

IT-SECURITY

*PRAXISWÄCHTER

KZBV
IT-Sicherheits-
richtlinie

icmed
Das Systemhaus für die Medizin

F1
DENTALSYSTEME

KZBV

DATENSICHERUNG

Wir sichern Ihren Praxisbetrieb –
richtlinienkonform, zuverlässig und nachweisbar.

➔ **Ein IT-Vorfall ist keine Frage des Ob, sondern des Wann.**

Betroffen sind ohne Datensicherung:

- Patientendaten
- Abrechnung
- Röntgen- und Befunddaten
- Terminverwaltung

Die Folgen:

- Behandlungsausfälle
- Umsatzeinbruch
- Vertrauensverlust
- mögliche Sanktionen durch Prüfstellen

Rechtliche Grundlagen

DSGVO (Datenschutz Grundverordnung)

Daten müssen integritätssicher
und wiederherstellbar sein.
Die Speicherung darf nur auf
sicheren Systemen erfolgen.

Bundesmantelvertrag, Röntgenverordnung, Finanzamt

Röntgen-, Befund- und Abrech-
nungsdaten müssen über mind.
10 bis teilweise 30 Jahre
verfügbar sein, auch nach der
Praxisschließung.

Sicherheitsmaßnahmen nach BSI / KZBV

Regelmäßige Backups,
Zugriffskontrollen,
Protokollierung von
Änderungen

Besondere Anforderungen / Maßnahmen

- **Vollständige Datensicherung erstellen (Sind die Nebenstellen gesichert?)**
- **Verantwortliche Personen bestimmen**
- **Regelmäßiger Wiederherstellungstest**

Unsere Lösung:

Datensicherung als Service – Cloud oder Hybrid (KZBV-konform)

1. **Lokales Backup für sofortige Verfügbarkeit**
2. **Zusätzliche Cloud-Sicherung außerhalb der Praxis**
3. **Schutz vor Hardwaredefekt, Diebstahl, Brand und Ransomware**
4. **Vollautomatische, vollständige und verschlüsselte Sicherung**
5. **Permanente Überwachung**
6. **Regelmäßiger Wiederherstellungstest – sind die Daten nutzbar, die Sie sichern?**
7. **Proaktive Meldung bei Fehlern**
8. **Dokumentierte Prüfprotokolle**
9. **Fester Ansprechpartner im Notfall**

Nächster Schritt:

Lassen Sie Ihre Datensicherung jetzt prüfen – bevor ein Vorfall Sie dazu zwingt.

* gemäß den Vorgaben und Sicherheitsrichtlinien der KZBV

PRAXISNETZWERK

richtig schützen – was ist wichtig?

In einer Zahnarztpraxis ist die Einhaltung der IT-Sicherheitsrichtlinie (nach § 75b SGB V bzw. den Vorgaben der KZBV) seit dem 2. Januar 2026 mit verschärften Anforderungen verpflichtend.

Drittgeräte (Smartphones, Tablets, Laptops ...) dürfen niemals physisch oder logisch ungeschützt in das interne Praxisnetzwerk integriert werden.

Nutzungsverbot für Patientendaten: Die Verarbeitung oder Speicherung von Patientendaten auf privaten Geräten ist grundsätzlich untersagt, sofern keine speziellen technischen Schutzmaßnahmen (wie verschlüsselte Container-Apps) implementiert sind.

Zugriff durch Dritte

mobile Endgeräte (Tablets, Patientenhandy etc.)

Müssen durch Verschlüsselung und starke Passwörter / Biometrie gesichert sein.

externe Dienstleister / Patienten:

Nutzen Sie ein separates Gäste-WLAN.
Kein unbeaufsichtigter und unprotokollierter Zugriff.
Wartungen per Fernzugriff sollten nur durch gesicherte VPN-Verbindungen erfolgen.

private Geräte: (Mitarbeiter / Kollegen)

Private Geräte von Mitarbeitern sollten keinen Zugriff auf das Praxisnetz haben. Eine strikte Trennung von privaten Daten und Praxisdaten ist zwingend erforderlich.

Unsere Lösung:

Unsere Empfehlungen als Ergebnis der Regelungen der KZBV

✓ **Einsatz einer Hardware-Firewall**

✓ **Aktiver und aktueller Virenschutz**

✓ **Zugangskontrolle und Verschlüsselung
(Passwörter, USB-Schnittstellen, Mikrofone,
Kameras, Datenträger)**

✓ **Zugangskontrolle / Trennung von
Cloud-Diensten**

✓ **Verpflichtung Ihrer Partner über AVV**

Nächster Schritt:

Wir prüfen Ihr Praxisnetzwerk auf Herz und Nieren – kontaktieren Sie uns einfach!

