AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

Ausgabe Dezember 2019 | Seite 1

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

INHALT

Aufsichtsbehörden stellen neues Bußgeldmodell vor

Die Datenschutz-Grundverordnung hat Aufsichtsbehörden einen großen Spielraum bei der Verhängung von Bußgeldern gegeben. Nach Art. 83 DS-GVO sind Bußgelder von 2 bis 4 Prozent des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs möglich. Um die künftige Verhängung von Bußgeldern bundesweit zu harmonisieren, hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) am 14.10.2019 ein Konzept zur Bußgeldzumessung in Verfahren gegen Unternehmen veröffentlicht. Dieser Beitrag setzt sich mit dem Konzept kritisch auseinander.

Sven Venzke-Caprarese

Das Konzept

Das Bußgeldkonzept der DSK geht von fünf Schritten aus:

Zuerst wird eine Kategorisierung der Unternehmen nach Größenklassen vorgenommen. Hierbei werden auf Grundlage von verschiedenen Jahresumsatzreichweiten Unternehmenskategorien gebildet. Unternehmen mit einem Jahresumsatz von bis zu 700.000 Euro fallen etwa in Kategorie A.I, Unternehmen mit einem Jahresumsatz von 100 bis 200 Millionen Euro in Kategorie D.III. Anhand dieser Kategorien wird in einem zweiten Schritt ein mittlerer Jahresumsatz gebildet. Dieser beträgt in Kategorie A.I 350.000 Euro und in Kategorie D.III 150 Millionen Euro.

Danach wird auf Grundlage des mittleren Jahresumsatzes ein wirtschaftlicher Grundwert ermittelt. Hierbei handelt es

sich dann um eine Art Tagessatz. In Kategorie A.I beträgt der Tagessatz z.B. 972 Euro und in Kategorie D.III bereits 416.667 Euro.

Im vierten Schritt wird der errechnete Tagessatz mit dem Schweregrad der Ordnungswidrigkeit multipliziert. Bei leichten, formellen Verstößen gilt Faktor eins bis zwei. Für sehr schwere formelle Verstöße sogar Faktor sechs. Leichte materielle Verstöße werden noch schwerer geahndet. Hierfür gilt Faktor eins bis vier. Für sehr schwere materielle Verstöße kommt sogar Faktor 12 in Betracht. Ein leichter formeller Verstoß würde für ein Unternehmen der Kategorie D.III unter Annahme des Faktors zwei also ein Bußgeld in Höhe von knapp einer Million Euro zur Folge haben.

Im fünften Schritt kann der errechnete Betrag allerdings noch einmal von der Datenschutzaufsichtsbehörde angepasst werden. Hierbei werden auch täterbezogene Umstände sowie eine etwaig drohende Zahlungsunfähigkeit des Unternehmens berücksichtigt.

Umsatz als Ausgangswert?

Insgesamt erscheint das Konzept der DSK unausgewogen und es liegt die Befürchtung nahe, dass es zu unverhältnismäßigen Ergebnissen führen wird. So sind z.B. Umsatz und Gewinn oftmals sehr verschieden.

Facebook wies im Jahr 2018 z.B. bei einem Umsatz von 55,83 Milliarden Euro einen Jahresüberschuss von 22,11 Milliarden Euro aus. Das bedeutet, dass Facebook in der Lage war, knapp 40% des Umsatzes als Gewinn zu realisieren. Im Gegensatz dazu sieht das Ergebnis bei Gesundheitseinrichtungen oftmals schlechter aus. Ein großes börsennotiertes Klinikum wies im selben Zeitraum bei einem Umsatz von 1,23 Milliarden Euro einen Gewinn von 51,2 Millionen Euro aus. Das Klinikum war also „nur“ in der Lage, knapp 4% des Umsatzes als Gewinn zu verbuchen.

Bereits an dieser Stelle zeigt sich ein Missverhältnis des Bußgeldkonzepts. Unternehmen, die mit viel Aufwand wenig Gewinn machen, werden stark benachteiligt, sofern das Bußgeld rein umsatzbezogen berechnet wird. Gesundheitseinrichtungen stehen an dieser Stelle im Vergleich zu Technologieunternehmen wie Facebook schlecht dar.

