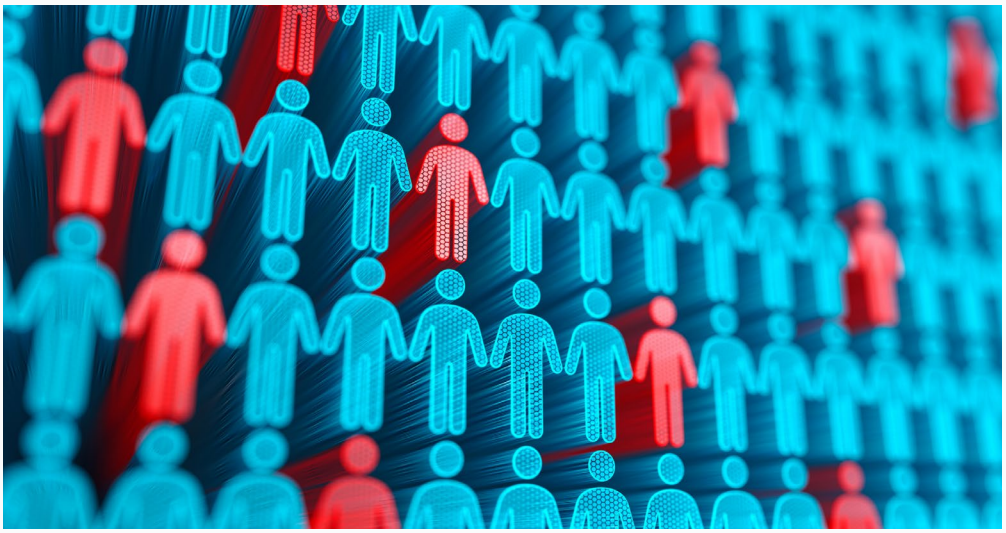
AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

Ausgabe Dezember 2020 | Seite 1

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



INHALT

SEITE 1
Corona – Verarbeitung von Beschäftigtendaten

SEITE 4
Datenschutz und Videokonferenzlösungen

SEITE 6
Kurznotiz

Corona – Verarbeitung von Beschäftigtendaten

Seit nunmehr über neun Monaten ist das Corona-Virus ein fester Bestandteil unseres Lebens. Für alle allgemein und für Beschäftigte im Gesundheitswesen ganz besonders. Nachdem im letzten Newsletter die Kontaktnachverfolgung im Mittelpunkt stand, beschäftigt sich der aktuelle Newsletter mit der Verarbeitung von Beschäftigtendaten im Zusammenhang mit dem Corona-Virus.

Dr. Sebastian Ertel

Grundsatz

Im Beschäftigungsverhältnis dürfen alle Daten eines Beschäftigten verarbeitet werden, die zur Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich sind. Wann eine solche Erforderlichkeit vorliegt, wird durch andere Gesetze oder Verordnungen bestimmt. Bestehen keine gesetzlichen Regelungen, muss im Rahmen einer Einzelfallprüfung die Erforderlichkeit ermittelt werden.

Private Kontaktdaten

Um seine Arbeitsleistung nicht mehr zur Verfügung stellen zu können, bedarf es keiner Erkrankung an Corona. Es genügt meist schon ein längerer Kontakt mit einem Corona-Erkrankten oder -Infizierten. In diesem Fällen muss sich der Beschäftigte in eine 14tägige Quarantäne begeben. Mit steigenden Infektionszahlen werden die Quarantäne-Fälle zunehmen. Hierdurch entstehen zunehmend Probleme bei der Flexibilität der Personalplanung und des Personaleinsatzes. Die schnelle und kurzfristige Erreichbarkeit der verbleibenden Beschäftigten rückt dadurch in den Fokus und damit die Frage, welche Kontaktdaten genutzt werden dürfen.

Eine freiwillig angegebene private E-Mail-Adresse kann zum Zwecke der allgemeinen Mitarbeiterinformation unproblematisch genutzt werden.

Problematisch ist die Bekanntgabe der privaten Mobilfunknummer. Das LAG Thüringen (Urt. vom 16.5.2018; Az: 6 Sa 442/17) hat diesbezüglich entschieden, dass die Bekanntgabe der Mobilfunknummer nur im Einzelfall zulässig ist: Der Mitarbeitende muss eine Schlüsselfunktion bekleiden und die telefonische Erreichbarkeit muss zwingend erforderlich sein.

