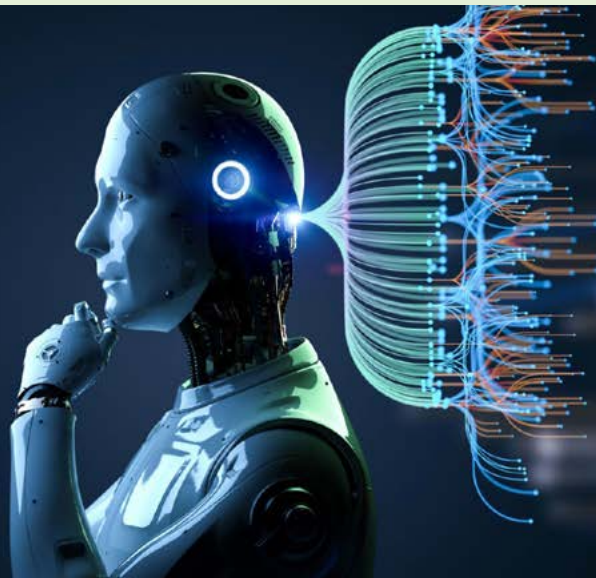


Inhalt

- 01 Künstliche Intelligenz
- 05 Ehegattennotvertretungsrecht



Künstliche Intelligenz

Seit dem Jahreswechsel nimmt das Thema Künstliche Intelligenz rasant an Fahrt auf. Insbesondere ChatBots, wie ChatGPT oder Anwendungen zur Bilderzeugung, wie Midjourney, haben dabei besondere Aufmerksamkeit erfahren. Doch was steckt dahinter, was kommt vielleicht noch und wie steht es um den Datenschutz?

Sven Venzke-Caprarese

Wirklich intelligent?

Schon der Begriff „Künstliche Intelligenz“ lädt zum Diskutieren ein. Sind Anwendungen wirklich intelligent? Vermutlich nicht, denn tatsächlich handelt es sich bei den bisherigen Anwendungen eher um das Ergebnis sogenannter Deep-Learning-Algorithmen. ChatGPT wird dabei beispielsweise als Large Language

Model bezeichnet und wurde mit einer Vielzahl von Daten trainiert. Dies ermöglicht es der Anwendung, Muster und Wahrscheinlichkeiten von Texten zu erkennen bzw. vorherzusagen und darauf aufbauend zu kommunizieren. Eine „echte“ nachdenkende Intelligenz ist das wohl nicht, allerdings sind die Ergebnisse mehr als beeindruckend. Das gleiche

gilt eigentlich auch für alle anderen KI-Anwendungen. Midjourney etwa wurde mit einer Vielzahl von Bildern trainiert und kann nun anhand von Textbeschreibungen fotorealistische Bilder erzeugen. Und auch in der Radiologie wird schon seit längerem versucht, Deep-Learning-Modelle im Rahmen der Diagnostikunterstützung einzusetzen.

Wahrheitsgehalt

Bei der Nutzung von aktuellen KI-Anwendungen ist schon aus einem ganz praktischen Grund Vorsicht geboten, denn auch, wenn die Ergebnisse auf den ersten Blick beeindruckend, müssen sie nicht richtig sein. Ein gutes Beispiel ist ChatGPT. Dieser „verkauft“ seine Antworten auf bestimmte Fragen durchaus glaubwürdig und gibt auf Nachfrage meistens auch Quellen an. Richtig ist die Antwort aber nicht unbedingt. Fragt man ChatGPT etwa nach den datenschutzrechtlichen Voraussetzungen zum Einsatz von Google Analytics ist vom Einwilligungserfordernis des § 25 TTDSG nichts zu lesen. Dies mag zum einen daran liegen, dass die Trainingsdaten von ChatGPT vor dem Inkrafttreten des TTDSG erstellt wurden. Zum anderen „phantasiert“ der ChatBot gelegentlich gerne.

Bilderzeugende Anwendungen sind da schon ein ganzes Stück weiter. Hier kann kaum noch ein echtes von einem generierten Bild unterschieden werden. Ein Bild, das durch die Presse ging, verdeutlicht die damit zusammenhängenden Herausforderungen gut: War der Papst wirklich in der Jacke eines Luxusmarkenherstellers unterwegs? Nein, das Bild wurde mithilfe von Midjourney erzeugt. Wirklich erkennen konnte man den Unterschied zu einem echten Foto aber nicht.

