FAQ – IT Sicherheit

Inhalt

Was regelt die IT-Sicherheitsrichtlinie? 2
Was ist neu und ist bis Oktober 2025 von allen Praxen umzusetzen? 2
Gilt die IT-Sicherheitsrichtlinie für alle Praxen in gleicher gleichermaßen? 2
Wer trägt die Verantwortung für die Datensicherheit in den Praxen? 2
Wie stelle ich einen sicheren Umgang mit der Datensicherheit des Praxispersonals sicher? ... 2
Welche Maßnahmen müssen ergriffen werden, wenn Praxispersonal austritt? 3
Welche Maßnahmen gelten für externes Personal? 3
Wie erfolgt der Umgang mit Spam E-Mails? 3
Gibt es unterstützende Materialien zum Thema IT-Sicherheit für Ärzte und Psychotherapeuten? 3
Muss der Netzplan der Praxis dokumentiert werden? 3
Wie müssen die Netzübergangspunkte abgesichert werden? 3
Ist eine Hardware-Firewall verpflichtend? 3
Software-Firewall oder Hardware-Firewall? 4
Gibt es eine Pflicht zur Zertifizierung der IT-Dienstleister? 4
Wer trägt die Kosten die bei der Umsetzung der IT Sicherheitsrichtlinie entstehen? ..... **Fehler! Textmarke nicht definiert.**
Werden Praxen die die IT-Sicherheitsrichtlinie nicht einhalten sanktioniert? 4
Gibt es Tipps zur Umsetzung der IT Sicherheitsrichtlinie? 4

Was regelt die IT-Sicherheitsrichtlinie?

Die Sicherheitsrichtlinie legt die relevanten sicherheitstechnischen Anforderungen für verschiedene Bereiche der Praxis-IT fest und beschreibt damit das Mindestmaß, die in der vertragsärztlichen und -psychotherapeutischen Praxis ergriffen werden müssen. Mit der Umsetzung der Anforderungen, die in fünf Anlagen zur Richtlinie kategorisiert aufgelistet sind, werden die Risiken der IT-Nutzung minimiert und die IT-Sicherheit insgesamt erhöht. Die aktuelle IT-Sicherheitsrichtlinie finden Sie hier KBV - IT-Sicherheitsrichtlinie.

Was ist neu und ist bis Oktober 2025 von allen Praxen umzusetzen?

- Das Praxispersonal muss in den sicheren Umgang mit der Praxis-IT eingewiesen und sensibilisiert werden, soweit dies für die Arbeit relevant ist (Anlage 1 Nummer 9 der Richtlinie).
- Das Praxispersonal muss regelmäßig geschult werden, insbesondere zur eingesetzten Technik/IT (Anlage 1 Nummer 6 der Richtline).
- Das Praxispersonal sollte entsprechend seiner Aufgaben und Verantwortlichkeiten zu Informationssicherheitsthemen geschult werden (Anlage 1 Nummer 10 der Richtline).
- Neue Mitarbeiterinnen und Mitarbeiter müssen in die Praxis-IT eingearbeitet werden (Anlage 1 Nummer 1 der Richtline). Tipp: Hierfür gibt es ein Musterdokument im Hub zur IT-Sicherheitsrichtlinie.
- Bei Beendigung des Beschäftigungsverhältnisses muss die Praxisleitung der Person bekannte oder von ihr verwendete Passwörter und Zugangsdaten ändern oder vernichten (Anlage 1 Nummer 2 der Richtline). Auch hierfür gibt es ein Musterdokument im Hub.
- Externes Personal, etwa von einem IT-Dienstleister zur Installation, Prüfung oder Reparatur von Technik, muss verpflichtet werden, Gesetze, Vorschriften und interne Regelungen einzuhalten. Bei kurzfristigem oder einmaligem Einsatz muss es beaufsichtigt werden (Anlage 1 Nummer 3 der Richtline).
- In der Praxis ist der Umgang mit Spam bei E-Mails geregelt. Grundsätzlich sollten alle, die in der Praxis mit E-Mails arbeiten, Spam ignorieren und löschen (Anlage 1 Nummer 41 der Richtline).