Corona-WarnApp

Eine Installation auf dem privaten Gerät des Beschäftigten kann der Arbeitgeber nicht verlangen.

Für eine Installationspflicht auf einem dienstlichen Smartphone spricht die gesundheitliche Fürsorgepflicht des Arbeitgebers für weitere Beschäftigte und Geschäftspartner. Allerdings ist als Rechtsgrundlage der WarnApp laut Information der verantwortlichen Stelle (RKI) ausschließlich die Einwilligung der Nutzer erforderlich. Zudem wäre es problematisch, sofern das Handy in der Pausen- oder Freizeit ebenfalls vom Beschäftigten mitgeführt wird.

Denkbar wäre allerdings eine freiwillige Nutzung, wobei sich das Standardproblem der Freiwilligkeit im Beschäftigungsverhältnis stellt. Hier darf der Arbeitgeber also keinen Druck und auch keine Erwartungshaltung aufbauen, sondern muss es den einzelnen Beschäftigten freistellen, die App zu nutzen oder nicht.

Sofern entgegen der hier dargestellten Meinung dennoch eine verpflichtende Nutzung auf dem Diensthandy während der Dienstzeiten vorgeschrieben werden soll, müssen in jedem Fall der Datenschutzbeauftragte und – sofern vorhanden – die Mitarbeitervertretung bzw. der Betriebs- oder Personalrat eingebunden werden, da der Einsatz der App eine Maßnahme des Arbeitsschutzes nach § 3 Abs. 1 ArbSchG darstellt.

Frage nach Aufenthalten in Risikogebieten

Die Frage nach Aufenthalten in Risikogebieten sowie Kontakt zu positiv Getesteten ist von der Fürsorgepflicht des Arbeitgebers erfasst. Unter dem Aspekt der Datenminimierung wird hier regelmäßig eine Negativauskunft ausreichen.

Bekanntgabe der Identität infizierter Kollegen

Die Bekanntgabe der Identität infizierter Kollegen ist, gerade im Hinblick auf eine mögliche Stigmatisierung, grundsätzlich unzulässig. Ausreichend ist in vielen Fällen eine namenlose Warnung potentieller Kontaktpersonen sowie das Ergreifen weiterer Maßnahmen. Hierzu gehört beispielsweise die Freistellung von der Arbeit zur Umsetzung der Quarantäne.

Je nach Arbeitssituation kann im Einzelfall eine namenlose Warnung nicht ausreichend sein. Hier ist grundsätzlich eine Abstimmung mit den Gesundheitsbehörden, die zumindest in der Theorie dann die betroffenen Beschäftigten informieren, der gesetzlich vorgesehene Weg.

Gerade im Hinblick auf die steigenden Infektionszahlen und der damit verbundenen Überlastung der Gesundheitsbehörden wird man aber davon ausgehen müssen, dass eine Kontaktverfolgung durch die Gesundheitsbehörden nicht immer realisiert werden kann.

Unter diesem Aspekt kann im Einzelfall, nach sorgfältiger Abwägung unter Berücksichtigung der Belange der betroffenen Beschäftigten, der Arbeitgeber die Benachrichtigung vornehmen. In diesem Fall sollte dokumentiert werden, dass die Kontaktaufnahme

mit der Gesundheitsbehörde mehrfach erfolglos versucht wurde. Darüber hinaus ist der erkrankte Beschäftigte zeitnah zu informieren. Sofern möglich, sollte die Benachrichtigung des Mitarbeiters vorab erfolgen und der Name nur im zwingend erforderlichen Maß offengelegt werden.

Abfrage von Krankheitssymptomen

Kontrovers diskutiert wird die Zulässigkeit der Abfrage von Covid-19-spezifischen Symptomen, aber auch das Messen der Körpertemperatur. Verschiedene Aufsichtsbehörden haben sich hierzu positioniert. Nach Auffassung des Hamburgischen Datenschutzbeauftragten ist die Abfrage für die Durchführung des Beschäftigungsverhältnisses erforderlich, wenn die Besonderheiten des Arbeitsplatzes dies erforderlich machen. Dies wird insbesondere dann angenommen, wenn am Arbeitsplatz ein enger Körperkontakt nicht ausgeschlossen werden kann. Ferner in Einrichtungen wie Krankenhäusern oder bei Medizinprodukteherstellern. Allerdings gibt es auch hier eine Einschränkung bezüglich des Umfangs der Datenverarbeitung. Zulässig soll nur die Verarbeitung der Information sein, ob einem Mitarbeiter der Zutritt für einen festgelegten Zeitraum verwehrt wurde. Die Verarbeitung spezifischer Gesundheitsdaten sei hingegen weiterhin unzulässig.

