Rödl & Partner

FOKUS GESUNDHEITS- UND SOZIALWIRTSCHAFT

Ausgabe: DEZEMBER 2020

Informationen für Entscheider von Krankenhäusern, Pflegeeinrichtungen, Wohlfahrtsverbänden und Hochschulen

Frohe Weihnachten
und ein erfolgreiches Jahr 2021

Liebe Leserin, lieber Leser

was für ein Jahr!

2020 ist wohl für uns alle ein außergewöhnliches Jahr gewesen, vorsichtig formuliert. Ein Jahr, das uns vor noch nie da gewesene Herausforderungen gestellt und uns viele Nerven gekostet hat. Unser Land fest im Griff einer Pandemie, die im besonderen Maße natürlich auf den Schultern der Unternehmen der Gesundheits- und Sozialwirtschaft lastete. Die Front. Dort, wo die Kranken behandelt werden, die Risikogruppe geschützt und betreut werden musste, da wo der Kampf gegen das Virus jeden Tag tatsächlich ausgetragen wird. Viele über die Jahre zugespitzte Faktoren, wie der Pflegenotstand, erhöhten den Schwierigkeitsgrad zusätzlich massiv.

Die Vorweihnachtszeit ist traditionell die Zeit der Besinnung, die Zeit der Dankbarkeit. Es gab vermutlich selten ein Jahr, in dem wir all unseren Menschen im Gesundheits- und Sozialsystem so dankbar sein mussten, wie 2020. Vielen Dank! Für ihren unermüdlichen Einsatz für unser Leben, unsere Gesundheit und unsere Gesellschaft. Wir hoffen, dass wir Ihnen dieses Jahr zur Seite stehen konnten, Ihnen eine helfende Hand in der Krise sein durften und unser Ziel ist es auch, dass weiterhin immer zu sein. In unserer letzten Ausgabe dieses Jahr haben wir Ihnen wieder eine bunte Mischung an Themen zusammengestellt und hoffen, Ihnen damit wieder hilfreichen und interessanten Lesestoff bieten zu können.

Das Virus kennt kein Weihnachten. Wir wissen, für Sie gehört schon immer auch an Feiertagen die Arbeit dazu, dennoch hoffen wir, dass Sie Zeit finden für etwas Ruhe und Besinnlichkeit, für Plätzchen, Glühwein und einen ruhigen Abend neben dem Weihnachtsbaum. Wir wünschen von Herzen fröhliche Weihnachten und vor allem die Hoffnung auf ein GLÜCKLICHES, neues Jahr 2021.

Eine informative Lektüre wünschen

MARTIN WAMBACH
Geschäftsführender Partner

BERND VOGEL
Partner

Erste Erfahrungen mit der wirtschaftlichen Situation in Krankenhäusern während der Corona-Pandemie

von Tim Schilling

DIE CHANCE AUS DER KRISE – RÜCKBLICK AUF EINE TURBULENTE ZEIT OHNE BEVORSTEHENDES ENDE!

Die wirtschaftliche Situation der Krankenhäuser in Deutschland ist auch ohne anhaltende Corona-Pandemie ein zentrales Thema der Berichterstattung. Bereits im Jahr 2018 verschlechterte sich die wirtschaftliche Lage der deutschen Krankenhäuser deutlich laut Krankenhaus Rating Report. Zusätzlich besteht bei etwa 13 Prozent der Kliniken ein erhöhtes Insolvenzrisiko, was somit keine gute Ausgangsbasis für wirtschaftlich turbulente Zeiten ist. Dies erzeugt in den Kliniken neben einem enormen Handlungsdruck und den täglichen Aufgaben, eine konsequente Planung zusätzlicher operativer und strategischer Maßnahmen.

Ungeachtet einer solch wirtschaftlich erschwerten Lage und zusätzlicher Implikationen der Corona-Pandemie, müssen die ablauforganisatorischen Strukturen der Kliniken verbessert werden. Eine strukturelle Verbesserung sollte allerdings nicht ausschließlich über die Verknappung von Ressourcen generiert werden, da ein ungezielter Personalabbau lediglich ökonomische Einmaleffekte ohne die Chance einer Organisationsentwicklung bedeutet.

Sicherlich ist ein Teil der negativen wirtschaftlichen Lage der Krankenhäuser durch die rückläufigen stationären Fallzahlen, den weiter anhaltenden Fachkräftemangel und durch eine fokussierte Prüfung der Krankenhausrechnungen durch den Medizinischen Dienst der Krankenversicherung (MDK) begründet.

Nur ist ebenfalls absehbar, dass dieses Grundbetriebsrisiko der Krankenhäuser zukünftig nicht sinken, sondern durch fehlende Unternehmensagilität wachsen und somit die Untätigkeit den Handlungsdruck in den Kliniken steigern wird.

Die Corona-Pandemie bedeutet aber zusätzlich, neben einer wirtschaftlichen Berg- und Talfahrt für die Mitarbeiter, eine klare und transparente Strategie der Sicherung zu entwickeln.

Begrenzte Testkapazitäten – bei wachsender Zahl von corona-positiven Patienten und Mitarbeitern – führen die Organisation an die Belastungsgrenzen. Somit stellen Schutz und wertschätzende Führung des eigenen Personals und die sichere Versorgung der Patienten die größte Aufgabe dar.

STEIGENDER HANDLUNGSDRUCK

Hieraus folgt die Notwendigkeit zur Entwicklung eines klaren Konzeptes im Patientenmanagement unter verbesserten Sicherheitsstandards analog dem Infektionsschutzgesetz und der sog. Corona-Testverordnung.

Durch den steigenden Fachkräftemangel, verbunden mit dem stark ansteigenden Krankenstand oder Dienstausfall zu Testzwecken, müssen Kliniken stationäre Ressourcen besser verteilen und Kapazitäten planen. Insbesondere trifft dies die Kernbereiche der Organisation, nämlich die Notaufnahmen, OP und Intensivstationen. Das Problem des Fachkräftemangels ist kein temporäres Problem, das kurzfristig behoben werden kann. Allein zurzeit fehlen in Deutschland mehr als 4.000 ausgebildete Intensivpflegekräfte, um die vorhandenen Intensivbetten überhaupt betreiben zu können. Es muss an essenziellen Stellschrauben gearbeitet werden, um zukünftig und insbesondere langfristig erfolgreich Probleme zu lösen.

Ebenso ist dem Rückgang der stationären Fallzahlen mit einer Fokussierung des regionalen Leistungsangebotes in Kombination mit einem effektiveren Ressourceneinsatz entgegenzuwirken. Das qualitative Leistungsangebot muss auf die regionale Versorgungsnachfrage der Bevölkerung adaptiert werden und darf nicht durch ein rein wirtschaftlich profitables Portfolio getriggert werden.

Der sog. „medizinische Warenkorb“ wird zukünftig einen stärkeren Einfluss auf die Krankenhausplanung haben. So ist im Planungsentwurf für die Krankenhausplanung des Landes NRW erstmalig die Abkehr von den sog. Planbetten vollzogen, und er richtet sich vielmehr nach qualitativen Parametern der Versorgungssicherheit und des Bedarfes.

Damit wird ebenso klar, dass die Patienten für bestimmte elektive, aber auch notfallmäßige Leistungen weitere Wege auf sich nehmen müssen.

Heißt konkret, es wird nicht mehr an jedem Krankenhaus der Grundversorgung ein selten genutzter teilausgelasteter Links-Herz-Katheter-Messplatz betrieben werden können.

Auch die verschärften Rechnungsprüfungen des nun unabhängigen Medizinischen Dienstes, die mit dem MDK-Reformgesetz eingeführt worden sind, stellen Kliniken vor große Herausforderungen. Genau diese qualitativen Prüfungen werden den inhaltlichen Druck auf die Krankenhäuser erhöhen.

Zum einen wird der Druck durch die gestaffelte Prüfungsquote verstärkt, zum anderen zwingt dies die Einrichtungen entsprechende personelle und qualifizierte Ressourcen für den erkennbaren bürokratischen Mehraufwand aufzubauen.

CORONA – WAS NUN?

Mit Beginn der Corona-Pandemie wurden Krankenhäuser vor eine neue große Herausforderung und Zerreißprobe gestellt, denn die stationären Kapazitäten konnten nicht wie gewohnt genutzt, sondern mussten freigehalten werden.

Kliniken erhielten für die verschobenen elektiven Operationen einen finanziellen Ausgleich, der zeitlich begrenzt und in Abhängigkeit der Versorgungsstufe gestaffelt wurde. Der finanzielle Ausgleich betrug gemittelt 560 Euro pro nicht belegtem Bett pro Tag.

Darüber hinaus wurde eine Prämie in Höhe von 50.000 Euro pro aufgestocktem Intensivbett an die Krankenhäuser gezahlt. Ergänzend wurde sowohl die Rechnungsprüfung als auch die Zahlungsfrist der Kostenträger angepasst, um die Liquidität und finanzielle Situation der Kliniken zu verbessern. Die Maßnahmen zur Entlastung der wirtschaftlichen Situation von Krankenhäusern wurden im Covid-19-Krankenhausentlastungsgesetz gesetzlich fixiert.

Dabei ganz vergessen wurde, dass im pandemischen Krankheitsfall der Bevölkerung ebenfalls die Mitarbeiter zunehmend betroffen sind. Eingeschränkte Testkapazitäten, fehlende Anpassung der Ablauforganisationen und unzureichender Mitarbeiterschutz sowie fehlende Informationen führen in vielen Kliniken zum Chaos. Erstmalig in der Gesundheitswirtschaft stehen wir vor einem Versorgungsgau bestehend aus wirtschaftlicher Handlungsunfähigkeit, fehlender Strategie und eklatanter Personalfehlallokation!

ZUKÜNFTIGE STRATEGISCHE AUSRICHTUNG

Trotz einer staatlichen Überbrückung von wirtschaftlich schweren Zeiten durch die Corona-Pandemie ist eine wirtschaftliche solide Ausgangsbasis für Kliniken von enormer Wichtigkeit. Die finanziellen Überbrückungshilfen für Kliniken sichern nicht bei allen eine auskömmliche Refinanzierung der Zusatzkosten, sodass die wirtschaftliche Lage sich noch stärker verschlechtert. Umso wichtiger ist es, sich als Unternehmen in den Bereichen der Organisation, der Prozesssteuerung und den finanzwirtschaftlichen Kernbereichen effizient aufzustellen.