Diskriminierung

Eine weitere Herausforderung stellt der Umstand dar, dass es so scheint, als würden KI-Modelle zu Diskriminierung neigen. Erklärbar ist dies unter Umständen mit den verwendeten Trainingsdaten, die möglicherweise ebenfalls diskriminierende Inhalte enthielten. Anbieter von KI-Anwendungen versuchen daher teil-

weise Filter über die KI-Anwendung zu legen, um diskriminierende Antworten zu unterdrücken.

Automatisierte Einzelentscheidung

Der Einsatz von Künstlicher Intelligenz wirft auch datenschutzrechtlich eine ganze Reihe an Grundsatzfragen auf.

So muss zum Beispiel beachtet werden, dass es nach Art. 22 DS-GVO verboten ist, eine ausschließlich automatisierte Entscheidung zu treffen, die gegenüber der betroffenen Person eine rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Dies wird in der Praxis insbesondere dort zu beachten sein, wo der Einsatz von ChatBots für die Kundenkommunikation vorgesehen ist oder für Auswertungen mit Hilfe von auto-

matisierten Entscheidungsprozessen. Eine rein KI-gestützte Ablehnung eines Bewerbers dürfte zum Beispiel ebenfalls gegen Art. 22 DS-GVO verstoßen.

Weitergabe an Dritte und zweckfremde Nutzung

Je nach KI-Anwendung treten weitere Herausforderungen hinzu. Insbesondere ChatGPT ist in der Vergangenheit in die Kritik geraten, weil die eingegebenen Daten dort vermutlich vom Anbieter OpenAI für weitere Trainingszwecke gespeichert bzw. weiterverwendet wurden. Ohne Rechtsgrundlage wäre dies rechtswidrig, was auch schon die Übermittlung von personenbezogenen Daten Dritter an den Diensteanbieter einschließen würde. Problematisiert werden könnte an dieser Stelle ebenfalls, dass Daten in die USA übertragen werden.



Insgesamt wären für den Einsatz von ChatGPT in Unternehmen also noch eine Reihe von Voraussetzungen zu klären, wie z. B.:

- Erfordernis eines Vertrags zur Auftragsverarbeitung
- Herstellung eines angemessenen Datenschutzniveaus, da der Anbieter die Daten in einem unsicheren Drittstaat verarbeitet
- Sofern die eingegebenen Daten auch zu eigenen Zwecken des Diensteanbieters genutzt werden, wäre der Einsatz nur mit einer diesbezüglichen Einwilligung der Nutzer möglich

Eine in Zukunft denkbare Alternative könnte aber auch der Betrieb einer KI-Anwendung wie ChatGPT auf eigener Hardware sein.

So gibt es bereits die ersten Anwendungen, die ähnlich wie ChatGPT aufgebaut sind und die auf normalen Rechnern laufen. Insbesondere auch aufgrund der Hardwareanforderungen ist die Qualität von Anwendungen, die auf normalen Rechnern installiert werden können, aber noch nicht vergleich-

bar mit der Leistung von ChatGPT. Wenn es in Zukunft jedoch weitere Open Source Modelle gibt, die auch für den Betrieb auf eigenen Servern oder in Rechenzentren ausgelegt sind, könnte sich dies ändern. Die Daten würden dann nicht mehr von Dritten zweckfremd genutzt werden können und man könnte der Anwendung dann wohl auch verbieten, die neu eingegebenen Daten für weitere Trainingszwecke zu nutzen.

Verwendung von Trainingsdaten

Eine weitere komplexe Frage ist die rechtliche Einordnung der Trainingsdaten. Wurden Trainingsdaten genutzt, die personenbezogene Daten enthielten? Lag hierfür die entsprechende Rechtsgrundlage vor? Wirkt es sich auf die Nutzung der trainierten Anwendung aus, wenn die ursprünglichen Trainingsdaten rechtswidrig genutzt wurden und bis zu welchem Punkt würde eine solche Rechtswidrigkeit durchgreifen?

