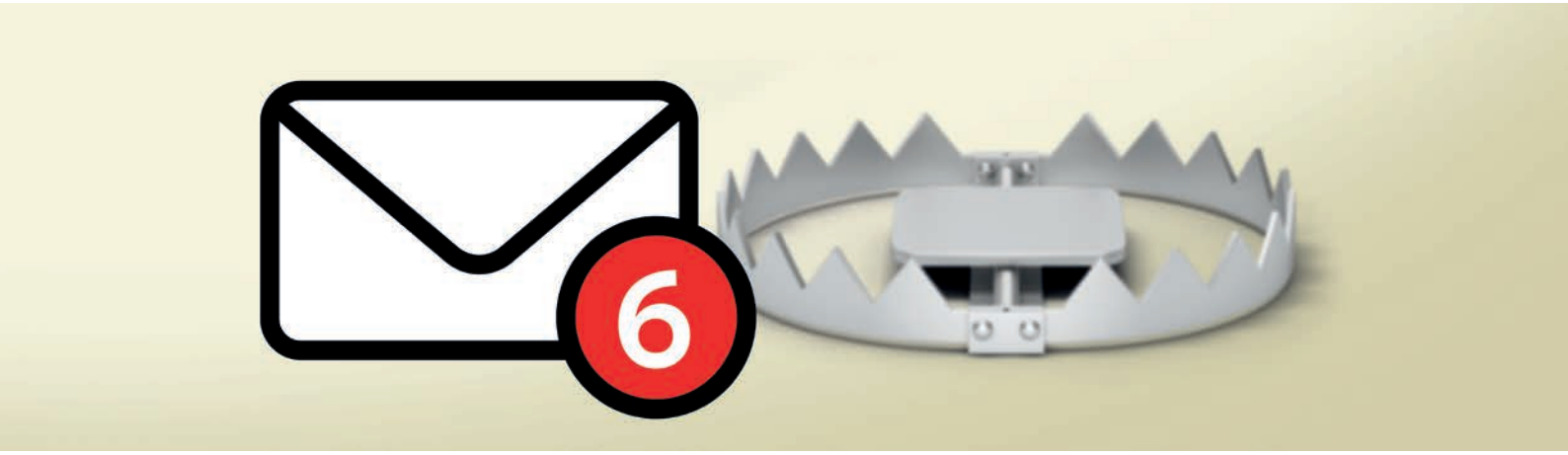
AOK Medien

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

www.aok-medien.info/ds-im-blick Ausgabe 05/2026

Inhalt



Fallstricke bei dienstlichen E-Mail-Accounts

Die meisten Beschäftigten besitzen eine dienstliche E-Mail-Adresse. Technisch leicht einzurichten, aber datenschutzrechtlich mit einigen Fallstricken verbunden. Welche das sind und wie diese umgangen werden können, soll nachfolgend aufgezeigt werden.

Dr. Sebastian Ertel

Individuell oder Funktion

Die erste Frage, die bei der Vergabe von E-Mail-Adressen zu klären ist, betrifft deren Art: Soll es eine individuelle oder eine Funktions-E-Mail-Adresse sein? Eine individuelle E-Mail-Adresse ist eindeutig einer bestimmten Person zugeordnet; sie setzt sich in der Regel aus Namensteilen des jeweiligen Beschäftigten zusammen, beispielsweise aus Vor- und Nachname oder deren Abkürzungen. Demgegenüber ist die Funktions-E-Mail-Adresse nicht an eine einzelne Person, sondern an eine bestimmte Organisationseinheit gebunden, der mehrere Mitarbeitende zugeordnet sind. Funktions-E-Mail-Adressen bestehen dauerhaft und unabhängig von personellen Veränderungen, während individuelle E-Mail-Adressen unmittelbar am Bestand des jeweiligen Beschäftigungsverhältnisses hängen und mit dessen Ende aufgelöst werden. Funktions-E-Mail-Adressen finden sich typischerweise in Bereichen wie dem Support, dem Vertrieb und Marketing, dem Personalwesen, der Verwaltung und Organisation, der Buchhaltung sowie der EDV. Sie gewährleisten dort eine kontinuierliche Erreichbarkeit, auch wenn einzelne Mitarbeitende das Unternehmen verlassen oder ihre Rolle wechseln.