Aus unserer Erfahrung heraus zeigten sich in vielen Kliniken erhebliche Defizite und Potenziale zur Optimierung der Personalallokation in nicht finanzierter Behandlungszeit und ein konsekutiver Verlust der Wirtschaftlichkeit. Es bedarf einer zielgerichteten Ressourcenplanung und eines einheitlichen Konzepts zur Verbesserung der Wirtschaftlichkeit.
Ein weiterer wichtiger Faktor für die zukünftige Entwicklung werden die Patientenströme sein, da auch aufgrund der Corona-Pandemie sich diese erfahrungsgemäß intern wie extern ändern werden. Sowohl die Nutzung der stationären als auch der ambulanten Strukturen wird sich verändern und eine stärkere Verzahnung, Interdisziplinarität und Flexibilität fordern.

Kontakt für weitere Informationen

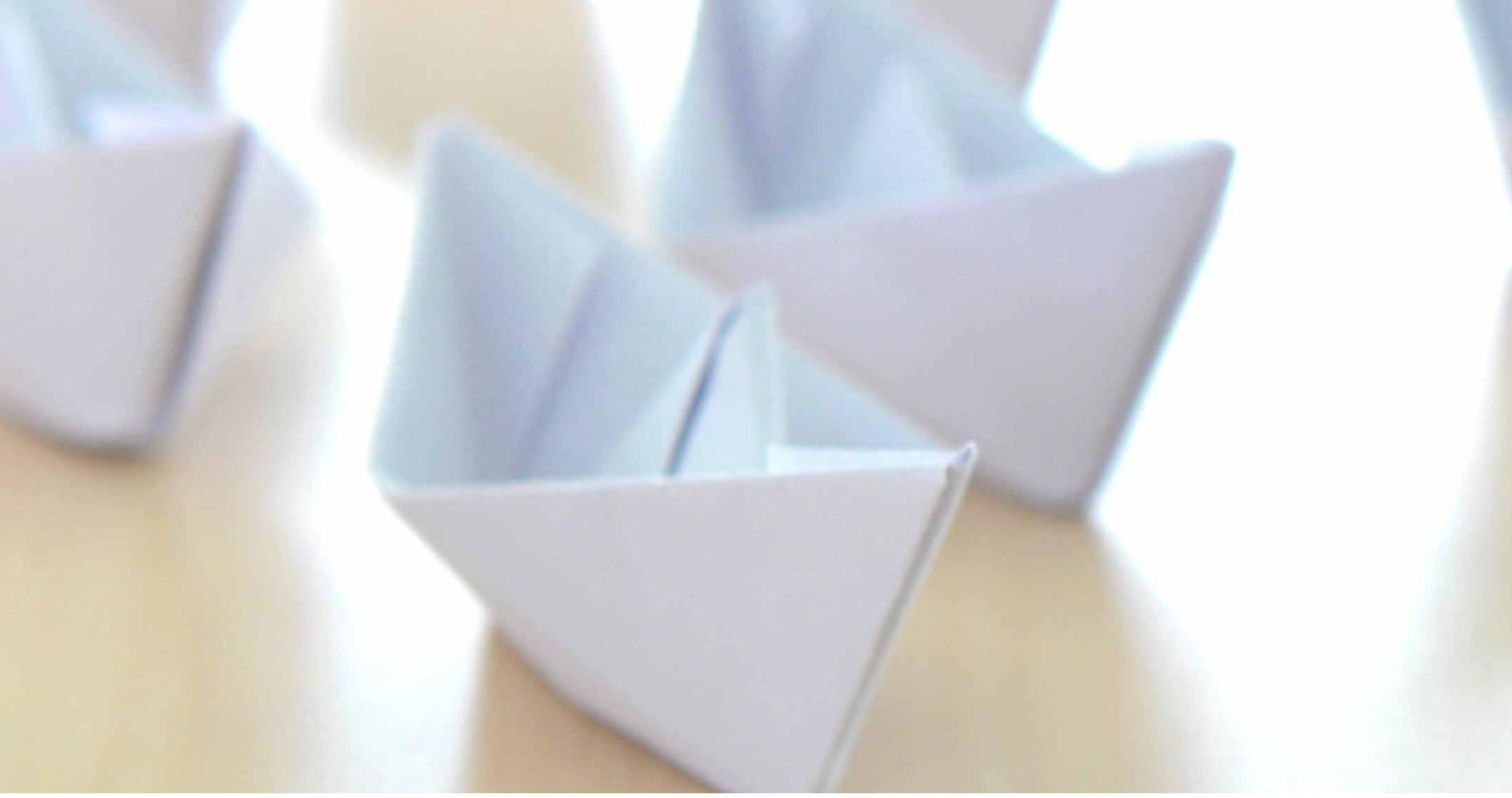
Tim Schilling
B. Sc. Medizinökonomie, Fachberater
T +49 221 949 909 141
E tim.schilling@roedl.com

Der wirtschaftliche Druck auf Krankenhäuser steigt jährlich!

Steigende und zum Teil nicht vollständig refinanzierte Aufwendungen führen zu einer immer stärkeren wirtschaftlichen Belastung und damit einem immer größeren Handlungsdruck auf Krankenhäuser. Neben der laufenden Steuerung und Überwachung der Aufwendungen wird jedoch häufig die Erlösseite vernachlässigt. Insbesondere durch das Fehlen eines aussagekräftigen Berichtswesens sowie nicht-optimale Begleitprozesse zur medizinischen und pflegerischen Behandlung und Dokumentation verlieren Krankenhäuser jährlich hohe Erlös-Potenziale für tatsächlich erbrachte Leistungen.

Identifizieren und heben Sie das wirtschaftliche Potenzial Ihrer Organisation. In unserem **KOSTENLOSEN** Whitepaper stellen wir Ihnen 6 Möglichkeiten zur Bewertung des stationären Geschehens und damit zur Bezifferung des wirtschaftlichen Potenzials Ihrer Organisation dar.

https://www.roedl.de/wen-wir-beraten/gesundheit-sozialwirtschaft/downloadcenter-gesundheit-sozialwirtschaft



→ Compliance

Von der Notwendigkeit eines Compliance-Managements sind alle überzeugt – und nun? Die Einrichtung eines CMS in der Praxis

von Christoph Naucke

Dass es für Sozialunternehmen und Krankenhäuser immer wichtiger wird, ein funktionsfähiges Compliance Management System (CMS) eingerichtet zu haben, ist inzwischen im Bewusstsein von Vorständen, Geschäftsführern und ehrenamtlichen Vorstandsmitgliedern angekommen. Zu vielfältig und unkalkulierbar sind die persönlichen Haftungsrisiken, egal ob strafrechtlich, steuerrechtlich, zivilrechtlich, nach dem Ordnungswidrigkeitengesetz oder nach dem demnächst anstehenden Unternehmensstrafrecht. Und nun? Was ist konkret zu tun, wenn man sich entscheidet, ein Compliance Management System einzuführen? Kurz gesagt: Organisation von Compliance ist nicht alles, aber ohne Organisation ist alles nichts. Der Prüfungsstandard 980 des IDW hilft dabei, nichts Wesentliches zu vergessen.

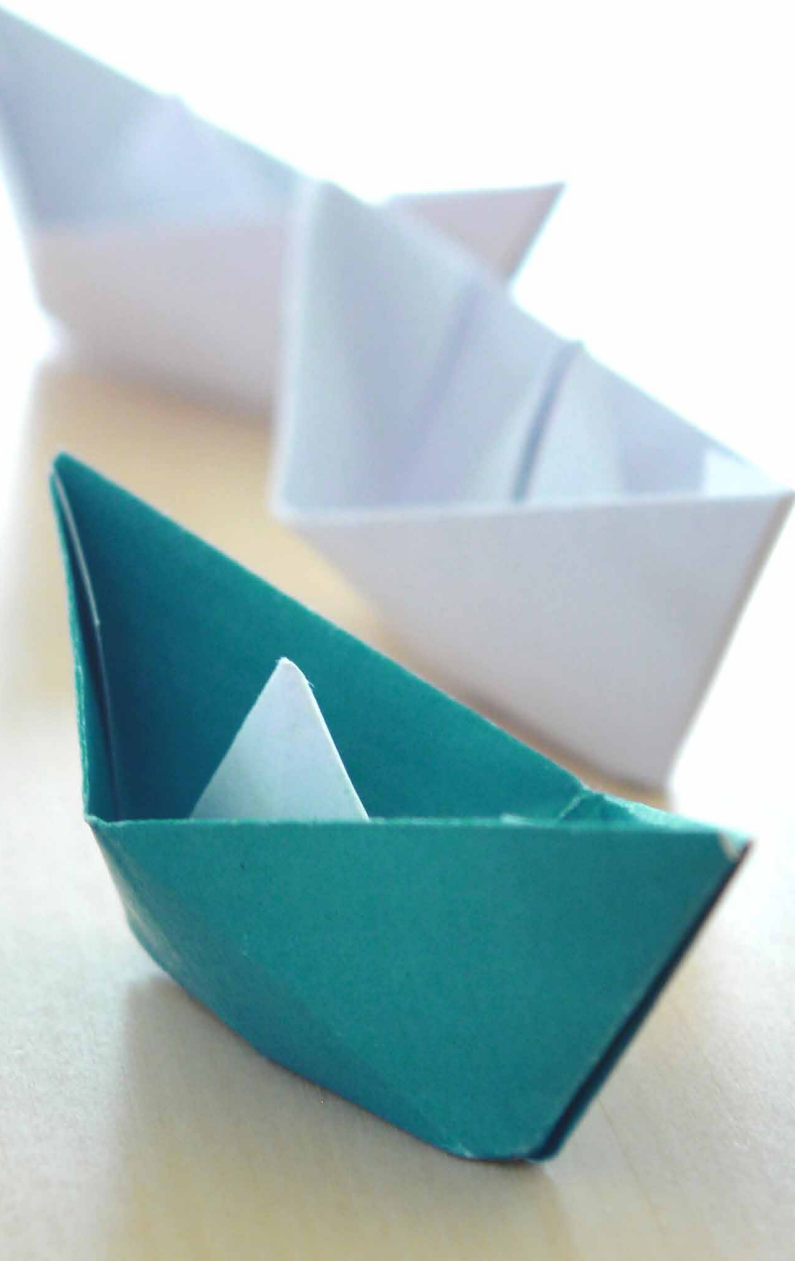
GEMEINSAMES VERSTÄNDNIS VON COMPLIANCE – EINE SCHEINBARE SELBSTVERSTÄNDLICHKEIT

Wenn die Entscheidung getroffen ist, ein Compliance Management System einzurichten, wird meist ein Projekt aufgelegt, das den Auftrag erhält, das CMS zu konzipieren und aufzubauen. Noch davor sollten die Verantwortlichen allerdings herausarbeiten, was die Compliance-Kultur dieses Unternehmens ausmacht und definiert und dem Projekt diese Vorgaben als Grundlage mitgeben. Denn in der praktischen Umsetzung lauern unerwartete Stolpersteine.