Gilt die IT-Sicherheitsrichtlinie für alle Praxen in gleicher gleichermaßen?

Nein, die Anforderungen richten sich nach Praxisgröße:

- Kleine Praxen: bis 5 Personen
- Mittlere Praxen: 6–20 Personen
- Große Praxen: mehr als 20 Personen

Wer trägt die Verantwortung für die Datensicherheit in den Praxen?

Die Verantwortung für die Datensicherheit der Praxis-IT liegt beim Praxisinhaber. Eine Praxis kann partielle Verantwortung an Dienstleister delegieren, sodass diese in einem Schadensfall als Auftragnehmer im Innenverhältnis haften.

Wie stelle ich einen sicheren Umgang mit der Datensicherheit des Praxispersonals sicher?

Das Praxispersonal wird in den sicheren Umgang mit der Praxis-IT eingewiesen und sensibilisiert, soweit das für die Arbeit relevant ist (Vorgabe in Anlage 1 Nummer 9 der Richtlinie). Die Mitarbeiterinnen und Mitarbeiter werden regelmäßig geschult beziehungsweise weitergebildet, insbesondere zur eingesetzten Technik/IT. Es muss zudem betriebliche Regelungen geben, um das Praxispersonal auf einem aktuellen Kenntnisstand zu halten (Anlage 1 Nummer 6 der Richtlinie). Die Mitarbeiterinnen und Mitarbeiter sollten entsprechend ihrer Aufgaben und Verantwortlichkeiten zu Informationssicherheitsthemen geschult werden (Anlage 1 Nummer 10 der Richtlinie). Neue

Mitarbeiterinnen und Mitarbeiter werden in die Praxis-IT eingearbeitet und über bestehende Regelungen und Verfahrensweisen informiert (Anlage 1 Nummer 1 der Richtlinie).

Welche Maßnahmen müssen ergriffen werden, wenn Praxispersonal austritt?

Gehen Mitarbeiterinnen und Mitarbeiter beispielsweise in Rente, müssen sie beispielsweise Arbeitsunterlagen, Schlüssel, Geräte, Ausweise und Zutrittsberechtigungen zurückgeben. Bekannte und verwendete Passwörter sowie andere Zugangsdaten muss die Praxisleitung ändern oder vernichten (Anlage 1 Nummer 2 der Richtlinie).

Welche Maßnahmen gelten für externes Personal?

Externe Mitarbeiter, zum Beispiel von IT-Dienstleistern, die Technik installieren, prüfen oder reparieren, werden verpflichtet, Gesetze, Vorschriften und interne Regelungen einzuhalten. Externes Personal, das kurzfristig oder einmalig eingesetzt ist, wird in sicherheitsrelevanten Bereichen beaufsichtigt. Zugangsberichtigungen sind so restriktiv wie möglich zu halten (Anlage 1 Nummer 3 der Richtlinie). Bevor externes Personal Zugang zu vertraulichen Informationen erhält, schließen Praxisinhaber mit der Firma oder den Personen Vertraulichkeitsvereinbarungen in schriftlicher Form ab (Anlage 1 Nummer 4 der Richtlinie).

Wie erfolgt der Umgang mit Spam E-Mails?

- Nicht öffnen, nicht beantworten
- Keine Links anklicken
- Sofort löschen
- Schulung der Mitarbeitenden zum Erkennen von Phishing

Die Praxis regelt den Umgang mit Spam bei E-Mails (Anlage 1 Nummer 41 der Richtlinie).

Gibt es unterstützende Materialien zum Thema IT-Sicherheit für Ärzte und Psychotherapeuten?