OWA

Neben der klassischen PC- oder Mobile-Applikation kann Outlook auch über den Browser in Form der sogenannten Outlook Web App (OWA) genutzt werden. Das grundlegende Problem dabei: In der Standardkonfiguration ist OWA direkt aus dem Internet aufrufbar. Hierzu werden lediglich die entsprechende URL sowie Benutzername und Passwort benötigt. Diese vergleichsweise wenigen Zugangsdaten können beispielsweise durch Phishing-, Keylogger- oder andere gezielte Angriffe verhältnismäßig leicht in die Hände unbefugter Dritter gelangen, die das betroffene Konto sowie die dort abrufbaren, teils sensiblen Daten, missbräuchlich nutzen können. Um dieses Risiko wirksam zu reduzieren und den Zugang zusätzlich abzusichern, ist die Verwendung einer Multi-Faktor-Authentifizierung (MFA) verpflichtend, beispielsweise über ein Time-based One-time Password (TOTP), das mithilfe einer Authenticator-App – etwa dem Google Authenticator – generiert wird und bei jedem Anmeldevorgang als zusätzlicher Sicherheitsfaktor eingegeben werden muss.

Privatnutzung

Grundsätzlich sind dienstliche E-Mail-Adressen nur dienstlich zu nutzen. Wird eine private Nutzung geduldet oder erlaubt, ist es für den Arbeitgeber nicht mehr ohne weiteres möglich, beispielsweise bei ungeplanten Abwesenheiten, auf ein Postfach zuzugreifen, um nach relevanten E-Mails zu sehen. Aus diesem Grund sollte die private Nutzung verboten werden.

Abwesenheiten

Bei geplanten (z. B. Urlaub) oder ungeplanten Abwesenheiten (z. B. Krankheit) ist die Nutzung eines Abwesenheitsassistenten der Regelfall. Hierfür sollten klare und verbindliche Vorgaben gemacht werden, wie entsprechende Abwesenheitsnotizen zu formulieren sind. Gerade bei ungeplanten Abwesenheiten wird häufig dazu geneigt, den konkreten Abwesenheitsgrund zu benennen. Dabei handelt es sich jedoch regelmäßig um eine Datenverarbeitung ohne ausreichende rechtliche Grundlage. Darüber hinaus werden auf diese Weise einer unbekannten Anzahl an Personen zum Teil sensible Informationen – wie der Gesundheitsstatus des Betroffenen und die voraussichtliche Dauer der Abwesenheit – bekanntgemacht. Dabei handelt es sich um Daten, die für einen Missbrauch, beispielsweise im Rahmen von Social-Engineering-Angriffen, geradezu prädestiniert sind. Eine mögliche Formulierung wäre beispielsweise:

> *Vielen Dank für Ihre Nachricht.*
>
> *Ich bin aktuell nicht verfügbar und werde Ihre Nachricht nach meiner Rückkehr bearbeiten. Für dringende Anliegen steht Ihnen in der Zwischenzeit folgende Kontaktperson zur Verfügung: Organisationseinheit / Name/E-Mail-Adresse].*
>
> *Mit freundlichen Grüßen*

BYOD/Weiterleitung

Werden private Geräte für dienstliche Zwecke eingesetzt (sog. „Bring your own device" - BYOD), besteht die konkrete Gefahr, dass dadurch die etablierten Sicherheitsmaßnahmen der Einrichtung geschwächt oder umgangen werden. Der Grund hierfür liegt darin, dass private Geräte in der Regel nicht im gleichen Maße konfiguriert und abgesichert sind wie dienstlich verwaltete Geräte und somit ein erhebliches Sicherheitsrisiko darstellen können. Sollen dienstliche Apps auf privaten Geräten genutzt werden, sollte mittels MDA (Mobile Device Access) eine Richtlinie zur Nutzung der dienstlichen Anwendungen geschaffen werden, beispielsweise wie diese Apps vor Zugriffen abgesichert werden und, dass die Datensynchronisation im Bedarfsfall (z. B. bei Verlust des Gerätes) gekappt werden kann.

