FAQs - IT-Sicherheitsrichtlinie

Version 1.0, Stand: 03.03.2021

Inhalt

I. IT-Sicherheitsrichtlinie

1. Warum bedarf es der Richtlinie?

Zur Konkretisierung der abstrakten DSGVO hat der Gesetzgeber einheitliche und verbindliche Vorgaben für Praxen in einer Richtlinie gefordert. Deshalb wurde die Kassenärztliche Bundesvereinigung nach § 75b SGB V beauftragt, die Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen Versorgung zu regeln.

2. Welchen Nutzen hat meine Praxis durch die Erfüllung der Maßnahmen?

In der IT-Sicherheitsrichtlinie werden Mindestmaßnahmen genannt, die Ihrer Praxis dabei helfen sollen, Risiken der IT-Sicherheit zu minimieren und IT-Systeme und sensible Praxisdaten bestmöglich zu schützen. Durch die klaren Vorgaben zur sicheren Verwaltung von Patientendaten und zur Risikominimierung kann die Sicherheit Ihrer sensiblen Daten gewährleistet werden.

3. Gilt die IT-Sicherheitsrichtlinie nur für diejenigen Praxen, die an die Telematikinfrastruktur (TI) angebunden sind?

Nein. Die Richtlinie ist unabhängig davon, ob eine Praxis an die TI angebunden ist oder nicht, verbindlich für alle Praxen.

4. Sind Praxen dazu verpflichtet, einen externen Dienstleister zur Unterstützung bei der Umsetzung der IT-Sicherheitsrichtlinie zu beauftragen?

Praxen sind nicht gezwungen, einen zertifizierten IT-Dienstleister zur Unterstützung bei der Umsetzung der IT-Sicherheitsrichtlinie zu beauftragen. Sollten Praxen die Richtlinien-Erfüllung auch ohne externe Unterstützung umsetzen können, ist ihnen das freigestellt; ebenso können sie einen externen Dienstleister einsetzen, der keine Zertifizierung gemäß § 75b Abs. 5 SGB V hat.
Bitte beauftragen Sie dann einen (zertifizierten) Anbieter, wenn Sie Zweifel haben, ob Sie die Anforderungen allein bzw. mit Ihren vorhandenen Fachkräften (z.B. Systemadministratoren) erfüllen können.

5. Wo und wie finde ich einen zertifizierten Dienstleister?

Sollten Sie einen zertifizierten IT-Dienstleister zur Umsetzung der IT-Sicherheitsanforderungen in Ihrer Praxis beauftragen wollen, dann finden Sie eine Liste der erfolgreich Zertifizierten auf der Homepage der KBV. Auf unserer Themenseite finden Sie den entsprechenden Link dazu.(https://www.kvb.de/praxis/it-in-der-praxis/it-sicherheitsrichtlinie/)

6. Können sich Praxen zertifizieren/verifizieren und prüfen lassen, ob sie alle Anforderungen zur IT-Sicherheitsrichtlinie erfüllt haben?

Este Basisanforderungen zur IT-Sicherheitsrichtlinie müssen ab dem 1. April 2021 in den Praxen umgesetzt werden. Jeder Praxisinhaber ist für die Einhaltung der Anforderungen selbst verantwortlich. Derzeit sind seitens der KBV keine Zertifizierungen oder Verifizierungen zur Einhaltung der IT-Sicherheitsrichtlinie in Praxen geplant.

7. Muss ich der KV gegenüber nachweisen, dass ich die Anforderungen erfüllt habe?

Nach aktuellen Informationen der KBV müssen Sie derzeit gegenüber Ihrer KV nicht nachweisen, dass Sie die Anforderungen zur IT-Sicherheitsrichtlinie erfüllt haben.

8. Was passiert, wenn ich gewisse Anforderungen nicht erfülle?

Die Anforderungen zur Gewährleistung der IT-Sicherheit schützen die sensiblen Daten Ihrer Praxis. Sollten Sie gewisse Anforderungen nicht erfüllen, ist kein vollständiger Schutz mehr in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit der IT-Systeme gewährleistet.

9. Wie ist die Definition "ständig mit der Datenverarbeitung betraute Person" zu verstehen? Müssen Auszubildende in die Anzahl eingerechnet werden?

Die Ausgestaltung der Regelung liegt im Ermessen der jeweiligen Arztpraxis. Sie wurde bewusst nicht abschließend definiert. Die Passage ist angelehnt an die entsprechenden Regelungen des Bundesdatenschutzgesetzes.

