AOK VERLAG

# Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

www.aok-verlag.info/ds-im-blick

Ausgabe März/April 2022 | **Seite 1**

## Inhalt

01 Unzureichende Berechtigungskonzepte

04 Datenschutzgefahr Smartphone?

07 Kurznotiz

# Unzureichende Berechtigungs-konzepte

**Zugriffsrechte und Berechtigungen sind immer von besonderer Bedeutung, wenn personenbezogene Daten unter Zuhilfenahme von elektronischen Fachverfahren (Softwareanwendungen) verarbeitet werden. Deren Bedeutung ist umso größer, wenn die Verarbeitung besondere Kategorien personenbezogener Daten, wie beispielsweise Gesundheitsdaten, umfasst.**

Dr. Sebastian Ertel

Je sensibler die Daten sind, umso strenger und differenzierter müssen die Rechte und Berechtigungen definiert sein. Restriktionen sind auch dann notwendig, wenn Daten von Beschäftigten verarbeitet werden.

Trifft die datenschutzrechtlich verantwortliche Stelle keine entsprechenden Maßnahmen und kommt es zu einer Verletzung der Vertraulichkeit und Integrität der Daten, stellt dies regelmäßig eine sanktionsbewehrte Datenpanne dar. Zudem kann daraus ein Schadensersatzanspruch der betroffenen Person resultieren

## Urteil des LG Flensburg

Einen solchen Fall musste kürzlich das Landgericht Flensburg (Urteil vom 19.11.2021, AZ: 3 O 227/19 – https://t1p.de/0jo7) entscheiden.

Verklagt wurde ein Krankenhaus auf Schadensersatz. Der Kläger war Chefarzt der Inneren Abteilung dieses Krankenhauses und infolge eines Herzinfarkts selbst dessen Patient, konkret der kardiologischen Abteilung. Während der Behandlung wurde von Beschäftigten etwa 150-mal auf die Patientendaten des Klägers im Krankenhaus-Informations-System (KIS) zugegriffen. Mindestes vier dieser Zugriffe

wurden als unzulässig angesehen. Das verklagte Krankenhaus gab folgende Stellungnahme ab:

*„Das Ergebnis der Prüfung der Zugriffe hat ergeben, dass die vier genannten Zugriffe zum Zwecke der Behandlung […] nicht erforderlich waren. Aus datenschutzrechtlicher Sicht wurden alle vier Zugriffe von unserem Datenschutzbeauftragten als nicht zulässig bewertet. Dieser Sachverhalt wurde jedoch von der zum Zeitpunkt des aufgenommenen Verstoßes verantwortlichen Geschäftsführung z. T. anders bewertet.* […] *Die Zugriffe waren aus meiner heutigen Sicht nicht zulässig.“*

Die eingeschaltete Aufsichtsbehörde stellte fest, „dass die […] Zugriffe einen Verstoß gegen […] Art. 5, 25, 32 DS-GVO bzw. § 22 BDSG darstellten.

Im Weiteren konnte der Kläger feststellen, dass es selbst vier Jahre nach seiner Behandlung von mehreren Computern aus möglich war, ohne Zugriffsdokumentation auf das installierte Radiologie-Programm PACS zuzugreifen. Durch die Eingabe des Namens des Klägers konnten dessen Koronarfilm und die durchgeführte Dilatation der Herzkranzgefäße eingesehen werden.

Das unzureichende Zugriffs- und Berechtigungskonzept wurde vom LG Flensburg als Datenschutzverstoß gewertet. Der Schutz der Daten sei eine Nebenpflicht aus dem Behandlungsvertrag, der mit der Inanspruchnahme medizinischer Versorgung geschlossen wurde. Aufgrund dieser Nebenpflicht habe das Krankenhaus „dafür Sorge zu tragen, dass die zur Behandlung und ihrer Dokumentation (§ 630f BGB) erhobenen personenbezogenen Daten des Patienten nur zu erlaubten Zwecken verarbeitet werden, sei es durch den Behandelnden selbst, sei es durch ihm unterstellte natürliche Personen oder Erfüllungsgehilfen, die Zugang zu den personenbezogenen Patientendaten haben.“

Keine Relevanz habe dabei die Frage, ob der Datenschutzverstoß seine Ursache in einem Organisationsverschulden des Krankenhauses oder in einem Fehlverhalten der Beschäftigten hat, da in beiden Fällen das Krankenhaus verantwortlich sei.