Testung in Gesundheitseinrichtungen

Im Falle eines positiven Corona-Tests in einem Zeitraum von zehn Tagen in einer Gesundheitseinrichtung bestimmt § 3 der Verordnung zum Anspruch auf Testung in Bezug auf einen direkten Erregernachweis des Coronavirus SARS-CoV-2 (Coronavirus-Testverordnung), dass alle Personen, die sich in diesem Zeitraum in der Einrichtung aufgehalten haben und asymptomatisch sind, einen Anspruch auf Testung haben.

Ferner besteht ein vorbeugender Testanspruch für (zukünftige) Patienten und zu Pflegende sowie für Mitarbeitende. Bei Letzteren jedoch nur in Form eines Antigen-Tests (§ 4 Coronavirus-Testverordnung).

Die Dokumentation der Testungen und der Testergebnisse bedeutet gerade bei größeren Einrichtungen eine große Herausforderung. Kann bei Patienten oder zu Pflegenden diese problemlos in der (digitalen) Akte erfolgen, ist es bei Mitarbeitenden ungleich schwieriger. Mit einer Erfassung in Papierform oder mittels Excel-Tabelle werden schnell Grenzen erreicht. Auch kann hier nicht konsequent die Verfügbarkeit, Vertraulichkeit und Integrität der Daten gewährleistet werden. Interessengerecht erscheint hier, die Mitarbeitenden im Krankenhaus-Informations-System oder in der digitalen Pflegedokumentation anzulegen, die Ergebnisse dort zu hinterlegen und die Akte systemseitig zu versiegeln bzw. die Zugriffsrechte maximal einzuschränken.

Datenschutz und Videokonferenzlösungen

Nicht zuletzt aufgrund der Pandemie machen sich viele Gesundheitseinrichtungen Gedanken über den Einsatz von Videokonferenzlösungen. In der Praxis werden Videokonferenzen mittlerweile in vielen Situationen genutzt, z.B. für die fachliche Besprechung mit Kolleg*innen, für Bewerbungsgespräche oder für Gespräche mit Patient*innen. Insgesamt herrscht dabei aber häufig eine Unsicherheit, ob die jeweilige Lösung datenschutzrechtlich überhaupt geeignet ist.

Sven Venzke-Caprarese

Auswahl der richtigen Lösung

Bereits bei der Auswahl der richtigen Videokonferenzlösung sind im Vorfeld einige zentrale Punkte zu klären.

So kommt es u.a. auf die Frage an, welchen Schutzbedarf die Daten haben werden, die im Rahmen von Videokonferenzen ausgetauscht werden. Zudem muss geprüft werden, ob für bestimmte Bereiche spezielle Regelungen gelten, die die Auswahl von Videokonferenzlösungen und Dienstleistern einschränken. Sofern Dienstleister an der Bereitstellung beteiligt sind, müssen die entsprechenden Verträge geprüft werden und es stellt sich zudem die Frage, ob bei Dienstleistern außerhalb der EU ein angemessenes Datenschutzniveau angenommen werden kann.

Schutzbedarf

Sofern eine Gesundheitseinrichtung auf der Suche nach einer passenden Videokonferenzlösung ist, muss bereits im Vorfeld geklärt werden, welchen Schutzbedarf die Daten haben werden, die im Rahmen von Videokonferenzen besprochen werden sollen. Sofern der Schutzbedarf hoch ist oder sofern besondere Arten personenbezogener Daten ausgetauscht werden sollen, spielt die Sicherheit der Videokonferenzlösung eine entsprechend hohe Rolle. Grundsätzlich empfiehlt das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Falle eines hohen Schutzbedarfs den Einsatz einer Lösung, die über eine Ende-zu-Ende Verschlüsselung verfügt. Da viele Anbieter in der Praxis eine solche Funktion aber leider noch nicht anbieten, stellt das BSI auch Alternativen dar. So könne selbst bei hohem Schutzbedarf eine Videokonferenzlösung zum Einsatz kommen, die nicht über eine Ende-zu-Ende-Verschlüsselung verfügt. In diesen Fällen ist aber eine Transportverschlüsselung notwendig. Zudem muss beachtet werden, dass laut BSI *„Verschlüsselungsendpunkte bei einem Provider, insbesondere einem Cloud-Provider, [...] vermieden werden [sollten]“.*