Beendigung des Beschäftigungsverhältnisses

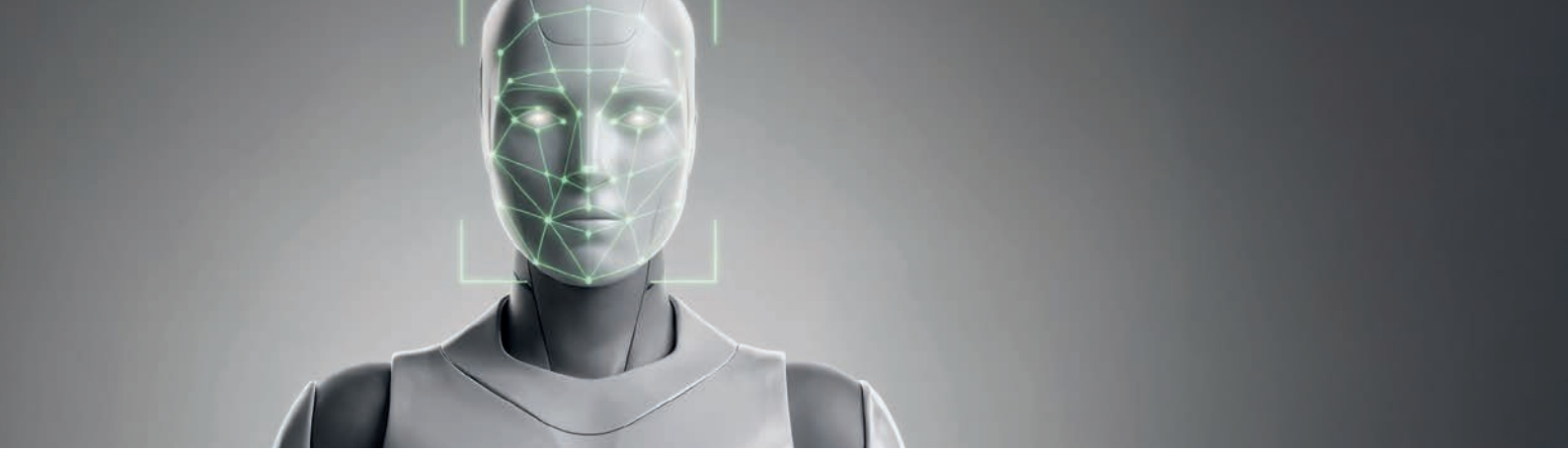
Endet ein Beschäftigungsverhältnis, muss klar geregelt sein, wie mit der persönlichen E-Mail-Adresse und dem E-Mailpostfach umgegangen wird. Zunächst ist auch hier mit einem einheitlichen Abwesenheitsassistenten zu arbeiten, der datensparsam darauf hinweist, dass der Inhaber des Postfaches nicht mehr erreichbar ist, und einen alternativen Kommunikationsweg aufzeigt. Eine mögliche Formulierung wäre:

> *Vielen Dank für Ihre Nachricht.*
>
> *Das von Ihnen kontaktierte Postfach ist nicht mehr aktiv. Für Ihr Anliegen wenden Sie sich bitte direkt an: [Organisationseinheit / Name/E-Mail-Adresse].*
>
> *Eingehende Nachrichten an diese Adresse werden nicht bearbeitet oder weitergeleitet. Wir bitten um Ihr Verständnis.*

Je nach Funktion der ausgeschiedenen Person – etwa Unternehmensleitung, mittleres Management oder fachliche Ebene ohne Führungsverantwortung – sind unterschiedliche Fristen vertretbar, innerhalb derer die jeweilige E-Mail-Adresse sowie das zugehörige Postfach zu löschen sind. Je nach Zuordnung und Hierarchieebene sollten E-Mail-Adressen nach zwei bis 13 Wochen und E-Mail-Konten nach zwei bis 26 Wochen vollständig gelöscht werden. Der Versand einer Nachricht an eine nicht mehr existierende E-Mail-Adresse löste früher in der Regel automatisch eine Fehlermeldung in Form eines sogenannten Non-Delivery Reports aus. Dies geschieht heutzutage kaum noch, da solche Rückmeldungen beispielsweise dazu missbraucht werden könnten, dass Spammer auf diesem Wege gültige von ungültigen E-Mail-Adressen unterscheiden und ihre Verteilerlisten entsprechend bereinigen. Eine Deaktivierung des Non-Delivery Reports ist daher zu empfehlen. Ein Nebeneffekt: Ausgeschiedene Mitarbeitende können die Löschung ihrer ehemaligen E-Mail-Adresse nicht mehr eigenständig prüfen und, was in der Vergangenheit öfters vorkam, Schadensersatzansprüche nicht mehr ohne weiteres geltend machen. Gleichwohl besteht die Möglichkeit, über verschiedene Webseiten (z.B. **https://captainverify.com** oder **https://mailn-joy.com**) zu prüfen, ob E-Mail-Adressen noch existieren. Löschroutinen sollten daher konsequent umgesetzt werden.