Die KBV stellt auf einer Online-Plattform unter hub.kbv.de Begleitinformationen und Umsetzungshinweise zu den Richtlinien bereit, die kontinuierlich aktualisiert werden. Auch Musterdokumente sind verfügbar, beispielsweise eine Richtlinie für Mitarbeiter zur Nutzung mobiler Geräte. Zusätzlich bietet die KBV über ihr Fortbildungsportal CME-zertifizierte Online-Schulungen für Ärzte und Psychotherapeuten an.

Muss der Netzplan der Praxis dokumentiert werden?

Ja, ein Netzplan mit allen Komponenten und deren Verbindung muss vorhanden sein.

Wie müssen die Netzübergangspunkte abgesichert werden?

Der Übergang zu anderen Netzen insbesondere dem Internet muss durch eine Firewall geschützt werden. Primäres Ziel ist es, keine unerlaubten Verbindungen von außen in das geschützte Netz zuzulassen. Zusätzlich sollten nur erlaubte Verbindungen aus dem geschützten Netz nach außenaufgebaut werden können.

Ist eine Hardware-Firewall verpflichtend?

Ja, laut Richtlinie muss das Praxisnetz auf Netzebene geschützt werden. Die KBV empfiehlt ausdrücklich eine Hardware-Firewall (z. B. UTM-Firewall) oder den Einsatz des Konnektors im Reihenbetrieb.

Software-Firewall oder Hardware-Firewall?

- Software-Firewall: Für einzelne Geräte (z. B. Windows Defender)
- Hardware-Firewall: Zentrale Absicherung des gesamten Praxisnetzwerks (empfohlen!)
- UTM-Firewall: Kombiniert Firewall, Virenschutz, Angriffserkennung und Webfilter

Empfehlung: Für Praxen ist eine professionell konfigurierte Hardware-Firewall unerlässlich. Eine reine Software-Lösung reicht in der Regel nicht aus.

Gibt es eine Pflicht zur Zertifizierung der IT-Dienstleister?

Praxen sind nicht verpflichtet (zertifizierte) IT-Dienstleister zu beauftragen. IT-Dienstleister sind nicht verpflichtet sich von der KBV zertifizieren zu lassen. Die zertifizierten IT-Dienstleister sind lediglich als Unterstützungsangebot zu verstehen.

Wer trägt die Kosten für die Umsetzung der IT-Sicherheitsrichtlinie?

Jede Praxis trägt eigenverantwortlich die Kosten für ihre IT-Sicherheit, die dafür sorgt, dass die elektronische Datenverarbeitung (EDV) geschützt ist und ordnungsgemäß funktioniert. Es handelt sich im vorliegenden Fall um eine Sicherheitsrichtlinie der IT, nicht der Telematikinfrastruktur (TI). Die TI ist erst in den letzten Jahren als weitere EDV-Komponente hinzugekommen und nicht die Ursache des Schutzbedarfs.

Werden Praxen die die IT-Sicherheitsrichtlinie nicht einhalten sanktioniert?

Das DVG, mit dem die IT-Sicherheitsrichtlinie eingeführt wurde (Paragraf 75 SGB V), sieht derzeit keine eigenen Sanktionen vor. Das bedeutet jedoch nicht, dass diese Vorgaben nicht eingehalten werden müssen. Die Richtlinie definiert Maßnahmen, die die Einhaltung der verschiedenen rechtlichen Vorgaben unterstützen. Gerade die europäische Datenschutzgrundverordnung (EU DSGVO) hat den Behörden die Möglichkeit gegeben, hohe Strafen durchzusetzen, und auch im Straf- und Berufsrecht sind entsprechende Sanktionen vorgesehen.

Gibt es Tipps zur Umsetzung der IT Sicherheitsrichtlinie?

- Ein IT-Sicherheitsbeauftragter (intern oder extern) ist empfehlenswert
- Regelmäßige interne Audits
- Nutzung der KBV-Mustervorlagen
- Notfallpläne für IT-Ausfälle erstellen und testen