Im Ergebnis bedeutet dies, dass bei hohem Schutzbedarf Videokonferenzlösungen genutzt werden können, die innerhalb der eigenen Infrastruktur betrieben werden, selbst wenn diese nicht über eine Ende-zu-Ende-Verschlüsselung verfügen. Hier sind z.B. Jitsi oder BigBlueButton zu nennen.

Cloud-Lösungen bzw. Software-as-a-Service-Lösungen dürfen grundsätzlich nicht zum Einsatz kommen, es

sei denn, dass diese über eine echte Ende-zu-Ende-Verschlüsselung verfügen (hier sind z.B. Zoom oder Webex zu nennen).

Spezielle Regelungen

In einigen Bereichen ist die Auswahl von Videokonferenzlösungen weiter eingeschränkt.

Sofern eine öffentliche Stelle unmittelbar Sozialdaten verarbeitet und diese Gegenstand von Videokonferenzen sein sollen, sind die Spezialregelungen des § 80 Sozialgesetzbuch (SGB X) zu beachten. Demnach ist die Einschaltung privater Dienstleister nicht ohne Weiteres möglich. Zudem ist eine Datenverarbeitung außerhalb der EU in den meisten Fällen durch § 80 SGB X von vornherein ausgeschlossen. Die gute Nachricht ist an dieser Stelle jedoch, dass Gesundheitseinrichtungen nur selten unmittelbar den Vorschriften des SGB unterliegen werden. Denn die Vorschriften der §§ 67 ff. SGB X gelten unmittelbar nur für behördliche Stellen, die in § 35 SGB I aufgeführt sind.

Weitere Spezialregelungen kommen jedoch zur Anwendung, wenn Gesundheitseinrichtungen Lösungen für Videosprechstunden suchen, um Gespräche zwischen Ärzten und Patienten zu realisieren. Hier dürfen nach Anlage 31b zum Bundesmantelvertrag-Ärzte (BMV-Ä) nur Videodienstanbieter eingesetzt werden, die neben einer wirksamen Ende-zu-Ende-Verschlüsselung auch weitere Anforderungen erfüllen und über eine bestimmte Zertifizierung verfügen müssen. Eine aktuelle Liste der zertifizierten Videoanbieter findet sich im Internet auf den Seiten der Kassenärztlichen Bundesvereinigung.

Dienstleister innerhalb der EU

Sofern nach den vorgenannten Überlegungen zum Schutzbedarf und zum Vorliegen spezieller Regelungen noch der Einsatz einer Videokonferenzlösung in Betracht kommt, die nicht selbst betrieben wird, muss mit den beteiligten Dienstleistern ein Vertrag zur Auftragsverarbeitung abgeschlossen werden. Sofern ein Zugriff des Dienstleisters auf Daten, die dem Berufsgeheimnis des § 203 StGB unterliegen, nicht ausgeschlossen werden kann, muss der entsprechende Dienstleister gem. § 203 Abs. 3 und 4 StGB als mitwirkende Person verpflichtet werden. An dieser Stelle sind also die gängigen Verträge, die Dienstleister bereitstellen, regelmäßig anzupassen. Lediglich im Fall einer wirksamen Ende-zu-Ende Verschlüsselung kann diese Anforderung entfallen. Allerdings muss bewertet werden, ob die Metadaten der Kommunikation (wer spricht mit wem) ggf. ebenfalls unter das Berufsgeheimnis fallen.

Dienstleister außerhalb der EU

Sofern Dienstleister außerhalb der EU eingesetzt werden sollen oder ein Zugriff von Dienstleistern außerhalb der EU nicht ausgeschlossen werden kann, muss unabhängig vom Schutzbedarf der Daten und zusätzlich zu Verträgen zur Auftragsverarbeitung dafür gesorgt werden, dass ein angemessenes Datenschutzniveau hergestellt wird.

