RWF
Radiologen WirtschaftsForum
Informationsdienst für Radiologen in Praxis und Klinik

Gesundheitsdatenschutz

Die IT-Sicherheitsrichtlinie – ein stumpfes Schwert

von RAin, FAin für MedizinR Taisija Taksijan, LL.M., Hamburg, legal-point.de

Die KBV hat im Auftrag des Gesetzgebers die sogenannte IT-Sicherheitsrichtlinie beschlossen. Die darin genannten Anforderungen bei Nutzung von IT-Systemen sind zum Teil seit dem 01.04.2021 umzusetzen. Was der Vereinheitlichung und Vereinfachung für die Praxen im Umgang mit den Anforderungen der seit 2018 geltenden Datenschutz-Grundverordnung (DS-GVO) dienen soll, sorgt zunächst für Unsicherheit bei den Praxisinhabern. Bei genauerem Hinsehen macht sich Erleichterung breit – jedenfalls bei allen, die die bereits seit Jahren erforderlichen Maßnahmen zur Gewährleistung des Datenschutzes in der Praxis implementiert haben.

Struktur

Die Richtlinie enthält fünf Anlagen, in denen die technischen und organisatorischen Maßnahmen für die Nutzung eines bestimmten Programms oder Geräts („Zielobjekt") erläutert werden (online unter iww.de/s4621). Welche der Anlagen jeweils gilt, hängt vor allem von der Größe der Praxis ab:

- Für kleine Praxen (bis zu 5 ständig mit Datenverarbeitung betraute Personen) gelten die Anlagen 1 und 5.
- Für mittlere Praxen (6-20 solche Personen) gelten die Anlagen 1, 2, und 5.
- Für eine Großpraxis oder Praxis mit Datenverarbeitung im erheblichen Umfang (über 20 solche Personen oder mit einem überdurchschnittlichen Umfang der Datenverarbeitung) gelten die Anlagen 1, 2, 3 und 5.
- Für Praxen mit medizinischen Großgeräten (CT, MRT etc.) gilt Anlage 4.

Inhalt

Inhaltlich handelt es sich bei den beschriebenen Anforderungen um eine Reihe selbstverständlicher technischer und organisatorischer Maßnahmen zur Gewährleistung des Datenschutzes in der Arztpraxis nach der DSGVO. So wird etwa bei Nutzung mobiler Anwendungen (Apps) in der Praxis gefordert, dass „sichere Apps" genutzt werden. Gemeint ist, dass Apps aus offiziellen Stores verwendet werden und diese wieder gelöscht werden, wenn keine Nutzung erfolgt.

Bei Internet-Anwendungen wird z. B. die kryptografische Sicherung vertraulicher Daten gefordert. Es sollen also nur verschlüsselte Internet-Anwendungen genutzt werden. Dies gehört heute zum allgemeinen Standard und wird etwa beim Aufruf einer https://-Homepage gewährleistet.

Merke

Derartige – heutzutage selbstverständliche – Maßnahmen zur Vermeidung von Datenschutzlücken müssen Sie in jeder „kleinen" Praxis ergreifen, auch wenn diese in einer nicht für kleine Praxen geltenden Anlage beschrieben sind – z. B. die Verschlüsselung externer Datenträger in Anlage 3 für Großpraxen.

Die ersten Anforderungen gelten ab dem 01.04.2021. In der Richtlinie selbst sind keine Sanktionen bei Nichteinhaltung vorgesehen. Vorrangig gelten jedoch die Bestimmungen der DSGVO, zur ärztlichen Schweigepflicht etc. mit den datenschutz- und strafrechtlichen Konsequenzen bei Verstößen.

Guerbet

RWF
Radiologen WirtschaftsForum
Informationsdienst für Radiologen in Praxis und Klinik

Fazit

Praxen, die datenschutzrechtlich bisher schlecht aufgestellt waren, können anhand der Richtlinie ggf. dringenden Handlungsbedarf identifizieren. Umgekehrt bietet die Richtlinie in der aktuellen Fassung leider keine gesicherte Aussage über das Datenschutzniveau in Ihrer Praxis, wenn Sie alle dort aufgezählten (Mindest-)Anforderungen erfüllen.

Angesichts der nur rudimentären Regelungen darf in Zukunft mit Anpassungen der Richtlinie an die tatsächlichen Anforderungen der DSGVO im Sinne einer echten Hilfestellung für die Arztpraxen gerechnet werden.