Der Erfolg der Klage scheiterte letztlich an der Verjährung des Anspruches.

## Was ist zu tun?

Der Fall veranschaulicht deutlich, wie wichtig ein differenziertes Berechtigungskonzept, die Protokollierung von Zugriffen und die Sperrung von Datensätzen sind. Diese Maßnahmen sollten regelmäßig, durch Audits, auf den Prüfstand gestellt werden. Hier kann der Datenschutzbeauftragte helfen. Daneben kann auf die Orientierungshilfe KIS (https://t1p.de/bl4b) zurückgegriffen werden, in der viele Fragestellungen des Datenschutzes im Klinikalltag im Zusammenhang

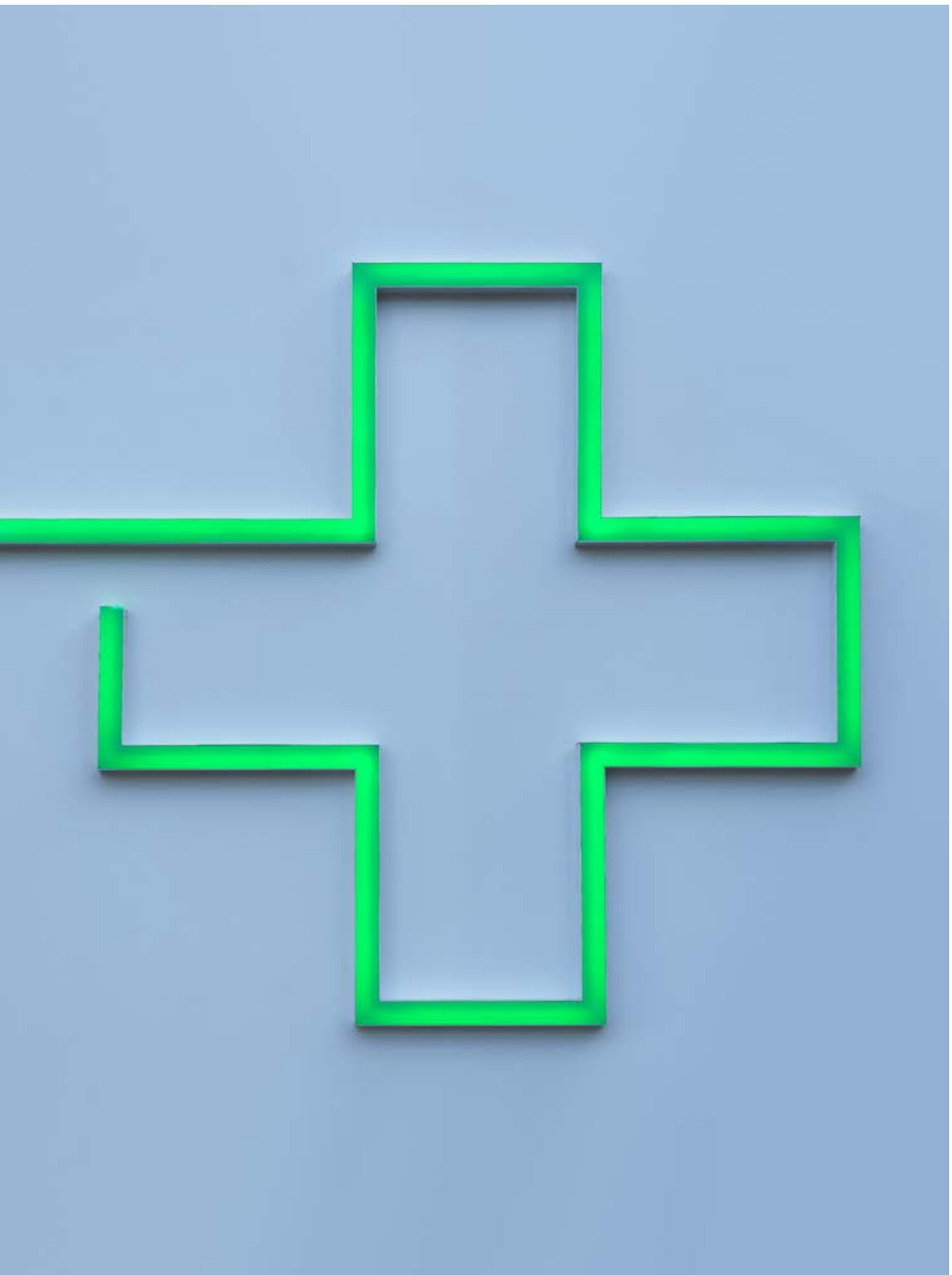
mit dem Einsatz von Krankenhaus-Informations-Systemen behandelt werden.