Warum die DSK den Umsatz als allgemein entscheidendes Kriterium der Bußgeldzumessung heranzieht, bleibt fraglich. Zwar ist es richtig, dass die DS-GVO den Höchstbußgeldrahmen am Umsatz bemisst. Allerdings bedeutet dies nicht, dass auch das konkrete Bußgeld starr am Umsatz hätte ausgerichtet werden müssen.

Umsatzermittlung und funktionaler Unternehmensbegriff

Das Konzept der DSK weist eine weitere Schwäche auf. Denn es geht bei der Ermittlung des Umsatzes vom sog. „funktionalen“ Unternehmensbegriff aus. Dies wird in der Praxis vermutlich dazu führen, dass bei Unternehmensgruppen und Konzernen stets der gesamte Umsatz der Gruppe bzw. des Konzerns zu Grunde gelegt wird. Einen inneren Sachzusammenhang der Tat setzt das Konzept der DSK hierfür nicht voraus. Dies hätte aber Sinn gemacht. Denn es wäre nachvollziehbar gewesen, den Konzernumsatz zum Maßstab zu machen, sofern ein Konzern eine datenschutzwidrige Verarbeitung bewusst auf ein kleineres Tochterunternehmen auslagert, um die eigenen Risiken zu minimieren und von den Verstößen zu profitieren. Für solche Fälle hat die DS-GVO den Aufsichtsbehörden einen weiten Bußgeldrahmen gegeben, der auch vor Unternehmensgrenzen nicht Halt macht. Diese Konzernhaftung jetzt aber zum Standardfall zu machen, wird in der Praxis vermutlich in vielen Fällen zu unverhältnismäßigen Ergebnissen führen. Und dabei muss man sich ganz ehrlich auch vor Augen führen, dass trotz technischer und organisatorischer Maßnahmen die Gefährdungen für die Einhaltung des Datenschutzes nie ganz ausgeschlossen werden können. Desto mehr Menschen in einem Unternehmen arbeiten, desto höher ist das Risiko, dass eine Verletzung des Datenschutzes durch ein Fehlverhalten Einzelner entsteht. Hier nun den Konzernumsatz als Maßstab zu nehmen, erscheint nicht verhältnismäßig.

Festlegung von Faktoren

Das Konzept verweist bei der Bestimmung der Faktoren auf die Berücksichtigung des Art. 82 DS-GVO und die dort festgelegten Kriterien. Im Ergebnis nennt das Konzept als Mindestfaktor aber den Faktor eins – auch für leichte formelle Verstöße.

Es bleibt dabei offen, ob das Konzept davon ausgeht, dass bei leichten oder sehr leichten Verstößen immer mindestens ein Tagessatz als Bußgeld verhängt werden muss, oder ob die Aufsichtsbehörden auch anstelle eines Bußgelds andere Maßnahmen nach Art. 58 DS-GVO treffen können, z.B. den Verantwortlichen lediglich auf einen vermeintlichen Verstoß gegen die DS-GVO hinzuweisen und es dabei zu belassen, wenn auf diesen Hinweis angemessen reagiert wird.