Diese beginnen damit, dass es sich bei „Compliance“ um eine scheinbare Selbstverständlichkeit handelt. Die Absicht compliant zu sein, also sich als Unternehmen regelkonform zu verhalten, war schon lange vor der Verwendung des Wortes „Compliance“ eine Selbstverständlichkeit. Gerade deshalb stehen kulturelle Leitfragen am Anfang: Welche Aktualität und welchen Bekanntheits- und Akzeptanzgrad genießen die Unternehmensziele bei den Mitarbeitern? Leitet sich aus diesen Zielen regelkonformes Verhalten ab? Ist ein gemeinsames Verständnis hinsichtlich Führung und Verantwortung im Unternehmen verankert? Eine ehrliche Ist-Aufnahme verhindert, dass aus einer gesundpositiven Selbsteinschätzung unversehens blinde Flecken werden, die das CMS als solches dauerhaft belasten würden.

Im Rahmen der Projektarbeit sollte es anschließend eines der ersten Ziele sein, die organisatorische Zuständigkeit für das Managementsystem CMS zu klären und eine personelle Besetzung dieser Aufgabe zu erreichen. Dabei ist es wichtig, zwischen dieser Zuständigkeit für das Managementsystem CMS einerseits und dem regelkonformen Verhalten aller Mitarbeiter andererseits, dem „being compliant“, sorgfältig zu unterscheiden. Ersteres ist Teil der Organisationsaufgabe „CMS“, letzteres ist untrennbar mit jeder Führungsverantwortung verbunden und daher eine persönliche Aufgabe für buchstäblich „jeden“.

Die frühzeitige Besetzung der Systemverantwortung für das CMS ermöglicht es der Geschäftsführung, frühzeitig aus der persönlich umsetzenden in eine überwachende und entscheidunggebende Rolle hinüberzuwechseln.



DIE COMPLIANCE-ORGANISATION: COMPLIANCE FEST VERANKERN

Dass die Einrichtung eines Compliance-Managements eine Art einmaliger, projekthafter Schritt ist und das Unternehmen anschließend davon ausgehen kann, „compliant zu sein“, ist ein häufiges Missverständnis. Compliance ist kein Zustand, sondern ein Anspruch. Damit liegt eine wesentliche Aufgabe für die Einrichtung des CMS in der Beschreibung der regelmäßigen Compliance-Prozesse und deren Verankerung in den existierenden Kernprozessen des Unternehmens. Die im CMS definierten Regelprozesse der Prävention, der laufenden Beobachtung und ggf. auch der Sanktionierung von Complianceverstößen müssen dann sukzessive in den Tagesbetrieb überführt werden. Wenn eine Bestätigung des CMS in Form eines Prüfungsberichts nach dem IDW PS 980 angestrebt wird, ist u. a. diese Frage ein zentrales Prüfungsthema.

WO DER TEUFEL IM DETAIL STECKT: ZU DEN COMPLIANCE-ZIELEN GEHÖRT WESENTLICH MEHR ALS EIN BEKENNTNIS ZU GESETZESKONFORMEM HANDELN

Wesentlicher Baustein für die Einrichtung eines CMS ist ein Handbuch, in dem das Verständnis und die Umsetzung von Compliance im Unternehmen für jeden Mitarbeiter verständlich beschrieben werden. Ein gemeinsamer und tragfähiger Konsens des Managements über die Compliance-Kultur und die Compliance-Ziele stellt die wichtigste Grundlage für das Handbuch dar.

Typischerweise taucht im Rahmen der Erarbeitung des Handbuchs die Frage auf, welche externen Rechtsquellen und internen Regeln für die Mitarbeiter eigentlich maßgeblich sind. Hier steckt meist der Teufel im Detail. Die Praxis zeigt, dass eine ad hoc verfügbare Zusammenstellung aller compliance-relevanten Regeln und Regelwerke oft eine große Herausforderung darstellt. Schließlich muss bei dieser Zusammenstellung garantiert werden können, dass jeweils die aktuellen Fassungen sowie, falls erforderlich, auch ältere Versionen abrufbar sind. Es gilt sowohl allgemeine Rechtsnormen, die für jedes Unternehmen gelten, als auch die spezifischen Rechtsgebiete abzubilden, die sich aus dem Leistungsspektrum ergeben. Bei einem komplexen Sozialunternehmen mit Dienstleistungen aus ambulanter und stationärer Pflege, Jugendarbeit, Behindertenhilfe und vielleicht auch Rettungsdienst kommt eine Menge zusammen.

Was tun, wenn die Liste völlig unübersichtlich wird und der Mitarbeiter den sprichwörtlichen „Wald vor lauter Bäumen“ nicht mehr sehen kann? Intelligente, teilweise mehrstufige Dialog- und Suchsysteme haben sich in dieser Herausforderung oft bewährt. Es ist keine Option,

den Vollständigkeitsanspruch aufzugeben, denn damit würde das Unternehmen einerseits Compliance vom Mitarbeiter fordern und ihn andererseits mit dieser Forderung allein im Regen stehen lassen.

COMPLIANCE-MANAGEMENT UND RISIKOMANAGEMENT: UNGLEICHE GESCHWISTER

Viele Unternehmen der Gesundheits- und Sozialwirtschaft haben bereits Risikomanagementsysteme eingerichtet. Dass es zwischen beiden Funktionen erhebliche Überschneidungen, aber auch Unterschiede gibt, ist unübersehbar. Es ist notwendig, zu diesen Unterschieden und Überschneidungen zwischen beiden Seiten ein gemeinsames Verständnis zu entwickeln. Nur dann kann man es vermeiden, in der Funktion des verantwortlichen Compliance-Managers nicht von vornherein einen dauerhaften, jedoch unproduktiven Rollenkonflikt mit dem Risikomanager anzulegen.

Wenn man bei der Ermittlung der Compliance-Ziele, also auch des verwendeten Regelwerks, seine Hausaufgaben nicht sorgfältig erledigt hat, fällt einem dies spätestens bei der Ermittlung der Compliance-Risiken „auf die Füße“. Denn um nachzudenken, woraus ungewollte Regelverstöße resultieren könnten, muss man die betreffende Regel und deren Anwendung im Arbeitsalltag vor Augen haben.

Unter dem Blickwinkel der Zielsetzungen betrachtet, geht es sowohl im Risikomanagement als auch im Compliance-Management darum, Risiken zu identifizieren und adäquate Risikovorsorge zu betreiben. Kennzeichnend für das Compliance-Management ist darüber hinaus ein unternehmensweiter Informations- und Kommunikationsauftrag, während zu den spezifischen Merkmalen des Risikomanagements auch die monetäre Bewertung und, darauf basierend, die Kategorisierung der einzelnen Risiken zählt. Dementsprechend unterscheiden sich auch die konkreten, alltäglichen Aktivitäten der beiden Funktionen wesentlich.

MONITORING DER COMPLIANCE-RISIKEN: SYSTEMATISCHE ENTWICKLUNG GEFRAGT

Das Monitoring der compliance-relevanten Risiken sollte in jedem Fall Bestandteil des bereits etablierten Risikomonitorings werden, da das Management auf diese Weise die Gewissheit erhält, sich aus einer Quelle über das komplette Risikoportfolio zu informieren. Was sich in der Praxis bewährt hat: bei der Compliance Risk Map neben der Liste der compliance-relevanten Regeln auf eine vollständige Abbildung der internen Organisation zu achten. Ohne ein hohes Maß an Praxiswissen aus buchstäblich allen Winkeln des Unternehmens ist die Risk Map letztlich nicht zu erarbeiten. Dabei kann ein externer Moderator als Sparringspartner, Organisationspartner, Unterstützer für die Aufbereitung und Strukturierung und, nicht selten, auch als Prozesstreiber wertvolle Hilfestellung leisten.

FAKTOR MENSCH: COMPLIANCE-KOMMUNIKATION

Da Compliance als solches kein einmalig erreichbarer und abzusichernder Zustand, sondern vielmehr ein im Unternehmen auf Dauer angelegter Anspruch ist, muss die dauerhafte Sensibilisierung aller Mitarbeiter für die Belange von Compliance immer wieder neu mit Leben gefüllt werden. Dabei ist jedoch mit dem eingangs genannten Irrtum umzugehen: Mitarbeiter nehmen zu Recht für sich in Anspruch, bei der Ausübung ihrer Tätigkeit jederzeit nach bestem Wissen und Gewissen regelkonform zu handeln und werden daher die Initiative zur Einrichtung eines CMS schnell als Misstrauensvotum verstehen.

Mit dieser Skepsis muss das Compliance-Management daher aktiv und sensibel umgehen. Wesentliche Faktoren für die Legitimation von Compliance sind ein über-

zeugtes, persönliches Auftreten des Topmanagements zum Thema Compliance, klare Argumente, die nicht allein darauf beruhen sollten, dass Topmanager Haftungsrisiken für sich ausschließen wollen und eine frühzeitige und verbindliche Einbindung des Managements insgesamt. Das Kernargument wird meist darin liegen, dass regelkonformes Verhalten einer (komplexen) Organisation nicht automatisch durch das nach bestem Wissen regelkonforme Handeln der Mitarbeiter erreicht wird. Compliance-Gefahren, die in komplexen und abteilungsübergreifenden Prozessen verborgen sind, sind ein typisches Beispiel für diese Erkenntnis.

REALISTISCH PLANEN

Die Herausforderungen sind nicht klein und zeigen sich oftmals erst während der Projektarbeit. Daher werden Projektaufwand und damit auch der Zeitbedarf in vielen Fällen unterschätzt. Die Praxis zeigt, dass für die Konzeptionsphase eines CMS, abhängig vom Status quo hinsichtlich Risikomanagement sowie den vorhandenen inhaltlichen Grundlagen und von der Komplexität insgesamt, mit einem Zeitbedarf von 12 bis 24 Monaten gerechnet werden muss.

Kontakt für weitere Informationen

Christoph Naucke
Betriebswirt (BA),
zertifizierter Compliance Officer,
zertifizierter Datenschutzbeauftragter DSB
T +49 911 9193 3628
E christoph.naucke@roedl.com

→ Datenschutz

Patientendatenschutzgesetz

Sind bald alle Krankenhäuser Kritis-Betreiber?

von Jürgen Schwestka und Konrad Klein

Krankenhäuser mit mehr als 30.000 vollstationären Fällen pro Jahr gelten gemäß Kritis-Verordnung als Betreiber einer Kritischen Infrastruktur und unterliegen somit einer regelmäßigen Nachweispflicht nach § 8a Abs. 3 BSI-Gesetz.