## KIS-Bordmittel

Die verschiedenen Krankenhaus-Informationssysteme bieten von Haus aus verschiedene Bordmittel, um einen Datenschutzverstoß wie in dem oben beschriebenen Fall zu vermeiden.

**Schutz besonderer Personen**
Die meisten KIS bieten Möglichkeiten an, um bestimmte Patienten (VIP, Beschäftigte) besonders zu schützen, indem der Zugriff auf deren Daten restriktiv geregelt wird. Die Beschreibung der abstrakten Vorgaben in der Orientierungshilfe KIS befinden sich in Teil I Absatz 41.

- **VIP-Kennzeichnung:** Der Datensatz wird bei der Patientensuche für nicht berechtigte Benutzerinnen ausgeblendet. Die VIP-Kennzeichnung kann genutzt werden, wenn Patienten eine Auskunftssperre, z. B. am Empfang bei Besucheranfragen, wünschen.
- **Extended Patient Privacy Protection (EPP):** Über EPP werden die Beschäftigten, die auf den Datensatz der betreffenden Person zugreifen dürfen, festgelegt. Für alle anderen Beschäftigten ist der Datensatz nicht abrufbar.
- **Versiegelung:** Ein versiegelter Datensatz ist vor dem allgemeinen Zugriff gesperrt. Das Siegel kann von den Anwenderinnen jederzeit gebrochen werden. Hierzu verlangt das KIS eine Begründung und eine Authentifizierung (Passworteingabe). Nach dem Schließen des Datensatzes wird ein neues Siegel erstellt, das bei einem nachfolgenden Zugriff wie beschrieben erneut gebrochen werden muss.



**Sperrung von Fällen**
Unabhängig vom Status der Patienten (VIP, Beschäftigte, etc.) muss eine Sperrung des Datensatzes nach Abschluss der Behandlung erfolgen. Die Beschreibung der abstrakten Vorgaben in der Orientierungshilfe KIS befindet sich in Teil I Absatz 22 und 25.

Eine Sperrung von Behandlungsfällen kann mit Hilfe von Bedingungen erreicht werden. So kann beispielsweise mit der Bedingung „Zeitbegrenzung nach Entlassung“ der Zugriff auf einen Patientendatensatz auf bestimmte Zeitfenster nach der Entlassung reglementiert werden. Ein großer Vorteil ist es, wenn die Bedingung an die Berechtigungen geknüpft ist. In diesem Fall ist es möglich, die Sperrung eines Datensatzes für die verschiedenen Personengruppen nach unterschiedlichen Zeiträumen festzulegen.