Überprüfung des Einzelfalls

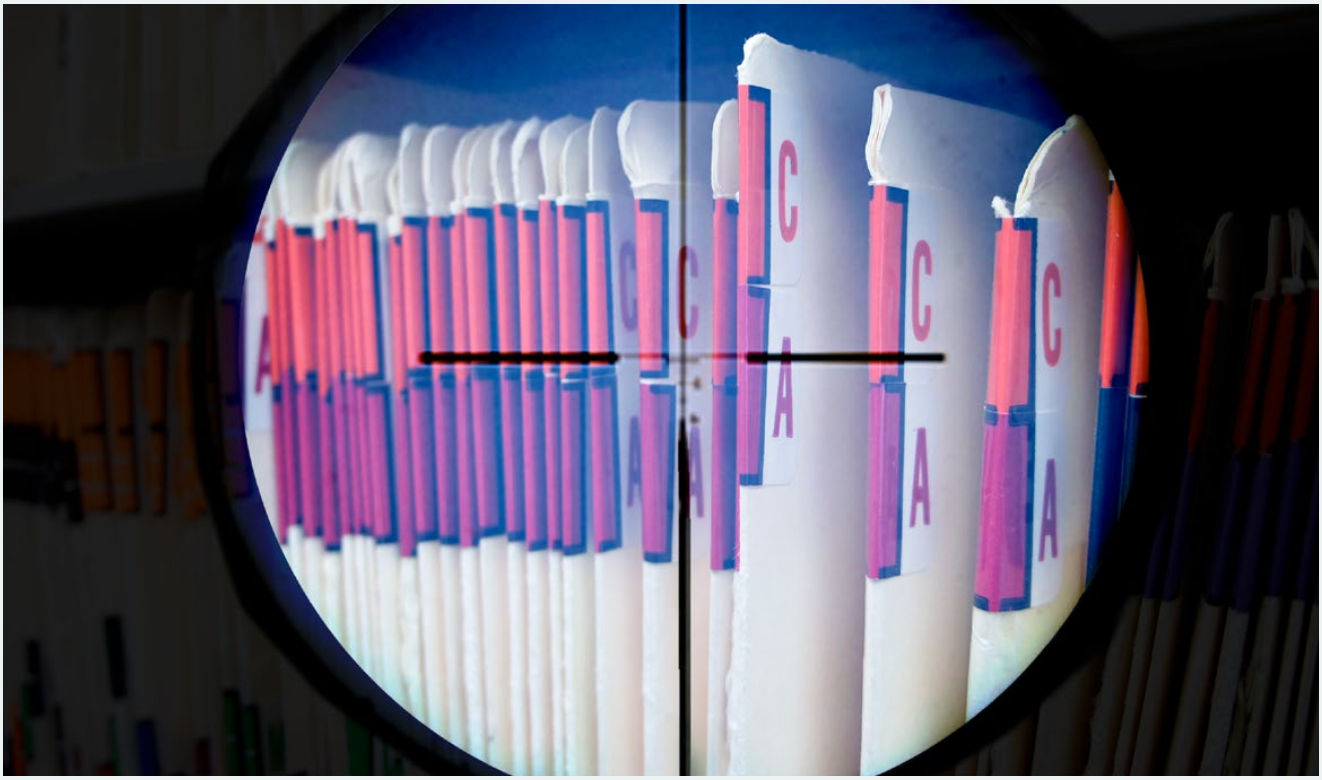
Im fünften Schritt erlaubt das Konzept die Überprüfung des ermittelten Bußgelds anhand des Einzelfalls. Allerdings erwähnt das Konzept kaum, was hierbei zu berücksichtigen ist, denn dieser Punkt erschöpft sich in der Aussage: „Der […] errechnete Betrag wird anhand aller für und gegen den Betroffenen sprechenden Umstände angepasst, soweit diese noch nicht […] berücksichtigt wurden. Hierzu zählen insbesondere sämtliche täterbezogenen Umstände (vgl. Kriterienkatalog des Art. 83 Abs. 2 DS-GVO) sowie sonstige Umstände, wie z.B. eine lange Verfahrensdauer oder eine drohende Zahlungsunfähigkeit des Unternehmens."

Fazit

Im Ergebnis ist das Konzept der DSK zur Bußgeldzumessung kritikwürdig. Denn es ist zu befürchten, dass Aufsichtsbehörden in der Praxis in vielen Fällen unverhältnismäßig hohe Bußgelder verhängen werden, die ohne angemessenen Blick auf den Einzelfall von konzernweiten Umsätzen ausgehen, ohne die wirtschaftliche Lage im Einzelfall zu berücksichtigen. Darüber hinaus nennt das Konzept kaum konkrete Punkte, die zur ggf. notwendigen Korrektur der ermittelten, hohen Grundwerte berücksichtigt werden können.

Die Berücksichtigung einer etwaig „drohenden Zahlungsunfähigkeit" wird nur ein Kriterium sein, welches die Aufsichtsbehörden bei der Beachtung des Grundsatzes der Verhältnismäßigkeit zu berücksichtigen haben werden.