Entsprechend müssen sie alle 2 Jahre gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nachweisen, dass sie geeignete technische und organisatorische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik umgesetzt werden.

WAS ÄNDERT SICH DURCH DAS PATIENTENDATENSCHUTZGESETZ?

Ab dem 1.1.2022 sind alle Krankenhäuser verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind.

Die informationstechnischen Systeme sind spätestens alle 2 Jahre an den aktuellen Stand der Technik anzupassen. Die Krankenhäuser können die Verpflichtungen insbesondere erfüllen, indem sie den branchenspezifischen Sicherheitsstandard (B3S) für die Gesundheitsversorgung im Krankenhaus in der jeweils gültigen Fassung anwenden und umsetzen. Dieser B3S wurde durch das BSI bereits auf angemessene Maßnahmen überprüft und freigegeben. Im Fokus der Maßnahmen steht ein Managementsystem für Informationssicherheit – das ISMS – und das damit einhergehende Management von Informationssicherheitsrisiken.

Diese Verpflichtungen gelten zukünftig für alle Krankenhäuser, unabhängig von den jährlichen Fallzahlen. Sie müssen allerdings, anders als die Betreiber Kritischer Infrastrukturen gemäß § 8a des BSI-Gesetzes, keinen Prüfnachweis beim BSI einreichen.

WELCHE VERPFLICHTUNGEN ERGEBEN SICH DARAUS?

Zwar ist die Umsetzung des aktuellen B3S für die Gesundheitsversorgung in Krankenhäusern nicht zwingend vorgeschrieben, da angemessene Informationssicherheit häufig auf unterschiedliche Arten und durch unterschiedliche Maßnahmen erreicht werden kann. Dennoch empfehlen wir die Umsetzung oder zumindest die Orientierung an dem aktuellen B3S. Viele der dort beschriebenen Maßnahmen sind obligatorisch umzusetzen und praxisnah formuliert, schließlich wurde der B3S von Krankenhausbetreibern für Krankenhausbetreiber geschrieben. Den aktuellen Stand des B3S für die Gesundheitsversorgung im Krankenhaus finden Sie auf den Internetseiten der Deutschen Krankenhausgesellschaft (https://www.dkgev.de/themen/digitalisierung-daten/informationssicherheit-und-technischer-datenschutz/informationssicherheit-im-krankenhaus/). Alternativ oder auch ergänzend kann eine Orientierung an der bekannten ISO/IEC 27001 Norm oder am BSI-Grundschutzkompendium stattfinden.

Aus dem B3S ergeben sich rund 200 Anforderungen aus verschiedenen Bereichen. Bei der Priorisierung von Maßnahmen zu diesen Anforderungen ist ein risikoorientierter Ansatz sinnvoll. Wir empfehlen hierbei ein zweistufiges Vorgehen:

- Absicherung von außen nach innen: Zuerst den Perimeterschutz sicherstellen (z. B. durch Firewalls, VPN-Zugänge, USB-Ports) und dann, nachdem man gegen externe Bedrohungen geschützt ist, auch noch die internen Bereiche absichern.
- Absicherung vom Allgemeinen zum Speziellen: Zunächst sollte eine allgemeine Basis-Absicherung erfolgen, die für alle Bereiche relevant ist, z. B. Virtualisierung und Backup. Anschließend können die einzelnen Systeme je nach Risiko und Priorität gesichert werden, z. B. KIS, Medizingeräte.

Bei der Planung von Maßnahmen und deren Fristen sollten stets die Risiken der Schwachstellen berücksichtigt werden. Auch „interne Schwachstellen“ können zu gro-

ßen Schäden führen. Neben der Stärkung der Strukturen und Verfahren im Risikomanagement geht es bei den Anforderungen aus dem B3S insbesondere um die folgenden Bereiche:

- Informationssicherheitsmanagementsystem (ISMS)
- Organisation der Informationssicherheit
- Meldepflichten nach § 8b Absatz 4 BSI-Gesetz
- Betriebliches Kontinuitätsmanagement
- Asset Management
- Robuste/resiliente Architektur
- Physische Sicherheit
- Personelle und organisatorische Sicherheit
- Vorfallerkennung und Behandlung
- Überprüfungen im laufenden Betrieb
- Externe Informationsversorgung und Unterstützung
- Lieferanten, Dienstleister und Dritte
- Technische Informationssicherheit

DAS INFORMATIONSSICHERHEITSMANAGEMENT-SYSTEM IM FOKUS

Während die technische Informationssicherheit bei den meisten Häusern im Fokus steht, kommt die Formalisierung des Informationssicherheitsmanagementsystems meistens zu kurz. Hier ist insbesondere hervorzuheben, dass ein Informationssicherheitsbeauftragter (bzw. IT-Sicherheitsbeauftragter) benötigt wird, der sich um den Aufbau und die Aufrechterhaltung des ISMS kümmert. Darüber hinaus muss der ISB durch Prüfungen sicherstellen, dass die Vorgaben zur Informationssicherheit eingehalten werden. Er entlastet und berät die Geschäftsleitung durch seine Tätigkeit hinsichtlich des Umsetzungsstandes zur Informationssicherheit. Den IT-Leiter gleichzeitig als ISB zu benennen ist nicht zielführend, weil entsprechend eine Selbstprüfung vorgenommen würde – darüber hinaus betreffen die Aufgaben des ISB nicht nur die Informationssicherheit in IT-gestützten Prozessen, sondern genauso auch papiergebundene Prozesse und Informationen.

Die aktuelle Corona-Krise macht uns zudem deutlich, dass Krankenhäuser stärker im Fokus von Cyber-Attacken bei gleichzeitig noch höherer Bedeutung der Gesundheitsversorgung stehen. Daher ist es umso wichtiger, das schwächste Glied in der Kette zu stärken: den Menschen. Man kann durch IT-Systeme einen hohen Grad von technischer Sicherheit erreichen, am Ende reicht jedoch ein Klick eines Mitarbeitenden in einer E-Mail und das Risiko ist auf den Systemen. Daher ist es umso wichtiger, ein Konzept zur Sensibilisierung der Mitarbeiter zu haben und laufend Maßnahmen zu ergreifen. Um Informationssicherheit zu schaffen, sind technische Maßnahmen genauso wichtig wie organisatorische und strukturelle Maßnahmen sowie ein Bewusstsein der Mitarbeiter für Risiken.

KEINE PRÜFPFLICHT, ALSO KEIN PROBLEM?

Eine Prüfpflicht besteht nicht, allerdings müssen sich die Krankenhäuser fragen, in welcher Form sie nachweisen können, dass sie den aktuellen Stand der Technik umgesetzt haben. Diese Frage wird insbesondere relevant, falls es doch mal zu einem Zwischenfall kommen

sollte – wie man der Presse entnehmen kann, werden Krankenhäuser immer häufiger Ziel von Cyber-Attacken. Es ist dann, ähnlich wie im Bereich Tax-Compliance, hilfreich, wenn man gegenüber den Aufsichtsbehörden nachweisen kann, dass notwendige Maßnahmen ergriffen wurden, um sich bestmöglich zu schützen.

Es empfiehlt sich daher aus unserer Sicht, die Durchführung eines simulierten Prüfverfahrens nach § 8a BSIG. Für das Nachweisverfahren von Kritis-Betreibern gibt es einen Prüfnachweisplaner, der im Branchenarbeitskreis Medizinische Versorgung erstellt wurde. Dieser enthält Empfehlungen für die Anzahl von Prüftagen, in Abhängigkeit von der Größe des Hauses. Da bei der simulierten Prüfung das Ergebnis nicht beim BSI eingereicht werden muss, kann der Prüfungsumfang theoretisch auch reduziert werden. Vorab empfiehlt sich eine kursorische Prüfung, die sogenannte GAP-Analyse, um strukturelle Schwachstellen zu identifizieren und die geplanten oder bereits initiierten Maßnahmen zu bestärken.

DOWNLOADCENTER

für die Gesundheits- und Sozialwirtschaft

KOSTENLOSE ...

Whitepaper

Checklisten

Eckpunktepapiere

Flyer

Broschüren

Und vieles mehr ...

Jetzt runterladen:
www.roedl.de/downloadcenter-gesundheit-sozialwirtschaft

Kontakt für weitere Informationen

Jürgen Schwestka
Diplom-Kaufmann (Univ.),
IT-Security-Manager/Auditor (TÜV),
CISA, IT Auditor IDW
T +49 911 9193 3508
E juergen.schwestka@roedl.com

Konrad Klein
Bachelor of Science, CISA,
IT-Auditor IDW
T +49 911 9193 3686
E konrad.klein@roedl.com

→ Datenschutz

Patientendaten-Schutz-Gesetz in Kraft getreten

Die elektronische Patientenakte kommt zum 1.1.2021 – jedoch unter datenschutzrechtlichen Bedenken

von Maximilian Dachlauer

Mit der Billigung des Bundesrats am 18.9.2020 nahm das Patientendaten-Schutz-Gesetz auch die letzte Hürde im Gesetzgebungsverfahren und wurde schließlich am 19.10.2020 im Bundesgesetzblatt veröffentlicht. Damit ist es seit dem 20.10.2020 in Kraft.

WELCHE DATEN WERDEN IN DER ELEKTRONISCHEN PATIENTENAKTE (EPA) GESPEICHERT UND WER STELLT SIE ZUR VERFÜGUNG?

Auf Wunsch des Patienten werden in der ePA Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte, Impfungen, elektronische Medikationspläne, elektronische Arztbriefe und Notfalldatensätze gespeichert. Neben diesen Daten können auch eigene Daten, wie z. B. ein Tagebuch über Blutzuckermessungen, abgelegt werden.[1]

Durch das Terminservice- und Versorgungsgesetz sind Krankenkassen ab 2021 verpflichtet, allen gesetzlich Versicherten eine ePA zur Verfügung stellen.

TELEMATIKINFRASTRUKTUR ERMÖGLICHT DEN DATENVERKEHR

Damit alle Daten gespeichert werden können, müssen sich Arztpraxen und weitere Einrichtungen wie zum Beispiel Krankenhäuser an die sogenannte Telematikinfrastruktur (TI) anschließen.

Die TI ist die „Datenautobahn des Gesundheitswesens“ und vernetzt Leistungserbringer, Kostenträger und Versicherte. Sie umfasst sowohl eine dezentrale Infrastruktur als auch eine zentrale Infrastruktur sowie verschiedene Anwendungen.