# Datenschutzgefahr Smartphone?

**Einrichtungen des Gesundheitswesens müssen dafür Sorge tragen, dass personenbezogene Patientendaten vertraulich verarbeitet werden. In der Praxis bedeutet dies an vielen Stellen eine nicht unerhebliche Herausforderung. Dieser Artikel beschäftigt sich mit der Frage, welche Risiken bedacht und welche Maßnahmen getroffen werden müssen, wenn Gesundheitseinrichtungen ihren Beschäftigten Smartphones zur Verfügung stellen wollen**

Sven Venzke-Caprarese

## Ausgangslage

Sofern Gesundheitseinrichtungen den Beschäftigten Smartphones zur Verfügung stellen wollen, muss Einiges beachtet werden. Um die Lage für die konkrete Einrichtung zu bewerten, sollte erst einmal die jeweilige Ausgangslage festgestellt werden.

**Betriebssystem**
In diesem Rahmen ist es relevant, über welches Betriebssystem die Smartphones verfügen sollen. In den meisten Fällen wird es sich heutzutage um Android- oder iOS-basierte Betriebssysteme handeln.

Relevant ist auch, ob die Gesundheitseinrichtung nur ein Betriebssystem zulässt oder mehrere unterschiedliche. Da die Risiken und Maßnahmen für jedes Betriebssystem separat festgestellt werden müssen, kann es in der Praxis empfehlenswert sein, sich für ein Betriebssystem zu entscheiden und die Maßnahmen hierauf auszurichten.

**Dienstliche und private Nutzung**
Ebenfalls relevant für die Bewertung der Ausgangslage ist die Frage, ob die dienstlich zur Verfügung gestellten Smartphones ausschließlich dienstlich oder auch privat genutzt werden dürfen. Die Vor- und Nachteile sind hier genau gegeneinander abzuwägen. Die Ermöglichung der Privatnutzung wird Beschäftigten oftmals die Möglichkeit geben, sich die Kosten für ein privates Smartphone zu sparen und nicht ständig zwei Smartphones mit sich führen zu müssen. Andererseits steigen die Risiken für die Vertraulichkeit der dienstlichen Daten, wenn Smartphones auch privat genutzt werden dürfen.

**BYOD**
Gelegentlich wird den Beschäftigten erlaubt, ihr eigenes Smartphone auch für die Verarbeitung dienstlicher Daten zu nutzen (Stichwort: „Bring Your Own Device“). Die Risiken bei der Variante BYOD sind dabei sogar noch höher als bei der gemischten privat-dienstlichen Nutzung von dienstlich zur Verfügung gestellten Geräten.

## Ohne MDM geht es fast nicht mehr

Gesundheitseinrichtungen, die die Nutzung von Smartphones zur Verarbeitung von dienstlichen Daten gestatten, kommen grundsätzlich nicht mehr um die Nutzung eines Mobile Device Managements (MDM) herum.

Mithilfe eines MDM können verschiedene Maßnahmen getroffen

werden, um den Risiken für die Vertraulichkeit der Daten in der Praxis zu begegnen.

**Containerlösung**
In den Fällen der gemischten privatdienstlichen Nutzung muss ein MDM grundsätzlich über die Funktion verfügen, die Bereiche, in denen dienstliche Daten verarbeitet werden, von den Bereichen, in denen private Daten verarbeitet werden, zu trennen. Dabei muss sichergestellt werden, dass die Daten des einen Bereichs nicht in den anderen Bereich gelangen können. Nutzt ein Mitarbeiter z.B. WhatsApp im privaten Bereich, darf hiervon keinesfalls der dienstliche Bereich berührt werden. Die Trennung gilt dabei z.B. auch für Kontaktdaten, Kalenderdaten, Notizen, Mails etc.

**Richtlinien**
Ein gutes MDM ermöglicht es der Gesundheitseinrichtung, bestimmte Vorgaben im Hinblick auf die Nutzung des Smartphones technisch zu erzwingen, z.B.:

