anforderungen	erfüllt (Ja)	nicht erfüllt (Nein)
MUSS-Anforderungen	0	0	0
SOLL-Anforderungen	0	0	0
KANN-Anforderungen	0	0	0

Entscheidungsregel (Empfehlung):

- Nicht erfüllte MUSS-Anforderungen:
  Ausschlusskriterium. Der Dienstleister kommt nicht in die engere Wahl, außer die Lücke ist kurzfristig schließbar oder die Praxis verfügt über einen anderen belastbaren Weg, die Anforderung zu erfüllen.
- Nicht erfüllte SOLL-Anforderungen:
  Vertieft zu diskutieren. Der Dienstleister erläutert schriftlich, wie die Lücke geschlossen wird (Kooperationspartner, Nachrüstung, alternative Umsetzung).
- Nicht erfüllte KANN-Anforderungen:
  unkritisch, sofern die Praxis die entsprechenden Funktionen nicht aktiv benötigt.

Zweite Meinung / Referenzgespräche:

Vor Vertragsabschluss wird empfohlen, mindestens zwei der benannten Referenzkunden telefonisch zu kontaktieren. Leitfragen: Reaktionszeiten im Alltag, Transparenz der Abrechnung, Qualität der Dokumentation, Verhalten in einem realen Störungsfall.

7. Unterschriften und Bestätigung

Der Dienstleister bestätigt mit seiner Unterschrift die wahrheitsgemäße Beantwortung der vorstehenden Anforderungen. Unrichtige Angaben können einen wichtigen Grund zur Kündigung eines daraufhin geschlossenen Vertrags darstellen.

Für den IT-Dienstleister:	**Für die Praxis:**
Unternehmen: Name, Funktion:	Praxis: Name, Funktion:
Ort, Datum:	Ort, Datum:
Unterschrift:	Unterschrift:

Anhang: Quellen und weiterführende Hinweise

- IT-Sicherheitsrichtlinie der KZBV nach § 390 SGB V einschließlich Anlagen 1, 2, 3, 4, 5 (veröffentlicht 01.07.2025, in Kraft seit 02.07.2025, neue/geänderte Anforderungen verbindlich ab 02.01.2026). Abrufbar unter kzbv.de.
- §§ 390, 393 SGB V (Digital-Gesetz – DigiG).
- Verzeichnis freiwillig zertifizierter Dienstleister nach § 390 SGB V, gepflegt durch die KBV.
- Mustervorlagen der KBV/KZBV zur Umsetzung: Checkliste IT-Sicherheit, IT-Notfallkarte, Basis- und Phishing-Schulung für das Praxisteam, Netzplan-Muster, persönliche Umsetzungscheckliste.
- BSI-Empfehlungen für Arzt- und Zahnarztpraxen, insb. Grundschutz-Bausteine zu Netzwerk, Endgeräten, Backup, Sensibilisierung.

Rechtlicher Hinweis: Dieses Dokument ist eine praktische Arbeitshilfe. Es ersetzt weder eine individuelle fachliche Beratung noch die eigene Prüfung der jeweils aktuellen Fassung der IT-Sicherheitsrichtlinie. Verbindlich ist stets der Text der Richtlinie in der zum Zeitpunkt der Umsetzung gültigen Fassung.