KI ALS CHANCE FÜR DIE PRAXIS-IT

Bedrohung oder Chance?

➔ **Künstliche Intelligenz (KI) ist bereits Bestandteil der IT-Sicherheitsrichtlinie** (gemäß § 75b SGB V und den Vorgaben der KZBV).

Sie kann:

- Cyberangriffe schneller erkennen
- Phishing-Mails besser filtern
- Abläufe standardisieren
- Diagnostik unterstützen

Gleichzeitig entstehen neue Risiken:

- Nutzung privater KI-Tools durch Mitarbeiter
- Datenabfluss durch nicht zertifizierte Anwendungen
- Haftungsrisiken nach EU AI Act

KI als Chance

Verbesserter Schutz vor Cyberangriffen:

Moderne Sicherheitssysteme nutzen KI, um Anomalien im Netzwerkverkehr in Echtzeit zu erkennen und Angriffe abzuwehren, bevor Daten verschlüsselt werden.

Automatisierte Früherkennung:

KI-gestützte E-Mail-Filter bieten einen effektiveren Schutz vor komplexen Phishing-Versuchen, die manuell kaum noch erkennbar sind.

Entlastung bei Routineaufgaben:

In der Diagnostik sorgt sie für höhere Präzision und Dokumentationsqualität, was indirekt die Datensicherheit durch standardisierte Prozesse erhöht.

KI als Bedrohung

Schatten-KI:

Eine große Gefahr ist die Nutzung privater, nicht zertifizierter KI-Tools durch das Personal. Dies hebt interne IT-Kontrollen aus und kann zum Abfluss sensibler Patientendaten führen.

Hochriskante Angriffe:

Angrifer nutzen KI für automatisierte, technologisch ausgereifte Angriffe auf Praxisnetze, was das Bedrohungspotenzial massiv erhöht.

Datenschutz:

Viele KI-Anwendungen gelten nach dem EU AI Act als Hochrisiko-Systeme. Zahnärzte haften dafür, dass diese Tools DSGVO-konform arbeiten und IT-Sicherheitsstandards einhalten.

Unsere Lösung: KI richtlinienkonform einsetzen

Verwenden Sie ausschließlich KI-Tools, die zertifiziert sind und deren Datenspeicherung in der EU erfolgt.

Untersagen Sie strikt die Nutzung privater KI-Anwendungen für Patientendaten (z. B. ChatGPT für Arztbriefe).

Unterweisen Sie Ihr Team im Rahmen der jährlichen IT-Sicherheitsbelehrung über die Risiken von KI-basiertem Social Engineering.

Informieren Sie Patienten über den Einsatz von KI in der Behandlung, wie es die aktuelle Rechtsprechung fordert.

Nächster Schritt:

Sprechen Sie uns an, wir gehen mit Ihnen alle Möglichkeiten für Ihre Praxis durch.



MEHR SICHERHEIT

Schulungen für Ihr Praxis-Team

In einer Zahnarztpraxis ist das Awarenessstraining (Sicherheitsunterweisung) keine freiwillige Option mehr, sondern eine obligatorische Maßnahme gemäß der IT-Sicherheitsrichtlinie nach § 75b SGB V.

Gesetzliche Pflicht & Dokumentation

- ☒ Das Personal muss mindestens einmal jährlich unterwiesen werden.
- ☒ Sie müssen die Durchführung protokollieren (Teilnehmerliste, Datum, Inhalte).
- ☒ Bei neuen Mitarbeitern muss die Schulung unmittelbar bei Eintritt erfolgen.

Schulungsinhalte für Awarenessstraining

KI-gestütztes Phishing:

Da Angreifer 2026 KI nutzen, um perfekte, fehlerfreie E-Mails (auch in der Sprache des Praxisinhabers) zu verfassen, ist das Erkennen von Absenderadressen und Link-Zielen wichtiger denn je.

Social Engineering:

Das Personal muss darauf trainiert werden, am Telefon keine Auskünfte über die IT-Struktur oder Passwörter zu geben, selbst wenn der Anrufer behauptet, vom "IT-Support" oder der "KZV" zu sein.

Umgang mit mobilen Datenträgern:

Striktes Verbot des Anschlusses privater USB-Sticks oder Handys an Praxis-PCs (Gefahr durch Malware).