Sofern ein Angemessenheitsbeschluss der EU für alle beteiligten Länder vorliegt, kann von einem angemessenen Datenschutzniveau ausgegangen werden. Allerdings müssen hier auch die Länder bewertet werden, in denen etwaige Unterauftragnehmer ihren Sitz haben bzw. Daten verarbeiten.

Lange Zeit war das angemessene Datenschutzniveau auch für Länder ohne Angemessenheitsbeschluss kaum ein Problem, da entsprechende Instrumente in Form von Privacy-Shield Zertifizierungen oder EU-Standardvertragsklauseln zur Verfügung standen, mit denen ein angemessenes Datenschutzniveau hergestellt werden konnte. Mit dem Urteil des Europäischen Gerichtshof vom 16. Juli 2020 zum EU-U.S. Privacy Shield (C-311/18) stehen diese Instrumente aber nicht mehr in gewohnter Wirksamkeit zur Verfügung. So erklärte der EuGH das EU-U.S. Privacy Shield für unwirksam und auch die EU-Standardvertragsklauseln werden nach dem Urteil in vielen Ländern nicht mehr ohne Weiteres ausreichen. Insbesondere für Dienstleister in den USA hat der EuGH ausdrücklich festgestellt, dass die Standardvertragsklauseln allein kein angemessenes Datenschutzniveau mehr herstellen. Im Ergebnis bedeutet dies, dass insbesondere der Einsatz von US-Dienstleistern grundsätzlich kaum noch möglich sein wird. Das Problem besteht dabei selbst dann, wenn US-Dienstleister die Datenverarbeitung zwar in europäischen

Rechenzentren vornehmen, jedoch weiterhin auf die Daten zugreifen könnten.

Die Lösung könnte an dieser Stelle wieder eine wirksame Ende-zu-Ende-Verschlüsselung bringen, die neben dem Abschluss der EU-Standardvertragsklauseln als weitere Maßnahme für ein angemessenes Datenschutzniveau sorgen kann. Dabei ist es aber wichtig, dass der Dienstleister nicht über die entsprechenden Schlüssel verfügt, mit denen der Datenstrom entschlüsselt werden kann. Es bliebe dann noch ein Risiko im Hinblick auf die Metadaten der Kommunikation, die nicht von der Ende-zu-Ende-Verschlüsselung erfasst sein werden. Vermutlich werden diese Metadaten aber nur in seltenen Fällen noch ein Problem im Hinblick auf die Angemessenheit des Datenschutzniveaus darstellen.

Ergebnis

Unabhängig vom Schutzbedarf dürfen US-Dienstleister oder Dienstleister aus Ländern ohne angemessenem Datenschutzniveau nur eingesetzt werden, wenn eine wirksame Ende-zu-Ende-Verschlüsselung genutzt werden kann, Verträge zur Auftragsverarbeitung vorliegen und Standardvertragsklauseln abgeschlossen werden.

Ansonsten müssen Dienstleiser in der EU bzw. in Ländern mit angemessenem Datenschutzniveau gewählt werden. Sofern Daten mit hohem Schutzbedarf ausgetauscht werden, scheiden jedoch auch hier Cloud- bzw. Software-as-a-Service-Lösungen ohne Ende-zu-Ende Verschlüsselung aus. Gesundheitseinrichtungen müssen die Videokonferenzlösung dann grundsätzlich innerhalb der eigenen Infrastruktur betreiben (ggf. unter Einschaltung von klassischen Hosting-Dienstleistern).

Noch eingeschränkter ist die Auswahl, wenn Videosprechstunden durchgeführt werden sollen. Hier muss auf eine Liste zertifizierter Videokonferenzlösungen zurückgegriffen werden.

Kurznotiz:

Gesetzesentwurf zur (weiteren) Digitalisierung im Gesundheitswesen

Nicht nur in Schulen ist das Thema Digitalisierung hochaktuell. Auch im medizinischen Bereich gewinnt das Thema zunehmend Bedeutung. Das Gesundheitsministerium hat am 15.11.2020 einen Entwurf für ein „Digitale Versorgung und Pflege - Modernisierungs-Gesetz“ (DVPMG) vorgelegt.