Es bleibt abzuwarten, inwiefern die Aufsichtsbehörden in der Praxis von diesem Konzept Gebrauch machen werden und ob entsprechende Bußgeldzumessungen einer gerichtlichen Überprüfung im Rechtsmittelverfahren Stand halten werden.



Die Patientenakte im Visier der Ermittlungsbehörden

Verstirbt ein Patient im Krankenhaus, bleiben meist viele offene Fragen. Besteht der Verdacht einer unnatürlichen Todesursache, ist dies den Strafermittlungsbehörden zu melden, die die genaueren Umstände des Todes aufklären müssen. Dabei könnte sich der Blick in die Patientenakte des Verstorbenen als äußerst nützlich erweisen, steht doch darin, wie es um die Gesundheit des Patienten vor seinem Tod bestellt war. Aber ist das Krankenhaus überhaupt dazu befugt, zu Ermittlungszwecken Einsicht in die Patientenakte zu gewähren oder ist diese Offenlegung der Patientendaten ein Verstoß gegen das Arztgeheimnis und damit strafbar? Fakt ist, dass das Arztgeheimnis aus § 203 StGB sehr weit verstanden wird und eine Einsicht durch Dritte nur in engen Fallkonstellationen erlaubt ist.

Dr. Sebastian Ertel, Philip Kroll

Einsichtnahme aufgrund der Einwilligung des Verstorbenen

Zu denken ist zunächst an die Möglichkeit der Einsichtnahme durch die Ermittlungsbehörden aufgrund einer Einwilligung/Schweigepflichtentbindung des Patienten. Da der Patient nicht mehr unter den Lebenden weilt, kann eine solche Einwilligung – sofern die Einwilligung nicht bereits zu Lebzeiten abgegeben wurde – nur vermutet werden. Im Strafrecht spricht man dann von einer sogenannten „mutmaßlichen Einwilligung".

Man könnte nun meinen, dass beim Verstorbenen ein mutmaßliches Interesse zur Ermittlung besteht, geht es doch um ein hoheitliches Verfahren zur Aufklärung einer möglichen Straftat. Liegt jedoch eine unerkannte natürliche Todesursache vor, kann gerade kein mutmaßliches Einverständnis angenommen werden. Vielmehr würden die Ermittlungen der Polizei unter den Angehörigen nur Leid und Unverständnis auslösen. Die Frage nach der mutmaßlichen Einwilligung lässt sich somit nicht generalisiert beantworten. Das hat auch die Rechtsprechung in mehreren Entscheidungen bestätigt. So entschied das Oberlandesge-

richt Naumburg bereits im Jahr 2004 (Beschluss v. 09.12.2004 – 4 W 43/04):

> *"Bleibt der mutmaßliche Wille des Verstorbenen nach dem Versuch seiner Ermittlung zweifelhaft, liegt es in der Verantwortung des Geheimnisträgers, von den ihm bekannten Umständen auf den mutmaßlichen Willen des Verstorbenen zu schließen und nach einer gewissenhaften Prüfung über die Ausübung des Zeugnisverweigerungsrechts zu befinden."*

und

> *"Hierbei verbleibt ihm [dem Arzt; Anm. d. Verf.] ein gewisser Entscheidungsspielraum, der durch die Gerichte nur eingeschränkt auf die Überschreitung seiner Grenzen überprüfbar ist."*

Dass nach dem OLG Naumburg der Geheimnisträger (also der Arzt) selbst hier entscheiden soll, ist zugegebenermaßen überraschend. Doch so muss der Arzt diese schon unter Juristen kaum lösbare Entscheidung mit sich selbst ausmachen.

Gleichzeitig kann aber als Ergebnis festgehalten werden, dass die Ermittlungsbehörden keine rechtliche Kompetenz haben, nur aufgrund eines Verdachts und unter Bezug auf die mutmaßliche Einwilligung Einsicht in die Patientenakten zu nehmen. Die letztendliche Entscheidung obliegt dem Arzt selbst, der gut daran tut, mit der Offenbarung von Patientendaten zurückhaltend zu verfahren.