Diese Fragen scheinen derzeit noch ungeklärt zu sein und berühren neben datenschutzrechtlichen

auch urheberrechtliche Aspekte. So weist der deutsche Berufsverband für Fotografen darauf hin, dass Deep-Learning-Algorithmen die Werke von Urhebern nutzen, um die KI anzulernen und dann neue Bilder zu erzeugen und zu vermarkten. Wirkt sich dies auch auf die Ergebnisse aus? An dieser Stelle wird rechtlich noch vieles diskutiert werden müssen.

Datenschutzinformation

Insgesamt gilt auch beim Einsatz von KI-Anwendungen, dass die betroffene Person vor einer erstmaligen Datenerhebung nach Art. 13 DS-GVO über die Datenerhebung und die geplante Verarbeitung informiert werden muss. Dies scheint auf den ersten Blick grundsätzlich auch gut möglich zu sein. Allerdings bleibt hier abzuwarten, welche Anforderungen Datenschutzaufsichtsbehörden an eine entsprechende Information stellen werden.

Bereits im Jahr 2019 haben die Datenschutzaufsichtsbehörden im Zusammenhang mit KI-Anwendungen die sogenannte „Hambacher Erklärung zur Künstlichen Intelligenz“ verfasst, welche eine Reihe



von datenschutzrechtlichen Anforderungen aufstellt. In Bezug auf die Transparenz der Datenverarbeitung heißt es dort u. a.: „Entscheidungen, die auf Grundlage des Einsatzes von KI-Systemen erfolgen, müssen nachvollziehbar und erklärbar sein. Es genügt nicht die Erklärbarkeit im Hinblick auf das Ergebnis, darüber hinaus muss die Nachvollziehbarkeit im Hinblick auf die Prozesse und das Zustandekommen von Entscheidungen gewährleistet sein. Nach der DS-GVO ist dafür auch über die involvierte Logik ausreichend aufzuklären.“

Insbesondere diese Anforderung der Aufsichtsbehörden scheint in der Praxis aber kaum umsetzbar zu sein, da es auf Grund der komplexen Strukturen von KI-Anwendungen wahrscheinlich kaum gelingen wird, konkret darüber Rechenschaft abzulegen, welche Prozesse innerhalb der Anwendung zu einem bestimmten Ergebnis führten.

Auch hier ist datenschutzrechtlich also noch einiges zu klären.

Datenschutz-Folgenabschätzung

Vor dem Einsatz von KI-Anwendungen zur Verarbeitung von personenbezogenen Daten sollte immer geprüft werden, ob eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO erforderlich ist.

In diesem Rahmen können auch die „Leitlinien zur Datenschutz-Folgenabschätzung“ der Datenschutzgruppe nach Art. 29 eine Rolle spielen. Diese finden sich im Working-Paper 248 Rev. 1 und weisen unter anderem darauf hin, dass die „Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen“ ein

Kriterium für das Erfordernis einer Datenschutz-Folgenabschätzung darstellen kann.

Auch die verschiedenen Listen, die von Aufsichtsbehörden gem. Art. 35 Abs. 4 DS-GVO erstellt wurden und die bestimmen, wann eine Datenschutz-Folgenabschätzung erforderlich ist, enthalten häufig den Einsatz Künstlicher Intelligenz. So ist ein häufig auffindbares Beispiel etwa der „Einsatz von Künstlicher Intelligenz zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den Betroffenen oder zur Bewertung persönlicher Aspekte der betroffenen Person“.

Verbreitung von KI-Anwendungen

Die meisten der verfügbaren modernen KI-Anwendungen stehen einer breiten Öffentlichkeit eigentlich erst seit Ende 2022 zur Verfügung. Dabei ist aber festzustellen, dass die Entwicklung rasant voranschreitet und die Funktionen von Monat zu Monat beeindruckender werden. Ob sich diese Geschwindigkeit der Entwicklung halten lässt, mag zwar bezweifelt werden. Allerdings scheint es die Tendenz zu geben, dass immer mehr Software-Anbieter darüber nachdenken, KI-Funktionen in ihre bestehenden Anwendungen zu implementieren. Webbrowser wie Bing von Microsoft stellen schon heute ChatGPT-Funktionen bereit. Auch im Zusammenhang mit der Entwicklung von Betriebssystemen scheint sich einiges zu tun. So wird berichtet, dass Microsoft für Windows einen sog. KI-Copiloten anbieten möchte. Für Videokonferenzsysteme wird an KI-Tools gearbeitet, die automatisch ein zusammenfassendes Protokoll der Videobesprechungsergebnisse möglich machen sollen. Die Anwendungsszenarien

scheinen an dieser Stelle sehr weit und das Anbieten von KI-Funktionen innerhalb von etablierter Software wird vermutlich auch vor Kunden-, Patienten- und Personaldaten keinen Halt machen.