- Viele MDMs ermöglichen es den Administratoren nicht nur zu sehen, welche Geräte über den aktuellen Updatestatus verfügen. Sie ermöglichen auch das automatische Ausspielen von Updates oder das Sperren von Geräten, bei denen die Nutzer nicht die aktuellen Updates vorgenommen haben.
- Daneben ist es über das MDM oftmals möglich, verloren gegangene Smartphones zu orten oder aus der Ferne zu löschen.
- Eine zentrale Funktion ist auch die Vorgabe von Mindestanforderungen an die Gerätesperre und an die Passwortkomplexität. Zudem kann über das MDM eingestellt werden, dass sich die Geräte bei mehrfacher Fehleingabe des Passworts von selbst löschen oder dauerhaft sperren.
- Smartphones zeigen selbst im gesperrten Zustand gelegentlich noch Benachrichtigungen an, z.B. im Rahmen von Kurznachrichten auf dem Sperrbildschirm. Die Anzeige solcher Benachrichtigungen im gesperrten Modus sollte vom MDM unterdrückt werden.
- Die Nutzung von Diensten der Betriebssystembetreiber kann über ein gutes MDM vorgegeben werden. So kann z.B. dafür gesorgt werden, dass die vom Anbieter bereitgestellten Cloud-Dienste nicht genutzt werden können, damit dienstliche Daten nicht aus Versehen in die Cloud synchronisiert werden.
- Viele MDMs erlauben auch die Steuerung, welche Apps Nutzer aus den App Stores laden dürfen und welche nicht. Bei gemischter privat-dienstlicher Nutzung und bei Anwendung eines MDMs mit Containerlösung wird dabei gelegentlich der private Bereich kaum und dafür der dienstliche Bereich auf die dienstlich notwendigen Apps beschränkt.


## Absicherung des MDM

Auch die Nutzung eines MDM erfordert aus datenschutzrechtlicher Sicht einige Vorkehrungen. So muss z.B. sichergestellt werden, dass nur berechtigte Personen Zugriff auf das Backend des MDM haben (in der Regel ein Administrator).

Zudem muss der Zugang zum MDM angemessen abgesichert sein. Sofern das MDM über eine Webanwendung administriert wird, kann sich das Erfordernis einer Zwei-Faktor-Authentisierung ergeben. In diesem Rahmen muss bei der Nutzung eines MDM immer auch geprüft werden, ob Auftragsverarbeiter involviert sind und ob Verträge nach Art. 28 DS-GVO zur Auftragsverarbeitung abgeschlossen werden müssen.

Daneben machen es die Überwachungsfunktionen, die Löschfunktionen und etwaige Ortungsfunktionen eines MDM erforderlich, dieses mit dem Datenschutzbeauftragten und der Personalvertretung abzustimmen.

Im Hinblick auf die Beschäftigten sollte der Einsatz eines MDM zu Beginn mit einer Datenschutzinformation nach Art. 13 DS-GVO verbunden sein.

## Verschlüsselung

Besonders wichtig (aber in der Praxis kaum noch ein Problem) ist die Anforderung, dass die Smartphones Daten nur verschlüsselt speichern dürfen. Im Hinblick auf Android und iOS kann mittlerweile davon ausgegangen werden, dass die auf dem Smartphone gespeicherten Daten verschlüsselt sind, sofern das Gerät gesperrt ist. Allerdings muss bei Android-basierten Geräten noch geprüft werden, ob sich diese Verschlüsselung auch auf etwaige zusätzliche Speichermedien erstreckt (z.B. auf SD-Karten, die zur Speichererweiterung genutzt werden).