Auskunftspflichten nach den Gesetzen zur Leichenschau

Fehlt es an einer Einwilligung, könnten die Patientendaten aufgrund einer gesetzlichen Pflicht den Ermittlungsbehörden zugänglich zu machen sein. Es handelt sich ja letztlich um ein Ermittlungsverfahren zur Verfolgung von Straftaten, also die Ahndung von Verstößen gegen Recht und Ordnung, ein äußerst wichtiges Rechtsinstrument in

einem Rechtsstaat. Und wer wäre der deutsche Gesetzgeber, wenn er dies nicht bereits in den Bestattungsgesetzen zur Leichenschau geregelt hätte.

Die Leichenschau wird bereits seit dem 13. Jahrhundert durchgeführt und erfolgte dabei zunächst durch Richter und seit Mitte des vergangenen Jahrhunderts ausschließlich durch Ärzte. Dabei kann jedes Bundesland eigene Gesetze zur Leichenschau erlassen, was zwischenzeitlich zu einer verwirrenden Vielfalt von Regelungen geführt hat. Klare Einigkeit besteht darüber, dass nur der Arzt der Leichenschau über eine Meldung an die Ermittlungsbehörden entscheidet.

Doch während in Nordrhein-Westfalen jeder Anhaltspunkt von Selbsttötung, Unfall oder Einwirkung Dritter zu melden ist (§ 9 Abs. 5 BestG NRW), spricht man in Hamburg nur von Anhaltspunkten für einen nichtnatürlichen Tod (§ 2 Abs. 4 BestG HH). Dagegen wurde in Niedersachsen das Bestattungsgesetz jüngst erweitert (§ 4 Abs. 4 BestattG), um die Meldepflicht bei Anhaltspunkten, dass der Tod durch eine ärztliche […] Fehlbehandlung verursacht (Nr. 2) wurde oder auf eine außergewöhnliche Entwicklung im Verlauf der Behandlung zurückzuführen ist (Nr. 3).

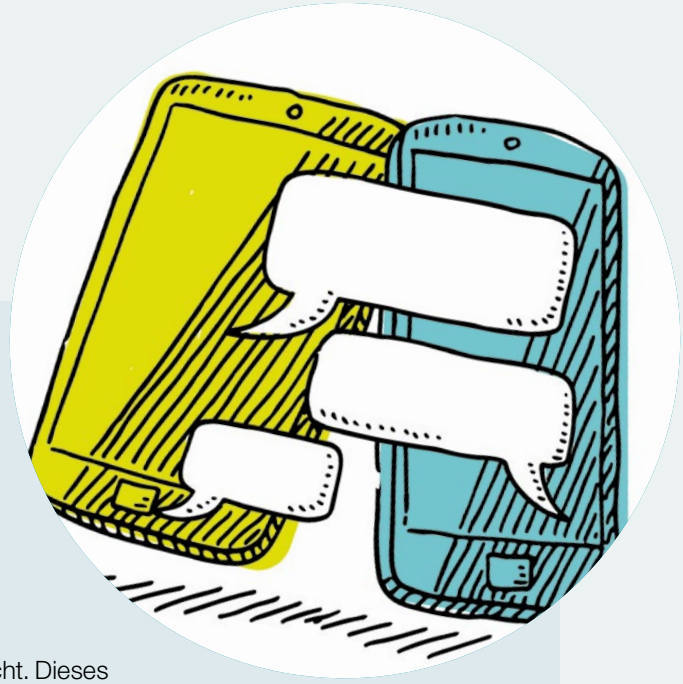
Von einem einheitlichen Standard zur Leichenschau kann also nicht gesprochen werden. Kein Wunder, dass Ärzten teils erhebliche Fehler im Rahmen der Leichenschau unterlaufen. Und es wundert auch nicht, dass die Vorschaltung des Arztes als weitere Prüfungsinstanz den Ermittlungsbehörden daher ein Dorn im Auge ist und diese den ärztlichen Befunden auf dem Totenschein nicht zu viel Vertrauen schenken wollen. Und wieder wäre der Blick in die Patientenakte ein willkommener und effizienter Ermittlungsansatz.

Und hier findet sich unter den Gesetzen zur Leichenschau eine verblüffende Übereinstimmung zu den Regeln einer Auskunftspflicht von allen Angehörigen von Heilberufen, die den Verstorbenen behandelt haben. Diese haben alle Informationen zu beauskunften, die für die Leichenschau von Bedeutung sein könnten.