Hier ist es empfehlenswert, insbesondere bei Updates oder Funktionserweiterungen darauf zu achten, ob neue KI-Funktionen implementiert wurden und ob sich diese bis zu einer datenschutzrechtlichen Überprüfung auch ausschalten lassen.

Anpassung von Datenschutz- oder Informationssicherheitsrichtlinien

Unternehmen und Einrichtungen des Gesundheitswesens sollten zudem prüfen, ob die Nutzung der neuen KI-Anwendungen geregelt werden muss. Denkbar ist es beispielsweise, dass bestehende Datenschutz- oder Informationssicherheitsrichtlinien auf die neue Lage angepasst werden. Denn es wäre derzeit nicht gut, wenn Beschäftigte ungeregelt personenbezogene Kunden-, Patienten- oder Personaldaten in ChatGPT eingeben, um Antworten zu Fragen oder Datenanalysen zu erhalten. Es wäre ebenfalls nicht gut, wenn die Öffentlichkeitsabteilung unreflektiert Midjourney nutzen würde, um Fotos mit Personenabbildungen von Beschäftigten zu bearbeiten.

Fazit

Die Möglichkeiten, die KI-Anwendungen versprechen, sind nicht zu unterschätzen und werden in Zukunft vermutlich immer relevanter. Derzeit setzt der Umgang mit den entsprechenden Anwendungen im datenschutzrechtlichen Kontext aber noch ein gehöriges Maß an Fingerspitzengefühl voraus.



Ehegattennotvertretungsrecht – zusätzliche Datenerhebungen bei der Patientenaufnahme notwendig

Das Gesetz zur Reform des Vormundschafts- und Betreuungsrechts führte zum 1.1.2023 das sogenannte Ehegattennotvertretungsrecht ein. In § 1358 BGB sind verschiedene Regelungen enthalten, die die Rechte von Ehepartnern und eingetragenen Lebenspartnern in Notfallsituationen erweitern. Die Regelungen greifen, wenn ein Ehe- oder Lebenspartner infolge von Bewusstlosigkeit oder Krankheit seine Angelegenheiten der Gesundheitspflege nicht mehr selbst besorgen kann. Damit dieses Recht auch umgesetzt werden kann, müssen die Gesundheitseinrichtungen verschiedene (datenschutzrechtliche) Vorkehrungen treffen.

Dr. Sebastian Ertel

Um was geht es?

Bisher galt: Ein Ehegatte/Eingetragener Lebenspartner darf den anderen nur dann vertreten, wenn er über eine entsprechende Vorsorgevollmacht (mit Regelungen zur Gesundheitspflege) verfügt oder eine gerichtliche Bestellung zum rechtlichen Betreuer erfolgte.

Mit der Regelung des § 1358 BGB darf, wenn ein Ehegatte/Eingetragener Lebenspartner aufgrund von Bewusstlosigkeit oder Krankheit die eigenen Angelegenheiten der Gesundheitspflege rechtlich nicht besorgen kann, der andere Ehegatte/Eingetragene Lebenspartner diese für sechs Monate vertreten.

Allerdings greift dieses Recht nicht uneingeschränkt. Es gibt verschiedene Ausschlussgründe, die einer Anwendbarkeit des Ehegattennotvertretungsrechts entgegenstehen:

- Die Ehegatten/Eingetragenen Lebenspartner leben nachweislich getrennt

- Dem behandelnden Arzt ist bekannt, dass der erkrankte Ehegatte/Eingetragene Lebenspartner eine Betreuung durch den anderen ablehnt
- Es liegt bereits eine Vorsorgevollmacht vor, in der für die Gesundheitsvorsorge eine andere Person bevollmächtigt wurde
- Es liegt eine Patientenverfügung vor
- Es liegt ein Widerspruch des zu vertretenden Ehegatten/Eingetragenen Lebenspartners vor

Der sechsmonatige Zeitraum beginnt, wenn die Notsituation eintritt und diese von den behandelnden Ärzten/Ärztinnen festgestellt wurde. Der Zeitpunkt und das Vorliegen der Voraussetzungen sind zu dokumentieren.