Die dezentrale Infrastruktur besteht aus Komponenten zur Authentifizierung und sicheren Übermittlung von Daten in die zentrale Infrastruktur. Komponenten der dezentralen Infrastruktur sind beispielsweise die elektronische Gesundheitskarte, die Heilberufs- und Berufsausweise sowie die Komponenten zur Authentifizierung von Leistungserbringerinstitutionen, die die Authentifizierung, Verschlüsselung und elektronische Signatur gewährleisten. Auch zählen die Konnektoren dazu, die die sichere Verbindung zur TI herstellen und sicherheitskritische Funktionalitäten anbieten, ebenso wie die E-Health-Kartenterminals zum Lesen der Karten und Ausweise.

Die zentrale Infrastruktur enthält sichere Zugangsdienste (z. B. über ein virtuelles privates Netzwerk, abgekürzt VPN) als Schnittstelle zur dezentralen Infrastruktur und ein gesichertes Kommunikationsnetz.

Die Anwendungsinfrastruktur als dritter Baustein der TI hingegen besteht aus verschiedenen technischen Diensten und Systemen, die einzelne Funktionalitäten der TI umsetzen und überhaupt nutzbar machen (z. B. das Versichertenstammdatenmanagement oder auch die elektronische Patientenakte als Software).

Mit dem Digitale-Versorgung-Gesetz wurden Apotheken bis Ende September 2020 und Krankenhäuser bis 1.1.2021 verpflichtet, sich an die TI anzuschließen. Ärzte, die sich nicht anschließen wollen, mussten ab 1.3.2020 einen Honorarabzug von 2,5 Prozent in Kauf nehmen.[2]

WAS REGELT DAS PATIENTENDATEN-SCHUTZ-GESETZ IN DIESEM ZUSAMMENHANG?

In der ePA werden zahlreiche sehr sensible Gesundheitsdaten eingestellt. Der nötige Datenschutz für die Gesundheitsdaten der Patienten soll durch das Patientendaten-Schutz-Gesetz gewährleistet werden. Für die Effektivität der ePA ist auch entscheidend, dass der Patient mit dem PDSG ein Recht darauf erhält, dass der Arzt die ePA befüllt.

DSK STUFT PDSG ALS EUROPARECHTSWIDRIG EIN

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hält mit Entschließung vom 1.9.2020 das PDSG für europarechtswidrig.[3]

[1] https://www.bundesgesundheitsministerium.de/service/begriffe-von-a-z/e/elektronische-patientenakte.html, zuletzt abgerufen am 09.11.2020.
[2] https://www.bundesgesundheitsministerium.de/service/begriffe-von-a-z/e/elektronische-patientenakte.html, zuletzt abgerufen am 09.11.2020.
[3] https://www.datenschutzkonferenz-online.de/media/en/20200901_PDSG_Entschlie%C3%9Fung.pdf, zuletzt abgerufen am 09.11.2020.

Durch das zu grob ausgestaltete Zugriffsmanagement werde gegen das datenschutzrechtliche Need-to-know-Prinzip verstoßen. Hintergrund ist, dass im Jahr 2021 keine Steuerung auf Dokumentenebene für die von den Ärzten eingestellten Daten vorgesehen ist. Alle Ärzte, denen die Patienten Einsicht gewähren, können alle Patientendaten einsehen, auch wenn dies in der konkreten Behandlungssituation nicht erforderlich ist. So kann beispielsweise der behandelnde Zahnarzt auf die Daten des behandelnden Psychiaters zugreifen und umgekehrt. Dies soll sich erst ab 2022 ändern. Versicherte, die keine geeigneten Endgeräte besitzen oder diese nicht nutzen möchten, erhalten aber auch über das Jahr 2021 hinaus nicht die Möglichkeit, die Zugriffsrechte im Einzelnen zu managen. Ab 1.1.2022 ist diesen sog. „Nicht-Frontend-Nutzern" lediglich eine Vertreterlösung möglich. Sie können ihre Rechte mittels eines Vertreters und dessen mobilem Endgerät ausüben, müssen hierzu jedoch dem Vertreter vollständigen Zugriff auf ihre Gesundheitsdaten gewähren.

Die DSK kritisiert jedoch auch das Authentifizierungsverfahren für die ePA. Nach der DSGVO muss die Authentifizierung ein höchstmögliches Sicherheitsniveau nach dem Stand der Technik gewährleisten. Schließlich handelt es sich bei den Daten in der ePA um höchstsensible Gesundheitsdaten. Dies gelte – so die DSK – insbesondere für Authentifizierungsverfahren ohne Einsatz der elektronischen Gesundheitskarte (sog. alternative Authentifizierungsverfahren). Erfüllen diese das höchstmögliche Sicherheitsniveau nicht, wird gegen geltendes Datenschutzrecht verstoßen.

DER BUNDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT KÜNDIGT MASSNAHMEN AN

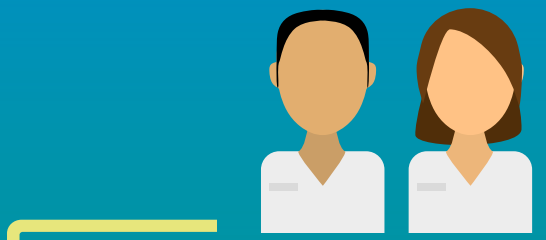
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) Professor Ulrich Kelber hat, wie berichtet, bereits aufsichtsrechtliche Mittel angekündigt.[4] Er ist für die Datenschutzaufsicht über einen Großteil der gesetzlichen Krankenkassen zuständig. Mit allen ihm zur Verfügung stehenden aufsichtsrechtlichen Mitteln werde er dafür sorgen, dass die Krankenkassen mit der von ihnen angebotenen ePA nicht gegen die DSGVO verstoßen. Zudem bereite er bereits entsprechende Warnungen und Weisungen vor, damit die Krankenkassen nur nach Nutzung eines nach Stand der Technik hochsicheren Authentifizierungsverfahrens Zugriffe auf Gesundheitsdaten erlauben. Wie die Medical Tribune berichtet[5], hat der BfDI den Krankenkassen, die seiner Aufsicht unterstehen, in einem Schreiben vom 6. November eine offizielle Warnung hinsichtlich der ePA übermittelt. Die Befugnisse der zuständigen Datenschutzaufsicht würden nach Art. 58 Abs. 2 lit. d) und f) DSGVO auch das Recht einschließen, den Verantwortlichen anzuweisen, eine Verarbeitungstätigkeit in Einklang mit der DSGVO zu bringen sowie das Recht, eine Verarbeitungstätigkeit zu verbieten.

[4] https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2020/20_BfDI-zu-PDSG.html#:~:text=Der%20Bundesbeauftragte%20f%C3%BCr%20den%20Datenschutz,wird%20aufsichtsrechtliche%20Ma%C3%9Fnahmen%20gegen%20die, zuletzt abgerufen am 09.11.2020.

[5] https://www.medical-tribune.de/praxis-und-wirtschaft/praxismanagement/artikel/bundesdatenschuetzer-schickt-warnung-an-krankenkassen-elektronische-patientenakte-nicht-dsgvo-konfor/

Kontakt für weitere Informationen

Maximilian Dachlauer
Rechtsanwalt, zertifizierter Datenschutzbeauftragter
T +49 911 9193 1514
E maximilian.dachlauer@roedl.com



E-LEARNING DATENSCHUTZ

IN DER PFLEGE

Eine Datenschutzschulung speziell für Pflege-einrichtungen und ambulante Pflegedienste.

E-LEARNING DATENSCHUTZ

IN DER KITA

Eine Datenschutzschulung speziell für Kindertagesstätten.

E-LEARNING DATENSCHUTZ

IM KRANKENHAUS

Eine Datenschutzschulung speziell für Krankenhäuser.

JETZT TEST ZU GANG BEAN TRA GEN

www.roedl.de/
e-learning-datenschutz

Homeoffice in Zeiten der Pandemie

Erhöhter Handlungsbedarf im Bereich IT-Sicherheit/Informationssicherheit

von Jonas Buckel

Als im Frühjahr das Corona-Virus erstmals das gesellschaftliche Leben fest im Griff hatte, waren viele Unternehmen gezwungen, ihre Mitarbeitenden unerwartet ins Homeoffice zu schicken. Bei der Umstellung stand zunächst primär die Aufrechterhaltung der Geschäftsfähigkeit im Vordergrund und nicht die Informationssicherheit. Dabei mussten die technischen Voraussetzungen für das Remotearbeiten bei vielen Unternehmen erst geschaffen werden. Die kurzfristige Einführung führte zu fehlenden Regelungen und Sicherheitsvorkehrungen. Auch wurde oftmals auf die privaten Rechner der Mitarbeitenden zurückgegriffen. Damit gehen die Unternehmen jedoch ein erhebliches Sicherheitsrisiko ein, dem sich die meisten womöglich gar nicht bewusst sind. Die Cyberkriminellen haben sich bereits auf die neue Situation ausgerichtet und gefährden aktiv viele Unternehmen. Doch konnte Ihr Unternehmen die IT-Sicherheit im Homeoffice ausreichend in den vergangenen Monaten aufrüsten?

STATUS QUO UND AUSBLICK

Knapp 6 Monate nach dem Ausbruch der Pandemie sehen sich Unternehmen wieder mit der gleichen Problematik konfrontiert. Waren die meisten Mitarbeiter gerade erst wieder ihrem geregelten Alltag im Büro nachgegangen, wurde aufgrund der steigenden Infektionszahlen erneut zunehmend auf Homeoffice umgestellt. Auch in solch einer Krisensituation sollten grundlegende Vorgaben zur IT-Sicherheit und Datenschutz nicht vernachlässigt werden. Diese außergewöhnlichen Umstände verlangen von Unternehmen eine schnelle und sichere Umsetzung von qualifizierten Maßnahmen. Das Bundesamt für Sicherheit und Informationstechnik (BSI) bestätigte jedoch in einer Meldung, dass in Sachen IT-Sicherheit, insbesondere Cyber-Sicherheitsstrategien, bei etlichen Unternehmen weiterhin Nachholbedarf besteht.

POTENZIELLE GEFAHREN IM HOMEOFFICE

Gefahren, die sich bei der Heimarbeit ergeben können, sind primär auf fehlende bzw. unzureichende Regelungen zurückzuführen. Eine in diesem Zusammenhang ausreichende Sensibilisierung der Mitarbeiter für das Arbeiten von Zuhause fehlt oftmals.

Wenn die Telearbeit nur unzureichend durchdacht ist, können für Unternehmen verschiedenste Risiken im Hinblick auf die Informationssicherheit entstehen. Der größte Schaden, der ein Unternehmen beeinträchtigt, ist, dass unternehmensinterne Informationen nach außen getragen werden.