## Private Accountinformationen

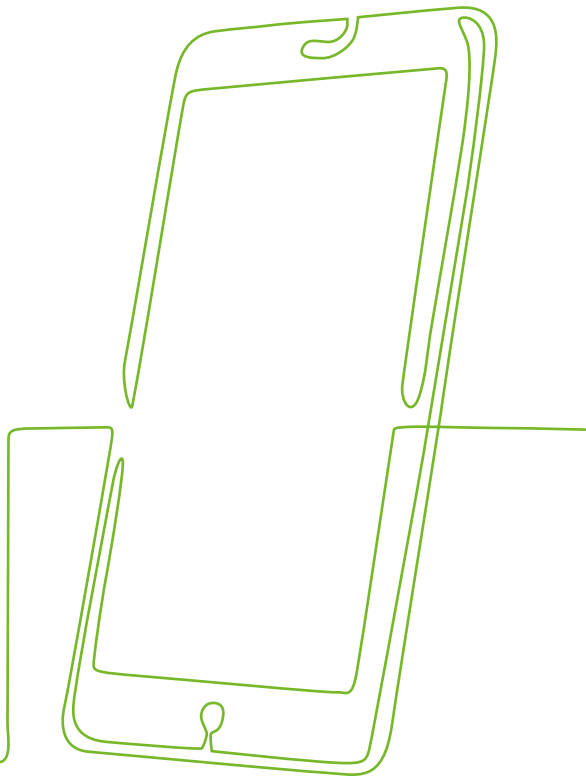
Insbesondere bei der gemischten privat-dienstlichen Nutzung oder bei BYOD kommt es vor, dass Beschäftigte private Accountdaten zur Nutzung der Betriebssysteme verwenden (z.B. die private AppleID). Dies kann jedoch schnell gefährlich werden. Denn was viele nicht wissen, ist, dass sich einige Apps geräteübergreifend synchronisieren, wenn sie z.B. mit derselben AppleID betrieben werden. Nachrichten oder Inhalte der Notizen App überwinden auf diese Weise schnell die Gerätegrenze und landen (oft unbewusst) auf anderen (privaten) Geräten der Beschäftigten.

## Life Cycle und Geräte-vernichtung

Gesundheitseinrichtungen sollten bereits bei der Entscheidung für ein Betriebssystem bzw. für einen Smartphonehersteller den Life Cycle des Geräts im Blick behalten.

Dabei kommt es insbesondere darauf an, wie lange für das jeweilige Smartphone voraussichtlich noch Sicherheitsupdates verfügbar sind. Wer sich hier für ein vermeintlich günstiges Modell entscheidet, für welches aber nur noch sehr kurz die entsprechenden Sicherheitsupdates bereitgestellt werden, der zahlt womöglich doppelt.

Auch die Vernichtung bzw. die datenschutzkonforme Löschung oder Wiederverwertung der Geräte sollte bedacht werden.



## Sonstiges

Wie bereits dargestellt, geht die Bereitstellung von Smartphones mit einer Reihe von notwendigen technischen Maßnahmen einher. Daneben müssen aber auch eine Reihe organisatorischer Maßnahmen getroffen werden, z.B.:

- Anweisungen zum Umgang mit Smartphones für Beschäftigte (z.B. die Anweisung, verloren gegangene Geräte unverzüglich zu melden; die Anweisung, bestimmte Apps nicht zu nutzen; die Anweisung, keine dienstlichen Daten im privaten Bereich zu speichern etc.)
- Im Hinblick auf die Nutzung von Smartphones im dienstlichen Bereich kann zudem an weitere Sensibilisierungsmaßnahmen (z.B. Schulungen) gedacht werden.

Daneben muss die Gesundheitseinrichtung prüfen, ob die etwaig notwendigen Betriebs- und Dienstvereinbarungen, Datenschutzinformationen nach Art. 13 DS-GVO, Auftragsverarbeitungsverträge, Einwilligungen von Beschäftigten (z.B. zur Fernlöschung oder Ortung im Falle der Verlustmeldung) vorliegen.