Das Notvertretungsrecht endet mit Ablauf der sechs Monate. Bedarf es einer weitergehenden Betreuung, muss das Betreuungsgericht eingeschaltet werden.

Was hat das mit Datenschutz zu tun?

Das Notvertretungsrecht bedingt eine Überarbeitung der Prozesse in der administrativen Patientenaufnahme. Zwar wird das Recht nicht in allen Fachbereichen gleichwertig relevant sein. Ein Schwerpunkt wird sicherlich in der Geriatrie liegen. Gleichwohl sollten direkt zu Beginn der medizinischen Behandlung die erforderlichen Informationen eingeholt werden, um im Bedarfsfall handlungsfähig zu sein und schnell reagieren zu können. Im Rahmen der admi-

nistrativen Patientenaufnahme müssen daher zusätzliche Daten erhoben und verarbeitet werden.

So muss, nach der Aufklärung über das Ehegattennotvertretungsrecht, zunächst erfasst werden, ob eine Ehe oder eingetragene Lebenspartnerschaft besteht und auch noch intakt ist. Die Personalien und Kontaktdaten des Partners sind zu erheben, um diesen im Bedarfsfall schnell zu kontaktieren und eine Authentifizierung zu ermöglichen.

Anschließend ist in Erfahrung zu bringen, ob der Patient der grundsätzlichen Anwendbarkeit widerspricht. Im Fall des Widerspruchs darf das Ehegattennotvertretungsrecht nicht zum Tragen kommen. Der Widerspruch ist zu dokumentieren und es müssen keine weiteren Daten erhoben werden.

Erfolgt kein Widerspruch, ist zu erfragen, ob eine Vorsorgevollmacht oder eine Patientenverfügung besteht. Ist dies der Fall, findet das Ehegattennotvertretungsrecht keine Anwendung. Das Vorliegen entspre-

chender Dokumente ist zu dokumentieren. Weitere Daten sind nicht zu erheben.

Der Notfall tritt ein und es liegen keine Informationen vor

Problematisch wird es, wenn die erforderlichen Daten nicht vorliegen, etwa weil der Prozess zum Notvertretungsrecht noch nicht etabliert ist oder der Patient bereits in einer Notfallsituation eingeliefert wurde.

Wenn dann ein Ehe- oder eingetragener Lebenspartner in der Gesundheitseinrichtung vorstellig wird, besteht die große Herausforderung, zu bewerten, wie mit der sich darbietenden Situation umzugehen ist.

Zunächst ist zu klären, ob eine Ehe bzw. eingetragene Lebenspartnerschaft besteht und noch intakt ist. Indizien können dafür



die Heiratsurkunde und der Personalausweis (zum Abgleich der Anschrift) sein.

Indizien deshalb, weil trotz vorgelegter Heiratsurkunde die Ehe oder eingetragene Partnerschaft zwischenzeitlich wieder aufgehoben sein könnte. Oder, weil unterschiedliche Anschriften in den Unterlagen der Partner nicht automatisch ein Scheitern der Ehe bzw. Lebenspartnerschaft bedeutet.

Ferner muss geprüft werden, ob der Patient der Anwendbarkeit des Notvertretungsrechts formuliert hat. Ein solcher könnte im Zentralen Vorsorgeregister der Bundesnotarkammer hinterlegt sein. Eine Auskunft kann über www.vorsorgeregister.de/aerzte eingeholt werden.