Neben der Cyber-Sicherheit von Computersystemen und Netzwerken ist der Faktor „Mensch“ ebenso wichtig. Beim Social Engineering können Mitarbeiter gezielt durch psychologische Tricks manipuliert werden, um kriminelle Absichten zu verwirklichen. Das zentrale Merkmal solcher Angriffe besteht vor allem in der Täuschung über die Identität. Je nach Position entstehen dem Unternehmen durch Social Engineering erhebliche Schäden. Die Absichten der Angreifer variieren dabei stark. Oftmals betrifft es jedoch auch dabei die Weitergabe sensibler Informationen.

Die wohl bekannteste Form ist das sogenannte „Phishing“. Dabei wird versucht, das Opfer zur Preisgabe vertraulicher Informationen zu verleiten. Mit sehr echt wirkenden E-Mails sollen Opfer dazu gebracht werden, Anmeldeinformationen und Passwörter auf gefälschten Zielseiten einzugeben, die im Anschluss abgegriffen werden. Daher ist es wichtig, verantwortungsvoll mit Informationen umzugehen, bei E-Mails von unbekannten Absendern Vorsicht walten lassen und sich im Zweifelsfall über die Legitimität zu informieren.

Durch die plötzliche Umstellung haben viele Unternehmen nach der Devise „Use your own device“ gehandelt. Doch das birgt reichlich Gefahren. Neben dem Verlust der Kontrolle über den Schutz unternehmensinterner Informationen, stellen auch fehlende Virenschutzprogramme und nicht durchgeführte Updates ein weiteres Sicherheitsrisiko dar. Daher ist dieses Vorgehen aus sicherheitstechnischer Sicht sehr bedenklich.

Das BSI weist an dieser Stelle in seinem Lagebericht „Die Lage der IT-Sicherheit in Deutschland 2020“ darauf hin, dass die IT-Sicherheit zugunsten eines ad hoc funktionierenden Homeoffices oftmals vernachlässigt wurde.

HANDLUNGSEMPFEHLUNGEN

Für das Arbeiten von Zuhause müssen technische und organisatorische Maßnahmen (TOMs) entwickelt werden, sodass ein möglichst sicheres und reibungsloses Arbeiten sichergestellt wird. Laut BSI muss gewährleistet sein, dass sicherheitstechnische Anforderungen getroffen werden. Insbesondere müssen Zugriffsrechte und Berechtigungen geregelt sein. Daher sollte ein Sicherheitskonzept entwickelt werden, sodass Sicherheitsanforderungen, Schutzziele und auch Risiken eindeutig identifiziert und definiert werden. Des Weiteren muss im Rahmen der Kommunikationsmöglichkeit geregelt werden, welche Endgeräte (Firmenrechner, Laptop, Smartphones) zur Heimarbeit genutzt werden und in welchem Umfang diese für private Zwecke verwendet werden dürfen.

In diesem Zuge hat das BSI folgende grundlegende Empfehlungen für das Arbeiten im Homeoffice ausgesprochen:

- Verbindliche Regelungen zur IT-Sicherheit sind schriftlich zu kommunizieren.
- Mitarbeiter müssen an ihrem Heimarbeitsplatz zwingend das Sicherheitsniveau sicherstellen, das mit dem eines Büroraumes vergleichbar ist. Dritten soll kein Zugriff gewährt werden.
- Für eine eindeutige Verifizierung sollten die Kommunikationswege genau definiert sein.
- Daher ist es auch unbedingt notwendig, Mitarbeiter bezüglich Phishing zu sensibilisieren. Cyber-Kriminelle nutzen die aktuelle Situation vermehrt aus und versuchen mit Phishing-Mails Zugriff auf sensible Daten zu erlangen.
- Auf interne Ressourcen des Unternehmens sollte nur mittels eines sicheren Kommunikationskanals, bspw. VPN, zugegriffen werden. Sofern noch keine sichere VPN-Infrastruktur besteht, bedarf es hierfür einer geeigneten Lösung.

WHITEPAPER – WOHLVERHALTENSREGELN

Grundsätzlich sollten die eigenen Mitarbeiter auf die möglichen Gefahren und das IT-Verhalten im Homeoffice ausreichend hingewiesen werden. Hierfür kann beispielsweise die folgende Rundmail verwendet werden:

Liebe Kolleginnen und Kollegen,

aus gegebenem Anlass möchten wir auf die folgenden IT-Verhaltensregeln hinweisen, die bei der Arbeit im Homeoffice zu berücksichtigen sind:

1. Einen sicheren Arbeitsplatz schaffen

Die Grundlage ist ein stabiler Netzanschluss über das sichere LAN oder das passwortgeschützte WLAN im Homeoffice. Sofern möglich, immer mittels VPN auf das Firmennetzwerk zugreifen.

2. Privat- und Diensthardware trennen

Es wird die Nutzung eines Firmengeräts vorausgesetzt, um sich mit den IT-Systemen im Unternehmen zu verbinden. Private Geräte wie Smartphones, USB-Sticks oder externe Festplatten dürfen nicht an den Dienstrechner angeschlossen werden. Umgekehrt dürfen Unternehmensanwendungen sowie auch -daten im Homeoffice nicht auf einem privaten Gerät installiert und genutzt werden.

3. Sichere Anwendungen wählen

Bei der Arbeit im Homeoffice sollten immer die bereitgestellten Sicherheitssysteme wie VPN-Client benutzt werden. Software für Privatanwender dürfen nicht dienstlich und auf Dienstgeräten genutzt werden. Viele Datentransfer- und Konferenzdienste für Privatpersonen erfüllen nicht die Mindestanforderungen an Datenschutz und IT-Sicherheit, die für unser Unternehmen erforderlich sind.

4. Vorsicht vor Phishing-E-Mails

Cyber-Kriminelle versenden zurzeit viele Phishing-Mails, die vermeintliche Neuigkeiten zur Corona-Krise enthalten. So groß das Interesse auch ist, lieber zweimal die Absenderadresse und den Inhalt jeder E-Mail prüfen. Im Zweifelsfall nicht auf Links klicken und keine Anhänge öffnen sowie den zuständigen IT-Support kontaktieren.

5. Internet Security im Homeoffice

Ihr zugeordneter Firmenrechner /-laptop darf nur durch Sie persönlich genutzt sowie Passwörter niemals an Familienmitglieder, Freunde oder Arbeitskollegen weitergegeben werden. Ihr persönlicher Rechner sollte außerdem sofort gesperrt werden, sobald Sie den Arbeitsplatz verlassen.

Wen kann ich bei Fragen erreichen?

Sollten Sie Fragen haben, erreichen Sie den Service Desk rund um die Uhr.

- per E-Mail an it-support@beispiel.de
- oder telefonisch unter +49 XXX XXXX

Mit freundlichen Grüßen

Bei der Umsetzung von technischen und organisatorischen Maßnahmen (TOM) ist es oftmals hilfreich, einen externen Berater zu haben, der bei der Umsetzung der Handlungsempfehlungen des BSI unterstützt, z. B. bei der Erstellung von Informationssicherheitsrichtlinien und Sicherheitskonzepten.

Hilfreich ist auch ein E-Learning IT-Sicherheit, denn die größte Schwachstelle von IT-Systemen ist oftmals nicht die Technik, sondern der Mensch, da gezielte Angriffe auf einzelne Mitarbeiter von Virenschutzprogrammen nicht erkannt werden können. Daher gilt der Mensch als Schlüsselfaktor beim Thema IT-Sicherheit. Die Durchführung der Online-Schulung richtet sich grundsätzlich an alle Mitarbeiter und dient der Sensibilisierung im Umgang mit Informationstechnik.

Sperren Sie den Rechner bei Abwesenheit: ⊞ + L

Verzichten Sie soweit es Ihnen möglich ist auf die Druckfunktion.

Papierunterlagen dürfen nicht mit dem Hausmüll entsorgt werden.

Fahren Sie Ihr System (z. B. Laptop) nach der Arbeit herunter.

Achten Sie auf Clean Desk : Unbefugte dürfen keinen Einblick in vertrauliche Unterlagen erhalten.

Verzichten Sie auf die Verwendung von privaten Datenträgern (z.B. externe)

Unterwegs : Nutzen Sie eine Sichtschutzfolie für Ihren Laptop.

CYBER SECURITY CHECK

Ein erfolgreicher Hackerangriff kann zu verheerenden Folgen für das gesamte Unternehmen führen. Um nicht Opfer von Cyberattacken zu werden, muss die Bedrohungslage aus dem Cyber-Raum ernst genommen und aktiv mit wirksamen Gegenmaßnahmen bekämpft werden.

Ein Cyber-Sicherheits-Check bietet eine praxisorientierte Beurteilung der IT-Sicherheit. Die Prüfung soll einen Überblick über den Status der Cyber-Sicherheit geben und die Verantwortlichen anhand konkreter Empfehlungen dabei unterstützen, festgestellte Sicherheitsmängel abzustellen.

EXTERNER INFORMATIONSSICHERHEITSBEAUFTRAGTER (ISB)

Das Thema Informationssicherheit gewinnt immer stärker an Bedeutung. Im gleichen Maße wie die Bedeutung zunehmend erkannt wird, sinkt die Verfügbarkeit geeigneter Mitarbeiter für die Stelle des Informationssicherheitsbeauftragten auf dem Arbeitsmarkt. Eine Option ist es daher, einen externen Mitarbeiter als Informationssicherheitsbeauftragten zu bestellen.

ABSCHLIESSENDES RESÜMEE

Die derzeitigen Umstände verlangen ein besonders stabiles IT-Umfeld. Schwachstellen in der IT-Sicherheit eines Unternehmens sollten schnellstmöglich beseitigt werden. Hierfür liefert das BSI zahlreiche Handlungsempfehlungen und Hilfestellungen.

Arbeiten im Homeoffice ist ein Modell der Zukunft und wird auch nach der Corona-Pandemie weiter auf dem Vormarsch sein. Unternehmen sollten daher bereits jetzt grundlegende Strukturen schaffen, um das Arbeiten von Zuhause aus sicher und effizient zu gestalten. Hieraus können sich Chancen und Herausforderungen ergeben, auf die man vorbereitet sein muss.

Wir helfen Ihnen, Risiken präventiv zu vermeiden und können Sie bei der Entwicklung und Umsetzung von geeigneten Maßnahmen mit unserem Fachwissen unterstützen!

Kontakt für weitere Informationen

Jonas Buckel
B.A. Wirtschaftsinformatik,
IT-Auditor IDW
T +49 911 9193 3627
E jonas.buckel@roedl.com

→ Rechtsberatung

Umsatzsteuerbefreiung bei Laborleistungen auch ohne „Vertrauensbeziehung“

von Sebastian Heinke LL.M. und Simone Müller

Zur Bekämpfung der Corona-Pandemie werden in Deutschland derzeit Corona-Tests in großem Umfang durchgeführt. In der 44. Kalenderwoche bestand eine Testkapazität von 1,6 Millionen Tests pro Woche.