## Fazit

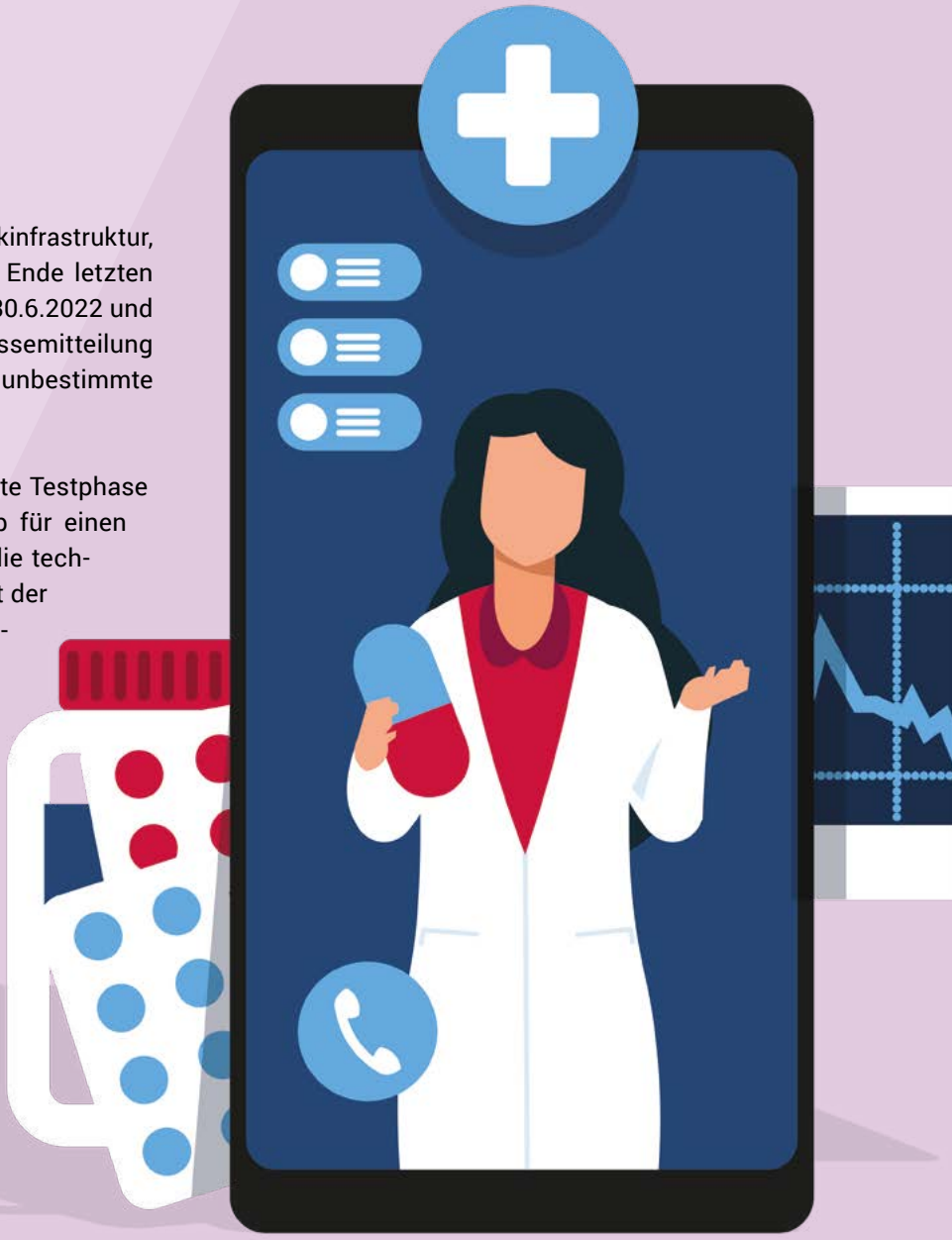
Die Nutzung von Smartphones ist datenschutzrechtlich auch für Gesundheitseinrichtungen gut möglich. Dabei ist grundsätzlich die rein dienstliche oder auch die gemischt privat-dienstliche Nutzung möglich und (theoretisch) sogar BYOD. Allerdings wird sich die Nutzung eines Mobile Device Managements vermutlich in keinem der genannten Fälle vermeiden lassen. Zudem muss jede Gesundheitseinrichtung eine individuelle Risikoanalyse auf Grundlage des festgestellten Ausgangszustands durchführen und dabei mindestens die hier genannten Punkte berücksichtigen.

# Kurznotiz

## Einführung des E-Rezeptes auf unbestimmte Zeit verschoben

Das E-Rezept, eine Anwendung der Telematikinfrastruktur, sollte ursprünglich zum 1.1.2022 starten. Ende letzten Jahres wurde der Start zunächst auf den 30.6.2022 und nunmehr, wie der Bundestag in einer Pressemitteilung vom 14.2.2022 (hib 53/2022) mitteilte, auf unbestimmte Zeit verschoben.