Clear Desk & Clear Screen:

Sperren des Bildschirms beim Verlassen des Behandlungszimmers und Wegschließen von Patientenakten.

Unsere Lösung: Umsetzung in der Praxis

Präsenzschulung:

Im Rahmen einer Teambesprechung (vorteilhaft für direkte Rückfragen)

E-Learning-Plattformen:

Es gibt zahlreiche Anbieter für Cyber-Security-Awareness, die spezialisierte Module für das Gesundheitswesen anbieten.

Phishing-Tests:

Unangekündigte, harmlose Test-Mails durch Ihren IT-Dienstleister, um das reale Verhalten der Mitarbeiter zu prüfen.

Nächster Schritt:

Fragen Sie uns, wir haben immer die passenden Lösungen!



QM – UP TO DATE?

Ist mein QM-Handbuch komplett?

Ihre QM-Dokumente müssen spezifische Anforderungen der aktualisierten IT-Sicherheitsrichtlinie nach § 75b SGB V erfüllen.

Unsere Lösung: Anforderungen & Maßnahmen

Netzplan

Grafische Darstellung aller Komponenten (PCs, Server, TI-Konnektor, Röntgengeräte) und deren Verbindung

Berechtigungskonzept

Dokumentation, wer Zugriff auf welche Daten (PVS, Röntgen) hat, inklusive einer Liste aller aktiven Benutzerkonten.

Datensicherungskonzept

Festlegung von Backup-Zyklen, Speicherorten (verschlüsselt) und regelmäßigen Rücksicherungstests

Inventarliste der IT-Werte

Erfassung aller Hardware, Softwarelizenzen und deren Standorte

Protokoll der Mitarbeiterunterweisung

Nachweis der jährlichen Schulung zu IT-Sicherheit und Datenschutz

Übersicht der Wartungsarbeiten

Protokollierung von Updates und Sicherheitsprüfungen durch externe Dienstleister

IT-Notfallplan

Klare Anweisungen was im Ernstfall zu tun ist, inklusive wichtiger Notfallkontakte (IT-Dienstleister, KZV).

Auftragsverarbeitungsverträge (AVV)

Verträge mit allen Dienstleistern, die Zugriff auf Patientendaten haben könnten (z. B. IT-Support, Cloud-Anbieter)

VVT (Verzeichnis von Verarbeitungstätigkeiten)

Dokumentation aller Prozesse, bei denen personenbezogene Daten verarbeitet werden (gem. Art. 30 DSGVO).

Nächster Schritt:

Rufen Sie uns an! Wir haben Beispiele und Vorlagen für Ihre Dokumentation.

Auch keine Lust auf Datensicherung?

Mit unserer **Managed Cloud Backup** übernehmen wir Einrichtung, Betreuung, Überwachung und Kontrolle Ihrer Datensicherung. Ihre Praxis arbeitet wie gewohnt weiter. Viele Backup-Lösungen sichern Daten. Wir gehen einen entscheidenden Schritt weiter. Einmal pro Quartal führen wir einen Rücklesetest durch und prüfen, ob gesicherte Daten erfolgreich wiederhergestellt werden können. So wissen Sie nicht erst im Ernstfall, ob Ihr Backup wirklich funktioniert. Der Rücklesetest erfolgt durch einen ic med Techniker, wird dokumentiert und unterstützt Sie bei der Umsetzung der KZBV-Anforderungen.

ic med Managed Cloud Backup:

- ✓ **Automatische Online-Sicherung:**
Ihre Praxisdaten werden täglich online gesichert – zuverlässig und ohne manuelle Eingriffe.
- ✓ **Backup im laufenden Betrieb:**
Die Sicherung läuft im Hintergrund. Anmeldung, Behandlung, Abrechnung und Verwaltung bleiben verfügbar.
- ✓ **Managed Service statt Eigenaufwand:**
Wir übernehmen Einrichtung, Betreuung, Überwachung und Kontrolle Ihrer Datensicherung.
- ✓ **Speicherung auf deutschen Servern:**
Ihre Sicherungsdaten bleiben in Deutschland. Das unterstützt die Umsetzung der DSGVO-Anforderungen.
- ✓ **Jederzeit eigener Zugriff:**
Ihre Praxis behält jederzeit Zugriff auf die Sicherung und kann bei Bedarf selbst auf gesicherte Daten zugreifen.
- ✓ **Quartalsweiser Rücklesetest:**
Wir prüfen einmal pro Quartal, ob sich Ihre Daten im Ernstfall tatsächlich wiederherstellen lassen.
- ✓ **Verschlüsselte Datenübertragung & Speicherung**
Ihre Daten werden geschützt übertragen und verschlüsselt gespeichert.
- ✓ **Keine Beeinträchtigung des Praxisbetriebs:**
Backup und Rücklesetest laufen im Hintergrund. Ihr Praxisablauf bleibt ungestört.