Vor diesem Hintergrund stellt sich die Frage, wie die Auswertung und Durchführung der Corona-Tests durch ein von dem anordnenden Arzt unabhängiges Drittlabor umsatzsteuerrechtlich zu bewerten ist.

Nach § 4 Nr. 14 Buchst. a S. 1 UStG sind „Heilbehandlungen im Bereich der Humanmedizin, die im Rahmen der Ausübung der Tätigkeit als Arzt, Zahnarzt, Heilpraktiker, Physiotherapeut, Hebamme oder einer ähnlichen heilberuflichen Tätigkeit durchgeführt werden“, von der Umsatzsteuer (i. S. v. § 1 Abs. 1 Nr. 1 UStG) befreit.

Der Bundesfinanzhof hat in seinem Urteil vom 22.1.2020 entschieden (XI R 24/19), dass die Umsatz-steuerbefreiung nach § 4 Nr. 14 Buchst. a S. 1 UStG auch bei einer entsprechenden beruflichen Qualifikation eines Gesellschafters einer GbR für Laborleistungen und bei der Erbringung der Leistungen für externe Ärzte und Kliniken zu gewähren ist. Ein Vertrauensverhältnis zwischen Arzt und Patient muss folglich für die Steuerbefreiung im Rahmen einer Heilbehandlung i. S. v. § 4 Nr. 14 Buchst. a S. 1 UStG nicht bestehen.

Entsprechendes muss auch bei der Auswertung von Corona-Tests durch ein Drittlabor gelten.

SACHVERHALT DES BFH-URTEILS

Die Klägerin, eine ärztliche Gemeinschaftspraxis (GbR), die vorwiegend im Bereich Dermatologie tätig ist, betreibt ein eigenes Labor zur Analyse und Befundung von Gewebeproben, verfügt aber über keine eigene vertragsärztliche Zulassung. Die Laboruntersuchungen werden aufgrund ärztlicher Anordnung durchgeführt und dienen der Erkennung von Krankheiten.

Die Beauftragung erfolgt durch eigene (Privat-)Patienten, aber auch durch externe niedergelassene oder privatärztlich tätige Ärzte sowie Kliniken. Die Durchführung der Analysen und der Befundung erfolgt durch die Gesellschafter persönlich. Alle Gesellschafter verfügen über eine fachärztliche Ausbildung mit entsprechender Zusatzausbildung.

Hinsichtlich der Leistungserbringung für die eigenen Patienten bestand Einvernehmen zwischen Klägerin und Finanzamt dahingehend, dass die Laborleistung als unselbstständige Nebenleistung zu der eigentlichen Behandlung (Heilbehandlung) diene und diese der Umsatzsteuerbefreiung nach § 4 Nr. 14 Buchst. a S. 1 UStG unterliege.

Die Klägerin war der Annahme, dass diese Befreiung ebenfalls für die extern erbrachten Laborleistungen gelte und erklärte die Umsätze entsprechend gegenüber ihrem Finanzamt.

Das Finanzamt erkannte die Befreiung für die extern erbrachten Laborleistungen nicht an und begründete dies mit der Auffassung, dass die erbrachten Laborleistungen wegen fehlendem persönlichen Vertrauensverhältnis zwischen den Ärzten (Klägerin) und den Patienten nicht als Nebenleistung unter die Befreiung gem. § 4 Nr. 14 Buchst. a S. 1 UStG fallen würde.

Gegen den letztendlich ergangenen Einspruchsbescheid seitens des Finanzamts erhob die Klägerin Klage beim Finanzgericht (FG) Hamburg, und hatte Erfolg (Urteil vom 29.8.2017; 2 K 221/15).

Der BFH als Revisionsgericht hat das Verfahren nach dessen Aussetzung bis zum Ergehen einer Entscheidung durch den Europäischen Gerichtshof (Peters-Urteil vom 18.9.2019; C-700/17) wieder aufgenommen und entschieden.

ENTSCHEIDUNGSGRÜNDE DES BFHs

In diesem Zusammenhang hat das BFH geurteilt, dass die Voraussetzungen der Umsatzsteuerbefreiung gem. § 4 Nr. 14 Buchst. a S. 1 UStG auch ohne das direkte „Vertrauensverhältnis“ zum Patienten erfüllt seien.

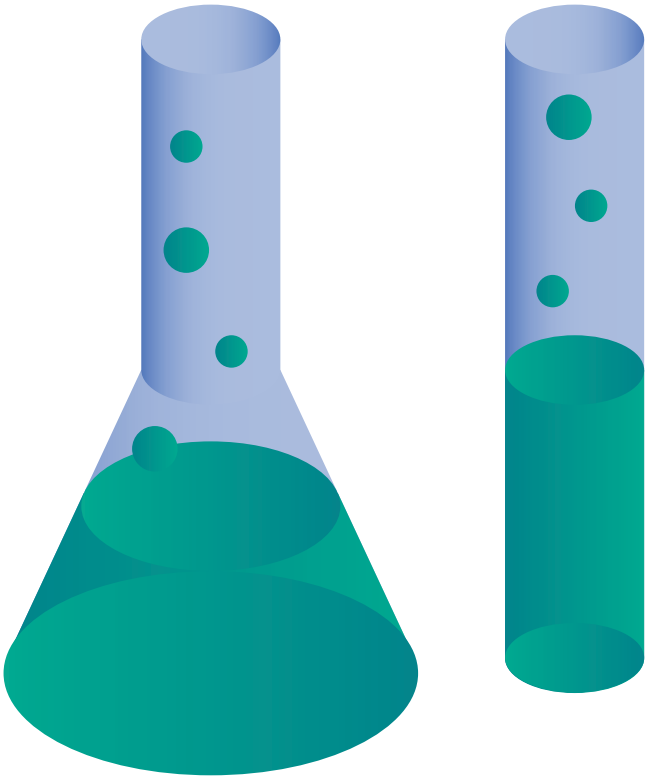
§ 4 Nr. 14 Buchst. a S. 1 UStG beruhe auf Art. 132 Abs. 1 lit. c) MwStSystRL. Der EuGH hatte in seinem Urteil in der Rechtssache Peters bereits entschieden, dass die Steuerbefreiung der Heilbehandlungen gem. Art. 132 Abs. 1 Buchst. c MwStSystRL nicht vom Vorliegen eines Vertrauensverhältnisses zwischen der behandelnden und der behandelten Person abhängen würde.

Es würde gegen den Grundsatz der steuerlichen Neutralität verstoßen, wenn abhängig vom Ort der Leistung eine andere Mehrwertsteuerregelung gelten würde, obwohl ihre Qualität angesichts der Ausbildung der betreffenden Dienstleistungserbringer gleichwertig ist.

Der EuGH hatte in einem seiner Leitsätze (Peters-Urteil vom 18.9.2019; C-700/17) ausdrücklich erklärt, dass die „Befreiung von der Mehrwertsteuer nicht von der Voraussetzung abhängt, dass die betreffende Heilbehandlungsleistung im Rahmen eines Vertrauensverhältnisses zwischen dem Patienten und dem Behandelnden erbracht wird“.

Die weiteren Tatbestandvoraussetzungen des § 4 Nr. 14 Buchst. a S. 1 UStG seien ebenfalls erfüllt.

So wurden die Laborleistungen im Zuge der Heilbehandlung im Rahmen der Ausübung der Tätigkeit als Arzt vorgenommen. Dabei sei auch unerheblich, dass die Gewebeproben vom nichtärztlichen Laborpersonal präpariert wurden. Es sei nicht erforderlich, dass jeder Schritt einer therapeutischen Behandlung von ärztlichem Personal durchgeführt wird. Die entscheidenden Arbeitsschritte der Untersuchung und der Befundung wurden bei der Klägerin von den Fachärzten vorgenommen, sodass insoweit die Tatbestandsvoraussetzungen ohne weitere Zweifel erfüllt waren.



ÜBERTRAGBARKEIT AUF DIE DURCHFÜHRUNG VON CORONA-TESTS

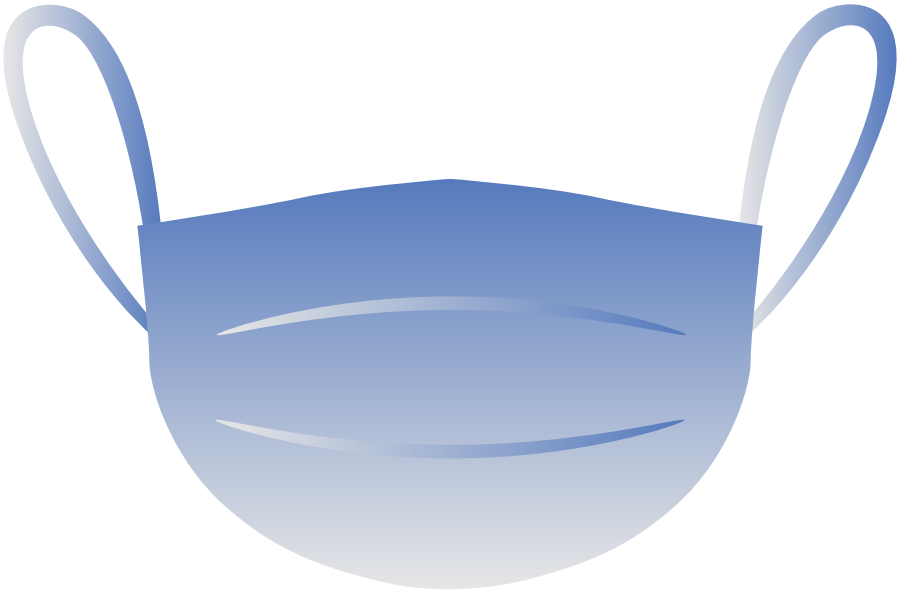
Die vorstehende Entscheidung ist unserer Auflassung nach auf die externe Durchführung und Auswertung von Corona-Tests (Laborleistungen) übertragbar. Auch in dieser Konstellation dürfte es regelmäßig am Vertrauensverhältnis zwischen Arzt und Labor fehlen. Dies ist nach der Rechtsprechung des EuGHs und BFHs jedoch unerheblich, weshalb die Umsatzsteuerbefreiung gem. § 4 Nr. 14 Buchst. a S. 1 UStG zur Anwendung kommen muss.