Fazit

Der Umgang mit E-Mail-Adressen und den dazugehörigen Postfächern bedarf klarer und verbindlicher Regelungen, insbesondere im Hinblick auf das Ende eines Beschäftigungsverhältnisses. Diese sollten schriftlich fixiert und allen Beteiligten zugänglich gemacht werden.



KI und Datenschutz

Der Einsatz von Künstlicher Intelligenz (KI) lässt sich aus dem Arbeitsalltag vieler Berufsgruppen nicht mehr wegdenken. Auch Einrichtungen des Gesundheitswesens verfügen daher immer häufiger über Regelungen, die die Nutzung von KI regeln. Doch was ist datenschutzrechtlich eigentlich zu beachten, wenn personenbezogene Daten mithilfe von KI-Systemen verarbeitet werden sollen?

Sven Venzke-Caprarese

Rahmenbedingungen

Bevor KI-Systeme für die Verarbeitung von personenbezogenen Daten genutzt werden können, müssen durch die Organisation einige Rahmenbedingungen bereitgestellt werden.

Zum einen muss, wie bei jedem anderen IT-System, gewährleistet werden, dass die notwendigen datenschutzrechtlichen Rahmenbedingungen geschaffen werden. Sofern Dienstleister den Betrieb des KI-Systems unterstützen, müssen daher Verträge zur Auftragsverarbeitung nach Art. 28 DSGVO geschlossen werden. Hier ist insbesondere darauf zu achten, dass die Anbieter von KI-Systemen die eingegebenen Daten nicht zweckfremd zum Training der KI verwenden. Sofern der Anbieter des KI-Systems in einem Drittland sitzt, muss die Angemessenheit des Datenschutzniveaus gewährleistet sein. Dies kann zum Beispiel auch durch den Abschluss von Standard-Datenschutzklauseln geschehen, wobei ggf. zusätzlich auch ein Transfer-Impact-Assessment durchgeführt werden muss. Sofern personenbezogene Daten in KI-Systemen verarbeitet werden sollen, die dem Berufsgeheimnis des § 203 StGB unterliegen, bedarf es zusätzlicher Regelungen, die den Dienstleister und seine Beschäftigten noch einmal ganz besonders zur Geheimhaltung verpflichten.

Neben diesen rechtlichen Rahmenbedingungen kommen weitere Anforderungen hinzu. Hier geht es dann zum Beispiel um die Frage, wie sich Beschäftigte gegenüber dem KI-System angemessen sicher anmelden können und ob hierfür Nutzername und Passwort ausreichend sind oder eine Zwei-Faktor-Authentisierung erforderlich ist. Hinzu kommt die Frage, ob personenbezogene Daten im KI-System gespeichert werden und wenn ja, wie lange. Bestenfalls werden hier im Vorfeld bereits Löschfristen definiert, die automatisch, also technisch, umgesetzt werden, ohne dass die Nutzer selbst tätig werden müssen. Sofern das KI-System eine automatische Löschung nicht unterstützt, muss die Löschung zumindest organisatorisch geregelt werden, zum Beispiel durch eine entsprechende Löschrichtlinie. Häufig wird bei KI-Systemen auch die administrative Parametrisierung der Einstellungen relevant – diese sollten nach dem Grundsatz privacy by default erfolgen und sind häufig nicht die Grundeinstellungen im Auslieferungszustand.

Daneben stellen sich häufig Fragen der Informationssicherheit, etwa wenn es darum geht, wie sicher der Datenfluss zum KI-System ist. Hier wird eine Transportverschlüsselung in der Regel unerlässlich sein. Daneben stellen sich auch bei einem KI-System grundsätzlich die gleichen Fragen, wie bei jedem anderen IT-System. Hierbei kann dann unter anderem relevant werden, wie das KI-System in die Prozesse zur Softwareverteilung eingebunden wird, ob ein Update- und Patchmanagement erforderlich ist, ob Backups des KI-Systems erforderlich werden und ob eine Berücksichtigung des KI-Systems in vorhandene On- und Offboarding-Prozesse erfolgt. Insgesamt sollte auch das KI-System anhand der vorhandenen Schutzziele der Organisation bewertet werden, also zum Beispiel im Hinblick auf Verfügbarkeit, Vertraulichkeit, Integrität und ggf. weiteren Schutzzielen, wie Patientensicherheit. Das KI-System sollte daher in ein etwaig vorhandenes Informations

sicherheits-managementsystem aufgenommen werden. Wie jedes andere IT-System, das für die Verarbeitung von personenbezogenen Daten bestimmt ist, sollte schließlich auch das KI-System in das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO aufgenommen werden. Zudem sollte die Erforderlichkeit einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO geprüft werden.