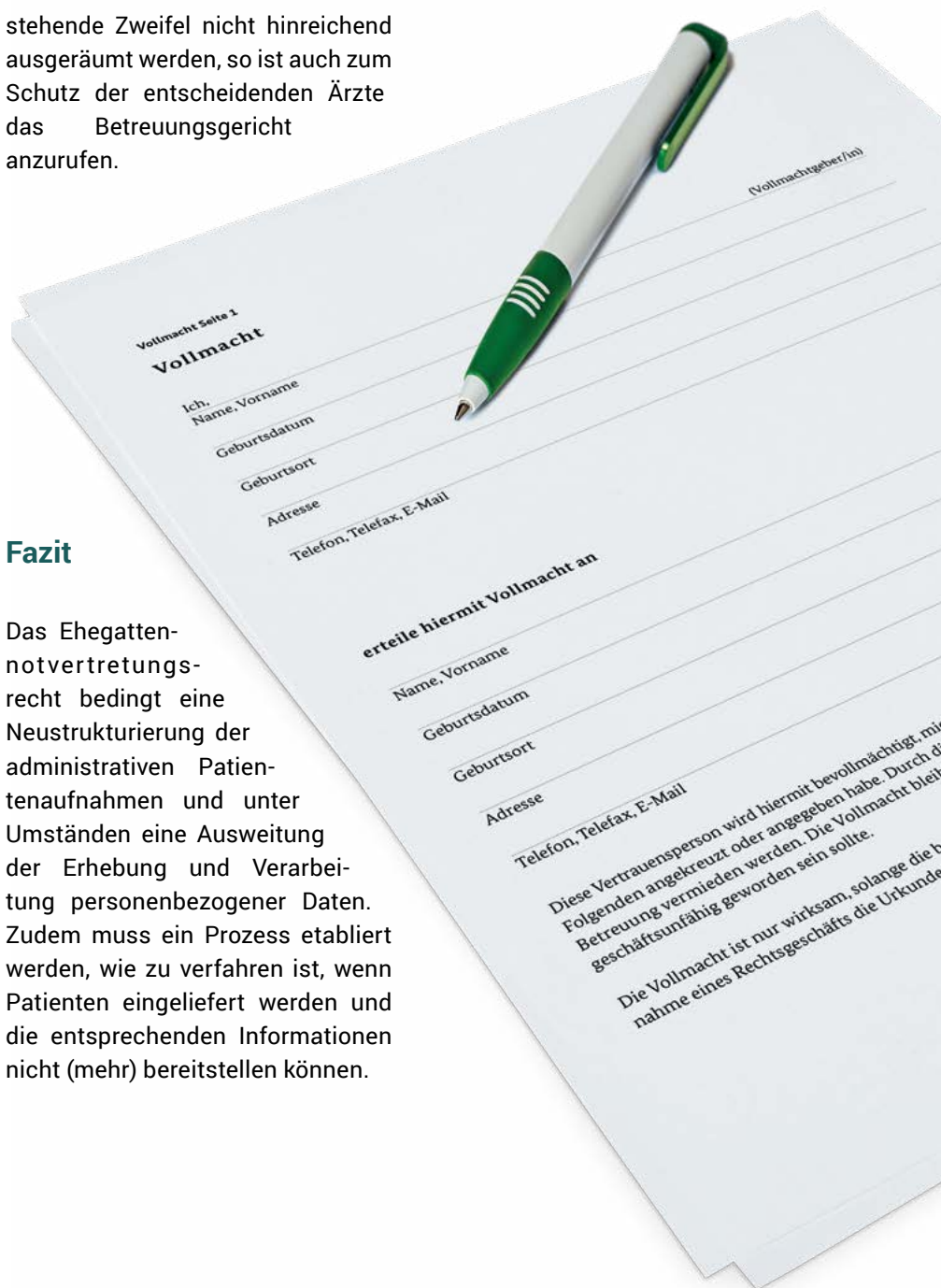
Zusätzlich kann man über das Notfalldatenmanagement, eine medizinische Fachanwendung der Telematik-Infrastruktur, und dort über den Datensatz „Persönliche Erklärungen“ von der elektronischen Gesundheitskarte auslesen, ob Hinweise auf den Aufbewahrungsort einer Patientenverfügung oder Vorsorgevollmacht hinterlegt wurden.

Können die Voraussetzungen für die Anwendbarkeit des Ehegattennotvertretungsrechts nicht eindeutig festgestellt werden oder entgegen-

stehende Zweifel nicht hinreichend ausgeräumt werden, so ist auch zum Schutz der entscheidenden Ärzte das Betreuungsgericht anzurufen.

Fazit

Das Ehegattennotvertretungsrecht bedingt eine Neustrukturierung der administrativen Patientenaufnahmen und unter Umständen eine Ausweitung der Erhebung und Verarbeitung personenbezogener Daten. Zudem muss ein Prozess etabliert werden, wie zu verfahren ist, wenn Patienten eingeliefert werden und die entsprechenden Informationen nicht (mehr) bereitstellen können.