Aufgrund der stark steigenden Zahl der Covid-19-Erkrankten ist es in der Praxis schon nicht möglich, dass Arztpraxen und Kliniken die Corona-Tests innerhalb ihrer eigenen Labore durchführen. Die Laborleistung muss zur effektiven Testung der Infizierten zwangläufig auch in Drittlaboren erfolgen.

PRAXISHINWEISE

Entgegen der Entscheidung des BFHs vertritt die Finanzverwaltung weiterhin eine abweichende Auffassung. Im Abschnitt 4.14.1. Abs. 1 S. 2 des Umsatzsteueranwendungserlasses (UStAE; Stand 1.10.2020) verlangt diese für die Steuerbefreiung weiterhin ein Vertrauensverhältnis zwischen Patient und Behandelndem. In Abgrenzung zu § 4 Nr. 14 Buchst. b UStG sei § 4 Nr. 14 Buchstabe a UStG auf Leistungen anzuwenden, die außerhalb von Krankenhäusern oder ähnlichen Einrichtungen im Rahmen eines persönlichen Vertrauensverhältnisses zwischen Patienten und Behandelndem, z. B. in Praxisräumen des Behandelnden, in der Wohnung des Patienten oder an einem anderen Ort erbracht werden. Dabei beruft sich die Finanzverwaltung auf das EuGH-Urteil vom 6.11.2003, C-45/01, Dornier.

Es sind in dieser Hinsicht also weitere Konflikte mit den Finanzämtern zu erwarten. Bei Fragen zur umsatzsteuerrechtlichen Behandlung von Laborleistungen beraten wir Sie gern.



Kontakt für weitere Informationen

Sebastian Heinke, LL.M.
Rechtsanwalt
T +49 221 949 909 146
E sebastian.heinke@roedl.com

Simone Müller
M.A. Medizinmanagement
T +49 221 949 909 434
E simone.mueller@roedl.com

→ Rechtsberatung

Die Reform des Stiftungsrechts

von Jan-Claas Hille und Simone Müller

Für die Neuregelung des deutschen Stiftungsrechts liegt ein Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) vor. Aufgrund der derzeitigen Rahmenbedingungen, wie wachsende Bürokratie, Rechtsunsicherheit infolge unterschiedlicher bundes- und landesrechtlicher Regelungen und Niedrigzinsen, wird die Verwirklichung der Stiftungszwecke erschwert. Mit dem Referentenentwurf am 28.9.2020 wurde ein Versuch zur Vereinheitlichung des Stiftungsrechts, basierend auf dem Diskussionsentwurf der Bund-Länder-Arbeitsgruppe „Stiftungsrecht" aus 2018, vorgelegt.

Der Entwurf sieht insbesondere bundeseinheitliche Regelungen für Stiftungen in den §§ 80 ff. BGB u. a. zu Namen, Sitz und Vermögen der Stiftung, zu Rechten und Pflichten der Organmitglieder, zur Änderung der Stiftungssatzung sowie zur Beendigung, u. a. zur Zulegung und Zusammenlegung von Stiftungen vor.

STIFTUNGSREGISTER UND NAMENSZUSATZ SOWIE WEGFALL DES TRANSPARENZREGISTERS

Mit der Stiftungsreform soll einheitlich analog zu dem Vereins- und Handelsregister nun auch ein Stiftungsregister mit Publizitätswirkung eingeführt werden. Mit einer Übergangsfrist von 3 Jahren soll für alle Stiftungen eine verpflichtende Eintragung gelten. Dies gilt sowohl für bestehende Stiftungen, als auch für Stiftungen, die zukünftig gegründet werden. Wesentliche Inhalte des Registers sind Angaben über die vertretungsberechtigten Organe und deren Vertretungsbefugnis sowie Name, Sitz, Grundlagen- und Satzungsänderungen der Stiftung. Mit dem Stiftungsregister sollen zum einen Stiftungen transparenter dargestellt und zum anderen eine Vereinfachung des Nachweises der Vertreter hinsichtlich ihrer Berechtigungen geregelt werden. Zusätzlicher Verwaltungsaufwand entsteht für die Stiftungen nicht, da mit der Eintragung in das Stiftungsregister die Pflicht zur Mitteilung an das Transparenzregister entfällt.

Die Organisation soll zentral vom Bundesamt für Justiz in Bonn erfolgen, was zum Vorteil hätte, dass alle Informationen über alle Bundesländer hinweg über ein Register abgerufen werden können.

Weiterhin sollen die Stiftungen künftig einen Namenszusatz erhalten: e. S. für die eingetragenen Stiftungen und e. VS. für die eingetragene Verbrauchsstiftung.

STIFTUNGSVERMÖGEN

Der Referentenentwurf sieht auch grundlegende Regelungen zum Stiftungsvermögen und seiner Vermögenszusammensetzung vor. Bei Stiftungen mit Errichtung auf unbestimmte Zeit soll das dauerhaft zu erhaltene Stiftungsvermögen als Grundstockvermögen bezeichnet werden, ergänzend gilt das sonstige Vermögen. Als Grundstockvermögen wird das Dotationskapital (Errichtungskapital), Zustiftungen sowie das von der Stiftung zu Grundvermögen bestimmte Vermögen bezeichnet. Auch Umschichtungsgewinne sollen zum Grundstockvermögen gehören, es sei denn, die Stiftungssatzung sieht etwas anderes vor. Das Vermögen einer Verbrauchsstiftung besteht nur als sonstiges Vermögen. Die Stiftungen sollten daher im Einzelfall prüfen, welche Auswirkungen in ihrer Stiftungssatzung schlummern könnten.

Die Erhaltung des Grundstockvermögens soll künftig einheitlich im BGB geregelt werden. Wobei eine Konkretisierung hinsichtlich des Erhalts, ob nach dem Nominal- oder Realwert, nicht vorgesehen ist. Maßgeblich wird hierfür der Stifterwille zur Zeit der Errichtung der Stiftung sein. Damit entfallen die Einzelregelungen der Bundesländer, die zum Teil einen realen Kapitalerhalt vorgesehen haben. Ansonsten dürften sich für die Stiftungen keine Änderungen ergeben: Waren die Stiftungen bislang über den Stifterwillen zum realen Kapitalerhalt verpflichtet, sind sie es nach der neuen Gesetzeslage immer noch. Allerdings könnte die gesetzliche Regelung zum Anlass genommen werden, den Stifterwillen nochmals zu erforschen.

GRUNDLAGEN DER HAFTUNG VON STIFTUNGSORGANEN

Bereits im Diskussionsentwurf wurde die aus dem Aktienrecht entlehnte und von der stiftungsrechtlichen Rechtsprechung übernommene Business Judgement Rule vorgeschlagen und in den Referentenentwurf übernommen. Wenn das Stiftungsorgan unter Beachtung gesetzlicher und satzungsmäßiger Vorgaben vernünftigerweise annehmen durfte, auf der Grundlage angemessener Informationen zum Wohle der Stiftung zu handeln, stellt es gem. § 84a Abs. 3 S. 2 BGB-RE kein pflichtwidriges Verhalten dar.

Eine satzungsmäßige Beschränkung der Haftung auf Vorsatz und grobe Fahrlässigkeit soll künftig nur noch in der Errichtungssatzung durch den Stifter selbst vorgesehen werden können, § 84a Abs. 3 S. 3 BGB-RE. Somit wird sie für die bereits bestehenden Stiftungen weniger Relevanz haben.

SATZUNGS- UND GRUNDLAGENÄNDERUNGEN

Voraussetzungen für Satzungsänderungen durch die Stiftungsorgane sind künftig in § 85 BGB-RE geregelt. Hier wurde der gestufte Ermächtigungskatalog des Diskussionsentwurfs in die § 85 ff. BGB-RE übernommen. D. h. je umfangreicher eine Satzungsänderung in das Wesen der Stiftung eingreift und damit eine Veränderung der Stiftung einhergeht, desto strenger sind die Voraussetzungen für die Satzungsänderungen.

Der Referentenentwurf sieht ebenfalls umfangreiche Regelungen für die Zulegung und Zusammenlegung von Stiftungen samt angeordneter Gesamtrechtsnachfolge vor. Dies kommt vor allem notleidenden Stiftungen zugute. Die Zulegung oder Zusammenlegung soll künftig als eigenständige Möglichkeit zur Vermögensübertragung dienen. Dies ist für Stiftungen relevant, wenn von wesentlichen Änderungen in den Verhältnissen auszugehen ist und eine Satzungsänderung nicht ausreichend ist.

FAZIT

Mit der Vereinheitlichung des Stiftungsrechts wird eine Erhöhung der Rechtssicherheit geschaffen und die Attraktivität der Rechtsform Stiftung erhöht. Mit einem Stiftungsregister kann frühestens Anfang 2024 gerechnet werden, vorausgesetzt, das Gesetzgebungsverfahren wird noch in diesem Jahr abgeschlossen. Ratsam für bestehende Stiftungen ist die Überprüfung ihrer derzeitigen Satzungsregelungen, ob und welche Änderungen sich für sie eventuell ergeben und die Satzung noch vor Inkrafttreten der Reform entsprechend geändert werden sollte. Die Klarstellung hinsichtlich der Frage des Kapitalerhalts ist erfreulich und schafft kurzfristig Bewegungsfreiheit. An der grundlegenden Frage der ausreichenden Kapitalausstattung ändert sich jedoch nichts. Im Rahmen des Niedrigzinsumfelds kommen neben alternativen und risikoreicheren Anlageformen nur die regelmäßige Einwerbung von neuen Mitteln in Frage. Inwieweit sich vermehrt Stiftungen zusammenschließen bleibt abzuwarten, da die Stiftungszwecke im Detail doch sehr heterogen sind.

Kontakt für weitere Informationen

Jan-Claas Hille
Dipl.-Kaufmann, Wirtschaftsprüfer, Steuerberater
T +49 221 949 909 432
E jan.claas-hille@roedl.com

Simone Müller
M.A. Medizinmanagement
T +49 221 949 909 434
E simone.mueller@roedl.com

Rödl & Partner

Impressum

Verantwortlich für redaktionelle Inhalte gemäß § 55 Abs. 2 RStV:
Prof. Dr. Christian Rödl
Äußere Sulzbacher Straße 100
90491 Nürnberg

Rödl GmbH Rechtsanwaltsgesellschaft Steuerberatungsgesellschaft
Wirtschaftsprüfungsgesellschaft
Äußere Sulzbacher Straße 100
90491 Nürnberg
Deutschland / Germany

Tel: +49 911 9193 0
Fax: +49 911 9193 1900
E-Mail: info@roedl.de
www.roedl.de

einzelvertretungsberechtigter Geschäftsführer:
Prof. Dr. Christian Rödl, LL.M., RA, StB