Dieses regelt unter anderem, dass das Ministerium eine Datenschutz-Folgeabschätzung, also eine Risikoanalyse, für die Telematikinfrastruktur erstellt. Durch die Telematikinfrastruktur sollen Ärzt*innen, Therapeut*innen, Kliniken bzw. Krankenhäuser, Apotheken und Krankenkassen vernetzt werden. Zudem soll hierdurch eine schnelle und sichere Kommunikationsmöglichkeit geschaffen werden, über die medizinische Informationen, die für eine schnelle und effektive Behandlung benötigt werden, verfügbar gemacht werden können. Ziel ist es, das medizinische Personal durch die Bereitstellung der entsprechenden Telematikinfrastruktur zu entlasten. Hierdurch sollen die Ärzt*innen und Pfleger*innen mehr zeitliche Kapazitäten für die Heilbehandlung haben. Nebenbei wird von einem Einsparpotential in Höhe von 800 Millionen Euro ausgegangen.

Auch die „Kommunikation im Medizinwesen“ (KIM) als sicheres Übermittlungsverfahren soll erweitert werden. KIM soll es Gesundheitseinrichtungen ermöglichen, medizinische Dokumente elektronisch und sicher über die Telematikinfrastruktur zu versenden und zu empfangen. Bislang erschöpft sich die Kommunikation auf das Versenden und Empfangen von E-Mails. Geplant ist eine Erweiterung um einen Messenger- und einen Videokommunikationsdienst.

Ob und in welcher Form der Gesetzesentwurf in Kraft treten wird, ist noch nicht abzusehen. Der Entwurf steht ganz am Anfang eines Gesetzgebungsverfahrens, sollte aber aufmerksam beobachtet werden.

© 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 | Geschäftsführer: 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

Datenschutz in der Pflege

Der rechtskonforme Umgang mit sensiblen Daten ist unverzichtbare Voraussetzung für einen vertrauensvollen und selbstbestimmten Pflegeprozess. Jedoch sind gerade im Pflegebereich die rechtlichen Vorgaben zum Datenschutz seit jeher besonders vielgestaltig und mit Geltung der europäischen Datenschutz-Grundverordnung (DS-GVO) nochmals komplexer geworden. Dies gilt vor allem für das teils nur schwer durchschaubare Zusammenspiel der europäischen Verordnung mit dem nationalen Datenschutzrecht. Besonders zu berücksichtigen sind im Pflegebereich zudem auch sozialrechtliche Vorgaben, die ordnungsrechtlichen Regelungen der Landesheimgesetze und schließlich auch die Grundsätze der ärztlichen Schweigepflicht. So bedeutet es oftmals eine ganz erhebliche Herausforderung, all diese vielfältigen und mitunter sehr detaillierten rechtlichen Anforderungen im Pflegealltag rechtssicher und praktikabel umzusetzen.

Die Broschüre soll dabei helfen, diese Herausforderung erfolgreich zu meistern und die Anforderungen eines rechtssicheren Datenschutzes und verantwortungsvoller Pflege so gut wie möglich in Einklang zu bringen.

Als Arbeitshilfe im Alltag weist sie passgenau für den Pflegebereich den Weg durch das Dickicht des Datenschutzrechts und zeigt praxisnahe Lösungsansätze auf.

Broschüre HIER bestellen

Broschüre DIN A5, ca. 264 Seiten
Preis: 49,80 € pro Stück inkl. MwSt. und versandkostenfreier Zusendung im Inland
Art. Nr.: 43111 | **ISBN: 978-3-553-43111-8**

Aus dem Inhalt (Auszug):

- **A – Datenschutz in der Pflege: Die rechtlichen Grundlagen**
  Konkrete Vorgaben für die Datenverarbeitung in der Pflege
- **B – Datenschutzorganisation**
  Praktische Umsetzung der DS-GVO in Gesundheitseinrichtungen durch den Datenschutzbeauftragten
- **C – Der Internetauftritt**
  Internetauftritt und Social Media-Plattformen rechtssicher ausgestalten
- **D – IT-Sicherheit**
  Schutzziele der Datenverarbeitung
- **E – Corona-Update**
  Datenschutz in Pandemie-Zeiten

AOK-Verlag GmbH | Lilienthalstraße 1-3 | 53424 Remagen | Tel 02642 931-333 | Fax 02642 931-215 | Mail fachinfo@aok-verlag.de
Jetzt Broschüre bestellen unter: aok-verlag.info/de/datenschutz-in-der-pflege/1/