Datenschutz

Im Hinblick auf den Datenschutz muss die Organisation gewährleisten, dass das KI-System auch im Betrieb datenschutzrechtlich in zulässiger Weise genutzt wird. Hier wird es häufig auch auf die Verhaltensweise der Beschäftigten ankommen, die das KI-System nutzen.

Je nachdem, wie das KI-System ausgeprägt ist, kann es erforderlich werden, die Beschäftigten auch noch einmal speziell zur Einhaltung des Datenschutzes zu schulen bzw. zu sensibilisieren. Insbesondere bei KI-Systemen mit allgemeinem Verwendungszweck (hierzu zählen zum Beispiel die klassischen KI-Chatsysteme wie ChatGPT oder Copilot) fällt es den Nutzern oftmals schwer, bereits erlernte Datenschutzprinzipien auf die neuen Lösungen anzuwenden. Oftmals besteht eine Unsicherheit schon bei der Frage, welche Rechtsgrundlage eigentlich für die Verarbeitung von personenbezogenen Daten in KI-Systemen herangezogen werden kann und ob Informationspflichten gegenüber betroffenen Personen bestehen. Daneben fehlt es häufig an dem Wissen, wie stark KI-Systeme in Entscheidungsprozesse eingebunden werden dürfen und dass das Verbot der automatisierten Einzelentscheidung nach Art. 22 DSGVO hier häufig eine Grenze darstellen wird.

In der Praxis kann es daher sinnvoll sein, insbesondere diese Punkte noch einmal in einer speziellen Datenschutzschulung zu behandeln.

Rechtsgrundlage und Informationspflichten

KI-Systeme mit allgemeinem Verwendungszweck bringen es mit sich, dass die Beschäftigten häufig selbst das Vorliegen einer Rechtsgrundlage prüfen müssen. Denn anders als bei KI-Systemen mit einem bestimmten Verwendungszweck, kann die Organisation hier nicht im Vorfeld die Rahmenbedingungen für jedes Anwendungsszenario vorgeben. Stellt die Organisation den Beschäftigten zum Beispiel eine Funktion zur Verfügung, die nur einem Zweck dient (etwa die KI-Transkription von Videokonferenzen), so kann die Organisation hier im Vorfeld eine ganze Reihe an Maßnahmen treffen. Zum Beispiel könnten die Einladungslinks zur Videokonferenz so gestaltet werden, dass bereits auf die Möglichkeit der KI-Transkription inklusive der Nutzungszwecke und der Speicherdauer hingewiesen wird. Es könnte zudem ein Mechanismus eingerichtet werden, der die KI-Transkription bei Aktivierung anzeigt bzw. aktiv die Einwilligung aller Teilnehmenden erfordert. Die Organisation hat es bei KI-Systemen mit einem bestimmten Verwendungszweck also in der Hand, über die Rechtsgrundlage (bei KI-Transkription zum Beispiel Interessenabwägung oder Einwilligung) zu entscheiden und die weiteren Maßnahmen zu treffen, die datenschutzrechtlich erforderlich sind.

Bei KI-Systemen mit allgemeinem Verwendungszweck ist das schon schwieriger – hier sind die Beschäftigten datenschutzrechtlich mehr gefordert. Am Beispiel von KI-Chatsystemen wird es dabei besonders wichtig, die Beschäftigten zu sensibilisieren, dass eine Eingabe, die zu einer Zweckänderung führt, grundsätzlich vermieden werden muss bzw. neue Pflichten (Prüfung einer neuen Rechtsgrundlage und Informationspflichten) auslöst. Auf der anderen Seite wird es häufig erforderlich sein, den Nutzern die Angst zu nehmen, dass jede Eingabe von personenbezogenen Daten neue, eigenständige Informationspflichten auslöst und komplexe rechtliche Prüfungen erforderlich macht.

Hierzu könnten im Rahmen von Schulungen zum Beispiel folgende Fälle verwendet werden:

- Wenn die Rahmenbedingungen stimmen, darf KI eigentlich fast immer für die Übersetzung von Texten (auch personenbezogenen Texten) verwendet werden, sofern dies erforderlich ist, um den Zweck, der bei der ursprünglichen rechtmäßigen Erhebung vorlag, erfüllen zu können. Hier wird die ursprüngliche Rechtsgrundlage in der Regel nur weitergeführt und es ist keine separate (neue) Information der betroffenen Person erforderlich.