Der Haken ist nur, dass diese Auskünfte nur vom Arzt der Leichenschau eingeholt werden dürfen. Ermittlungsbehörden können diese Auskünfte nicht einholen und müssen sich also weiterhin mit den Ergebnissen aus der Leichenschau zufriedengeben. Die Entscheidung darüber, ob die Leichenschau hinreichend Zweifel an einem natürlichen Tod ergibt, trifft der Arzt allein.

Fazit

Die Ermittlungsbehörden können die Herausgabe von Patientendaten aus der Patientenakte nicht verlangen. Die Entscheidung über die Beteiligung der Ermittlungsbehörden liegt beim Arzt, wobei diesem zur Prüfung und Abwägung sowie zur Durchführung einer Leichenschau viel abverlangt wird. Eine bundeseinheitliche Regelung ist derzeit nicht absehbar. Den Ärzten kann nur geraten werden, sich vor einer Leichenschau sorgfältig mit den Bestattungsgesetzen auseinanderzusetzen und bei einer Anfrage von Ermittlungsbehörden eine Offenbarung der Patientendaten sorgsam abzuwägen.



Kurznotiz:

Whitepaper zu den technischen Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich.

Der Einsatz von Messenger-Diensten ist nicht nur im Gesundheitsbereich sehr verlockend. Da wird in der Praxis “schon mal“ über WhatsApp ein Konsil eingeholt oder eine Schweigepflichtentbindungserklärung an den Hausarzt geschickt. Gerade beim Einsatz von Messengern bestehen allerdings viele Tücken und Fallstricke. Die DSK, also die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, hat nun ein Whitepaper zum Einsatz von Messenger-Diensten veröffentlicht. Dieses enthält einen umfassenden Kriterienkatalog, der für einen datenschutzkonformen Einsatz erfüllt sein muss. Im nächsten Newsletter werden wir uns mit dem Whitepaper und den Auswirkungen auf den Krankenhausalltag beschäftigen und konkrete Handlungsempfehlungen geben.

© 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

Datenschutz im Gesundheitswesen

Mit Geltung der Europäischen Datenschutz-Grundverordnung und der damit verbundenen umfassenden Anpassung der nationalen Datenschutzvorschriften haben sich die datenschutzrechtlichen Rahmenbedingungen auch für Gesundheitseinrichtungen seit Mai 2018 grundlegend geändert.

Die Broschüre soll Datenschutzverantwortlichen dabei helfen, die Datenverarbeitung in Gesundheitseinrichtungen auch künftig rechtskonform zu gestalten. Das Handbuch vermittelt die neuen gesetzlichen Grundlagen, führt praxisnah in die Datenschutzorganisation ein und erläutert am Beispiel des Krankenhauses die zentralen datenschutzrechtlichen Herausforderungen.

Neben dem Datenschutz wird dabei auch das neue für Gesundheitseinrichtungen zunehmend wichtigere Feld der IT-Sicherheit beleuchtet.

Broschüre HIER bestellen

Broschüre DIN A5, ca. 380 Seiten
Preis: 89,90 € pro Stück inkl. MwSt. und versandkostenfreier Zusendung im Inland
Art. Nr.: 43110 | **ISBN: 978-3-553-43110-1**

Aus dem Inhalt (Auszug):

- **A – Rechtliche Grundlagen**
  DS-GVO, neues BDSG und Auswirkungen für den Gesundheitsdatenschutz
- **B – Datenschutzorganisation**
  Praktische Umsetzung der DS-GVO in Gesundheitseinrichtungen durch den Datenschutzbeauftragten
- **C – Datenschutz im Krankenhaus**
  Patientendatenschutz im Betriebsgeschehen sicherstellen
- **D – Der Internetauftritt**
  Internetauftritt und Social Media-Plattformen rechtssicher ausgestalten
- **E – Datensicherheit**
  Rahmenvorschriften zur IT-Sicherheit und bereichsspezifische Vorgaben für den Gesundheits- und Medizinbereich

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/der-neue-datenschutz-im-gesundheitswesen