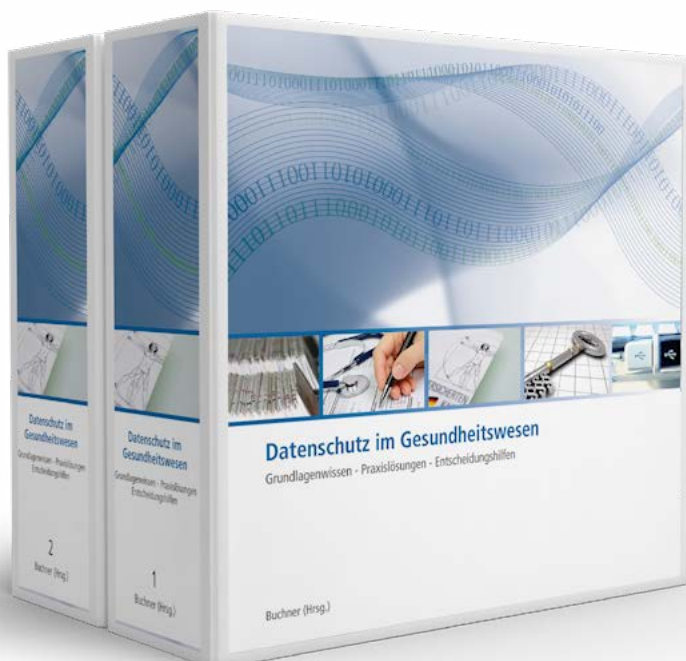
Praxishandbuch für Datenschutzbeauftragte im Gesundheitswesen

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 **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.

Interaktive eLearning-Kurse

Kaum ein Bereich im Datenschutz weist höhere Komplexität auf und stellt Verantwortliche vor größere Herausforderungen, als der rechtskonforme Umgang mit Gesundheitsdaten. Dabei handelt es sich in der Regel um hochsensible Informationen zu Erkrankungen, Diagnostik und Behandlungen von Personen, deren Bekanntwerden existenzielle Folgen für Betroffene haben kann. Folgerichtig unterliegen die Erfassung, Verarbeitung und Sicherung von Gesundheitsdaten verschärften Anforderungen, um Manipulation oder Missbrauch zu verhindern. Soweit die Theorie.

Wie steht es jedoch um die praktische Umsetzung der unzähligen datenschutzrechtlichen Vorschriften im Gesundheitswesen, deren Verletzung in konkreten Fällen mit Bußgeldern, Geld- oder sogar Freiheitsstrafen geahndet werden kann? An diesem Punkt, an dem für Datenschutzverantwortliche der Spaß ganz sicher aufhört, setzen wir mit unseren interaktiven Online-Schulungen an. Denn wie können Mitarbeitende handeln, wie sie sollen, wenn sie nicht wissen, wie sie handeln müssen?

Mit spannenden Geschichten, bildstarken Animationen und eine Prise Humor hilft privacy train Ihnen dabei, Datenschutz und Informationssicherheit spielend einfach und garantiert nachhaltig in den Arbeitsalltag aller Mitarbeitenden zu integrieren.

Unser Learning Management System bietet Ihnen dabei alle wesentlichen Funktionen von der Auswertung bis hin zur rechtskonformen Dokumentation Ihrer Schulungskampagnen.

Schulen Sie mit unserer smarten Lösung inklusive einem Training Ihrer Wahl für bis zu 100 Mitarbeitende ein Jahr lang kostenfrei. Senden Sie dazu einfach eine Nachricht mit dem Betreff „Nachhaltig schulen!“ an software@dsn-group.de.

Mitarbeitende nachhaltig schulen!

- + mitreißende Stories
- + interaktive Kurse
- + spielerischer Lernerfolg
- + Auswertung und Dokumentation
- + eigenständige Userverwaltung

1 Jahr
kostenfrei
schulen!*

www.privacy-train.de

*Das Angebot gilt für max. 100 Mitarbeitende und eine Erstregistrierung bis zum 31.08.2023. Es gelten unsere Allgemeinen Lizenzbedingungen [privacy train](#).

privacy train