Was kostet der Service?

Einmalige Einrichtung der Cloud-Datensicherung per Remote-Service.

Enthalten sind:

- Einrichtung und Konfiguration der Sicherung
- Abstimmung der zu sichernden Datenbereiche
- Prüfung der ersten erfolgreichen Sicherung
- Übergabe und Einweisung

390 €
mtl., zzgl. MwSt.

KZBV- und DSGVO-sicherheitskonform!

1 TB Daten-Speicher

inkl. vollem Zugriff auf Ihre Praxisdaten

109 €
mtl., zzgl. MwSt.

___ TB zusätzlicher Cloud-Speicher

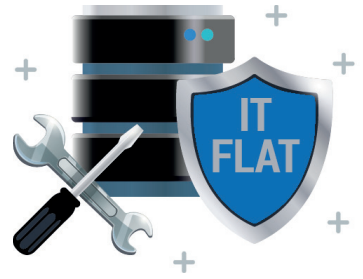
79 €
je 1TB, mtl., zzgl. MwSt.

☐ Quartalsweiser Rücklesetest

Ein ic med Techniker testet einmal pro Quartal, ob gesicherte Daten erfolgreich wiederhergestellt werden können. Der Test wird dokumentiert und unterstützt Ihre Praxis bei der Umsetzung der KZBV-Anforderungen.

40 €
mtl., zzgl. MwSt.

PRAXIS-IT OHNE LIEFERENGPÄSSE!



IT-FLAT – 5 JAHRE SORGLOS!

Leistungen pro Arbeitsplatz (Rechner):

- Praxisspezifische Vorinstallation inkl. Konfiguration
- Betriebssystem, Erstinstallation aller Software des ic med-Portfolios inkl. E-Mail und Virenschutz
- Anbindung der Peripherie (Drucker, Scanner, Kartenleser, EC-Cash u.ä.)
- Anbindung der Telematikinfrastruktur
- Einrichtung Datensicherung
- Anfahrt Erstinstallation

5 Jahre Sorglosleistungen im Überblick:

- Vollgarantie vor Ort
- Leihgerät bei Bedarf
- Technische Hotline
- Fernwartungsservice
- Administrierter Virenschutz
- Unterstützung bei Updates der Telematikinfrastruktur
- 24 Stunden Reaktionszeit innerhalb der ic med Geschäftszeiten
- Versicherungsschutz des Rechners gegen Feuer, Wasser, Diebstahl



**SOFORT
VERFÜGBAR!**

- ✓ Speziell für den Dentalbereich konfiguriert
- ✓ Komplettpaket statt Einzelbausteine
- ✓ Faire Preise



1 Platz / Rezeption

74,00 € brutto/mtl.



2D-Röntgenrechner

79,00 € brutto/mtl.



Clients

(Standard, SLIM, MINI)

64,00 € brutto/mtl.



All-in-One Rechner

79,00 € brutto/mtl.



Server

ab 189,00 € brutto/mtl.

*IT-Sicherheit made
in Germany!*

DIE FIREWALL SPEZIELL FÜR ZAHNÄRZTE & ÄRZTE

PRAXISWÄCHTER DIE FIREWALL FÜR DEN ARZT

- Überwachung aller ein- und ausgehenden (Internet-) Verbindungen Ihrer Praxis
- Trennung von Telematik- und Internetanwendungen
- Sichere Nutzung sämtlicher zukünftiger Telematikanwendungen
- DSGVO-konform
- Garantiert keine „Backdoor“ (NSA-sicher)
- Support, Einrichtung und Aktualisierung inklusive
- Sie bestimmen! Wer darf was im Internet und wer darf welche Daten einsehen



950 €*

*zzgl. MwSt., zzgl. Dienstleistung

WIE STEHT ES UM IHRE ANTIVIRUS-SOFTWARE?

*Wir managen
das für Sie!*

Highend Virenschutz für Ihr Praxisnetzwerk!