- Die Nutzung von personenbezogenen Daten einer Person innerhalb eines KI-Systems stellt hingegen meistens dann eine Zweckänderung dar, wenn diese herangezogen werden sollen, um den Fall einer anderen Person besser bearbeiten zu können. Es wäre also eine Zweckänderung, würde man den Kommunikationsverlauf von Person A in eine Wissensdatenbank oder einen Chatverlauf eingeben, um ähnliche Anfragen anderer Personen in Zukunft besser beantworten zu können.

Automatisierte Einzelentscheidung

Besonders wichtig ist es in der Praxis auch, dass die Beschäftigten noch einmal über das Verbot der automatisierten Einzelentscheidung gemäß Art. 22 DSGVO sensibilisiert werden. Häufig ist dieses Verbot vielen Beschäftigten nämlich gar nicht bekannt und der Einsatz von KI-Chatsystemen liefert vermeintlich schnell die richtigen Entscheidungen. Auch hier kann in Schulungen mit Beispielen gearbeitet werden. Dabei muss auch klar werden, welche Ausnahmen gelten und dass die Datenschutzaufsichtsbehörden hohe Anforderungen an den Grad der menschlichen Beteiligung stellen, sodass ein reines Abnicken von KI-Vorschlägen kein ausreichender Beteiligungsgrad ist. Im Hinblick auf die Datenrichtigkeit kann zudem noch einmal darauf hingewiesen werden, dass KI-Systeme häufig halluzinieren.

Eine Personalabteilung, die ein KI-Chatsystem nutzt, um Bewerberlisten hochzuladen und die KI um eine Entscheidung bittet, welchen Personen abgesagt und welche eingeladen werden sollen, wäre hier ein gutes Negativbeispiel für eine automatisierte Einzelentscheidung. In diesem Fall wäre über die DSGVO hinaus auch noch die KI-Verordnung relevant (Vorliegen eines Hochrisiko-KI-Systems nach Anhang III Ziffer 4 lit. a KI-VO). Die Anforderungen der KI-VO bilden neben den Anforderungen der DSGVO darüber hinaus insgesamt Raum für eine eigene Schulung. In der Praxis kann es sinnvoll sein, die Schulungen zu trennen und Schwerpunkte zu setzen, um die Teilnehmenden nicht zu überfrachten.

Kurznotiz

Faxverbot in katholischen Einrichtungen

Mit der Novellierung des KDG und der KDG-DVO gilt seit § 25 Satz 1 KDG-DVO ein grundsätzliches Verbot der Datenübermittlung per Fax. Ausschlaggebend sind zwei Risikofaktoren: die fehlende Verschlüsselung bei der heute üblichen IP-basierten Faxübertragung sowie die Gefahr von Anwendungsfehlern durch falsche Zielnummerneingabe.

Angesichts der fortschreitenden Anbindung von Gesundheitseinrichtungen, Apotheken und Pflegeeinrichtungen an die Telematikinfrastruktur bietet KIM (Kommunikation im Medizinwesen) einen geeigneten, datenschutzkonformen Übertragungsweg. Die Migration ist jedoch noch nicht überall abgeschlossen.

Für diesen Übergangszeitraum eröffnet § 25 Satz 2 KDG-DVO die Möglichkeit, für konkrete Einzelfälle befristete Ausnahmeregelungen zu dokumentieren, in denen ein Faxverzicht operativ noch nicht umsetzbar ist.

Eine detaillierte Aufbereitung des Themas – einschließlich Handlungsempfehlungen zur rechtssicheren Dokumentation von Ausnahmen – folgt in der nächsten Ausgabe.

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. 1.800 Seiten Inhalt
- ISBN: 978-3-553-43000-5
- Preis **195,00 €** inkl. MwSt.
- Uneingeschränkter Online-Zugriff
  inkl. 3-4 kostenpflichtige Nachtragslieferungen
  pro Jahr zum Preis von jeweils **89,90 €** inkl. MwSt.
  und versandkostenfreier Zusendung im Inland.

Hier bestellen!

AOK Medien

© AOK-Medien GmbH | Lilienthalstraße 1-3 | 53424 Remagen | Tel 02642 931-0 | Fax 02642 931-130 | Mail: fachinfo@aok-medien.de | Web: http://www.aok-medien.info | Herausgeber: AOK-Medien GmbH, Remagen | Geschäftsführung: Frank Schmidt, Thomas Reiner | 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-Medien GmbH, KI-generiert | 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.