10. Können Praxisgemeinschaften, die ein Netzwerk gemeinsam nutzen, gewisse Anforderungen zusammen erfüllen?

Eine Praxisgemeinschaft gilt im Sinne der IT-Sicherheitsrichtlinie nicht als Einheit. Jede Praxis mit eigener Betriebsstättennummer ist für die Einhaltung und Dokumentation der Richtlinie selbst zuständig.
Hintergrund: Die IT-Sicherheitsrichtlinie enthält Anforderungen zu unterschiedlichen Aspekten der IT-Sicherheit – hier geht es also weit über reine Netzwerk-Komponenten hinaus. Beispielsweise werden Maßnahmen in Bezug auf Office-Produkte, Internet-Anwendungen und mobile Anwendungen (Apps) ebenso adressiert wie Mobiltelefone, Smartphones und Endgeräte.
Da es bei der gemeinsamen Nutzung einer einheitlichen technischen Infrastruktur für jeden „Mandanten“ möglich und sinnvoll ist, eigene Festlegungen für konkrete IT-Sicherheitsvorkehrungen zu treffen, muss die IT-Sicherheitsrichtlinie auch von jeder Praxiseinheit persönlich angewendet und erfüllt werden.

11. Was ist mit „Dienstleistern vor Ort" gemeint?

Laut herkömmlicher Definition sind Dienstleister vor Ort (DVOs) „natürliche Personen." Es handelt sich also um externe Dienstleister, die Praxen unterstützen – nicht um interne System- oder Netzwerkadministratoren.

12. Können die Kosten zur Erfüllung der Anforderungen an die IT-Sicherheitsrichtlinie erstattet werden?

Viele der in der IT-Sicherheitsrichtlinie aufgeführten Anforderungen werden im Praxisalltag bereits angewendet, da sie durch die seit längerer Zeit geltenden Hinweise und Empfehlungen oder auch durch die Europäische Datenschutzgrundverordnung (DSGVO) vorgegeben sind. Zur Erfüllung der Vorgaben gemäß DSGVO und der „Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis" wurde auch keine Erstattung anfallender Kosten vereinbart. Die Erfüllung der Anforderungen aus der IT-Sicherheitsrichtlinie dient der Gewährleistung der eigenen Praxis-IT-Sicherheit.

13. Sind bei Nutzung des Parallelbetriebs in der Telematikinfrastruktur gesonderte Sicherheitsmaßnahmen erforderlich?

Wird die TI in Ihrer Praxis im Parallelbetrieb eingesetzt, dann sind gesonderte Sicherheitsmaßnahmen wie Firewall und Virenscanner zwingende Voraussetzung, denn im Parallelbetrieb wird das Praxisnetzwerk nicht durch den Konnektor geschützt. Wie der Konnektor in das Praxisnetzwerk integriert wird und welche Sicherheitsmaßnahmen ergriffen werden müssen, richtet sich nach den praxisspezifischen IT-Anforderungen und ist daher immer mit dem TI-Anbieter/IT-Servicepartner abzuklären.

14. Ist eine Hardware-Firewall (UTM Firewall, etc.) nach der "Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit" verpflichtend vorgeschrieben?

In Anlage 5 Nr. 4 in Verbindung mit Anlage 1 Nr. 32 wird gefordert, die Praxis bzw. das Praxisnetz auf Netzebene zu schützen. Die Kassenärztliche Bundesvereinigung empfiehlt dies mittels einer korrekt installierten, konfigurierten und gewarteten Hardware-Firewall oder mittels Konnektor im Reihenbetrieb umzusetzen.

15. Welche Auswirkungen hat die IT-Sicherheitsrichtlinie auf den Einsatz von zertifizierten Videosprechstunden-Diensten?

Die IT-Sicherheitsrichtlinie sieht nicht vor, dass es an den bestehenden Voraussetzungen zur Durchführung von Videosprechstunden Änderungen geben wird. Es wird nicht erforderlich sein, Videosprechstunden über die Telematikinfrastruktur durchzuführen.

16. Müssen Netzwerkadministratoren die Anforderungen zur IT-Sicherheitsrichtlinie erfüllen?

Externe Dienstleister können die Zertifizierung gemäß § 75b Abs. 5 SGB V erlangen – sie müssen es aber nicht zwingend tun. Interne Netzwerkadministratoren müssen sich nicht zertifizieren lassen.