- Zentrale Steuerung und automatischer Schutz für beliebige Mailserver, Fileserver, Desktops und Notebooks
- Mit No-Backdoor-Garantie „Made in Germany“
- Individualisierbar für die Sicherheitsansprüche Ihrer Praxis-IT
- Zentrale Steuerung und Überwachung
- Testsieger Stiftung Warentest 03/2026 (GDATA für Windows)

ab 3,20 €/mtl.**



**TRUST IN
GERMAN
SICHERHEIT**

**zzgl. MwSt., Gebühr pro Monat für einen Arbeitsplatz, zzgl. Server, Mindestlaufzeit ein Jahr

BOXENSTOPP VOR IHRER PRAXIS

Bundesweite „Diplomaten“-Tour

Warum zu einer Messe oder in einen Showroom fahren? Wir bringen die Innovation **direkt vor Ihre Tür** – egal, wo in Deutschland!

Testen Sie die neueste Technik live in Ihrer gewohnten Umgebung – wir machen einen **Boxenstopp vor Ihrer Praxis** und Sie schauen sich in Ruhe unsere **Diplomat Behandlungseinheit** sowie den **kabellosen Intraoralscanner von AlliedStar** an.

Machen Sie einen Schritt vor die Tür, nehmen Sie Platz und scannen Sie selbst!



DIPLOMAT MODEL PRO 600

inkl. iPad-Software, 210 kg Traglast, Lifteinheit (stuhlgetragen möglich), kabellose Fußsteuerung & Instrumentenbrücke mit hängenden Schläuchen möglich, Lichtturbineneinrichtung & Speibecken motorisiert, Funktionsspritze & OP-Lampe, Hygienemodul und Mikromotor, Absaugelement und LED-ZEG, große Polsterfarbenauswahl



ab 26.990 €*

INTRAORALSCANNER AS 260



Alliedstar

Schnell & präzise, offenes System, beeindruckendes Preis-Leistungs-Verhältnis und keine versteckten Gebühren! Verbinden, scannen, übertragen & laden, inkl. KI-Technologie, inkl. 3 Jahre Garantie

8.888 €*



Ihre Highlights vor Ort:

- **Diplomat:** Behandlungseinheit live erleben & Probesitzen
- **AlliedStar:** Kabelloser Intraoralscanner im Praxis-Check
- **Team-Bonus:** Kleine Überraschungen für Ihre entspannte Pause!

GUTSCHEIN IT-SECURITY CHECK

IM WERT VON 490 € – FÜR SIE KOSTENFREI*

Wir sind spezialisiert auf IT für Zahnarztpraxen. Durch unsere langjährige Erfahrung im Dentalbereich kennen wir die Anforderungen aus § 75b SGB V, KZBV, DSGVO, TI-Infrastruktur, Röntgen und Abrechnung im Detail. Wir wissen, wie eine Praxis arbeitet und wo reale Risiken entstehen. Unsere Lösungen sind praxisnah, prüfungssicher und auf maximale Betriebssicherheit ausgelegt. Die ic med GmbH steht für Spezialisierung, Erfahrung und verlässliche Sicherheit – damit Ihre Praxis jederzeit arbeitsfähig bleibt.

Der IT-Security-Check umfasst:

- ✓ Analyse Ihrer Datensicherung
- ✓ Prüfung der Netzwerksicherheit
- ✓ Überprüfung der Dokumentation
- ✓ Bewertung der Mitarbeiterunterweisung
- ✓ Erste Risikoeinschätzung & Handlungsempfehlung

Sie erhalten:

- eine strukturierte Übersicht
- konkrete Maßnahmenempfehlungen
- klare Priorisierung
- Transparenz über Ihren aktuellen Sicherheitsstatus

*Der Gutschein ist einmalig pro Praxis einlösbar und nicht auszahlbar, vollständige Verrechnung bei Auftragserteilung.

WARTEN SIE NICHT AUF DEN ERNSTFALL!

IT-Sicherheit ist keine technische Spielerei.
Sie ist Bestandteil Ihrer unternehmerischen Verantwortung.

Wir begleiten Zahnarztpraxen bundesweit –
pragmatisch, lösungsorientiert und prüfungssicher.



Das Systemhaus für die Medizin

Tel. 0345 298 419-0
info@ic-med.de
www.ic-med.de



Tel. 07231 28 01-80
keltern@f1-dentalsysteme.de
www.f1-dentalsysteme.de

#WIRKÖNNENSERVICE

BUNDESWEIT FÜR SIE DA!

Halle/S. | Berlin | Chemnitz | Dresden
Wiehl | München | Stuttgart | Keltern