Die Offizielle Begründung: „Die bundesweite Testphase sei offen verlängert worden […]. Maßstab für einen späteren flächendeckenden Roll-Out sei die technische Verfügbarkeit gemessen an den mit der Selbstverwaltung vereinbarten Qualitätskriterien." Dies ist gerade in den ländlichen Regionen nachvollziehbar, benötigt man doch neben verschiedener Hardware auch eine stabile und schnelle Internetverbindung.



© AOK-Verlag GmbH | Lilienthalstraße 1-3 | 53424 Remagen | Tel 02642 931-333 | Fax 02642 931-215
Mail: fachinfo@aok-verlag.de | Web: http://www.aok-verlag.info | Herausgeber: AOK-Verlag GmbH, Remagen
Geschäftsführung: Frank Schmidt | Redaktion: Prof. Dr. Benedikt Buchner, Dr. Sebastian Ertel, Sven Venzke-Caprarese
Der Inhalt des vorliegenden Newsletters ist mit größter Sorgfalt zusammengestellt worden.
Eine Haftung für die Angaben übernimmt der Verlag jedoch nicht. | Bildnachweise: GettyImages, AOK-Verlag

Wir bemühen uns um eine geschlechtergerechte Sprache. Weil wir Ihnen den Lesefluss so angenehm wie möglich gestalten möchten, wählen wir in vielen Fällen dennoch die männliche Form. Die Inhalte beziehen sich aber immer auf alle Geschlechter. Wenn nicht, weisen wir ausdrücklich darauf hin.

# Praxishandbuch für Datenschutzbeauftragte im Gesundheitswesen

Welche Patientendaten dürfen an wen und in welcher Form übermittelt werden? Wie ist ein Empfangsbereich im Krankenhaus zu strukturieren, damit die Privatsphäre jedes Einzelnen gewährleistet wird? Wie muss ein Datenschutzkonzept aussehen, damit es als Grundlage für einen Audit dienen kann? Und wer hat eigentlich auf welche Patientendaten Zugriff?

Die Herausforderung ist, dass die innerbetrieblichen Abläufe durch die Umsetzung datenschutzrechtlicher Vorgaben nicht beeinträchtigt werden sollen - ein Spagat, der gemeistert werden muss. Hinzu kommt, dass viele Datenschutzbeauftragte diese Tätigkeit neben ihrem Hauptaufgabengebiet ausüben und sich ein fundiertes Wissen im IT-Bereich erst aneignen müssen, um mit Kollegen oder Externen auf Augenhöhe zu kommunizieren.

Das Handbuch „Datenschutz im Gesundheitswesen“ greift die typischen Arbeits- und Problemfelder auf und liefert Lösungen, die Rechtssicherheit, Nachhaltigkeit und Akzeptanz bei Aufsichtsbehörden bieten. Der Schwerpunkt des Handbuches liegt in der praktischen Umsetzung der datenschutzrechtlichen Vorgaben im betrieblichen Alltag, bspw. bei den spezifischen Anforderungen in den verschiedenen Bereichen des Gesundheitswesens, wie Krankenhaus oder Arztpraxis.

Im exklusiven Online-Kundenbereich finden Sie das Werk als E-Book. Mittels pdf-Download laden Sie kapitelweise Ihr Handbuch herunter und können es direkt an Ihrem Rechner einsetzen. So sind Sie unabhängig von Ihrem Arbeitsort und haben jederzeit Zugriff auf die Datenschutzbestimmungen.


- 2 Ordner mit Register im Format DIN A5,
- ca. 1.500 Seiten Inhalt
- ISBN: 978-3-553-43000-5
- Preis **177,20 €** inkl. MwSt.
- Uneingeschränkter Online-Zugriff
  inkl. 3-4 kostenpflichtige Nachtragslieferungen
  pro Jahr zum Preis von jeweils **84,90 €** inkl. MwSt.
  und versandkostenfreier Zusendung im Inland.