Rödl & Partner

FOKUS GESUNDHEITS- UND SOZIALWIRTSCHAFT

Ausgabe: OKTO-BER 2021

Informationen für Entscheider von Krankenhäusern, Pflegeeinrichtungen, Wohlfahrtsverbänden und Hochschulen

Liebe Leserin, lieber Leser

in der aktuellen Ausgabe unseres Fokus Gesundheits- und Sozialwirtschaft haben wir wieder Neuigkeiten und Eindrücke aus verschiedensten Bereichen für Sie zusammengestellt.

Das Pflegebudget befindet sich in einem ständigen Wandel. Wir erläutern in dieser Ausgabe, welche wichtigen Änderungen sich durch das am 20.7.21 in Kraft getretene Gesundheitsversorgungsweiterentwicklungsgesetz ergeben und stellen dazu verschiedene Sachverhalte dar.

Um die Digitalisierung des Gesundheitswesens in Deutschland voranzutreiben, wurde das Patientendatenschutzgesetz (PDSG) im Herbst letzten Jahres verabschiedet. Was dies für Krankenhäuser bedeutet, lesen Sie im Kapitel Datenschutz. Nicht nur das PDSG bringt Herausforderungen mit sich, auch Cloudlösungen wie Microsoft 365 können Schwierigkeiten bereiten. Erfahren Sie worauf Sie achten müssen, wenn Sie ein solches System nutzen.

Die Verfahrensdokumentation ist verpflichtend für jedes Unternehmen in Deutschland. Jedoch wird sie oft nur als Notwendigkeit gesehen und deren Bedeutung außer Acht gelassen. Wir zeigen Ihnen in dieser Ausgabe Chancen und Risiken auf, die mit dem verkannten Thema in Verbindung stehen.

Den Abschluss dieser Fokus-Ausgabe bildet der zweite Teil der Reihe „Ein Tax Compliance Management System ist mehr als ein paar Checklisten“. In diesem wird die Umsetzung und die damit potenziell auftretenden Probleme eines Tax CMS in der Praxis betrachtet.

MARTIN WAMBACH
Geschäftsführender Partner

NORMAN LENGER-BAUCHOWITZ, LL.M.
Partner

Ab 2022 erscheint unser Newsletter nur noch digital. Mehr Informationen finden Sie auf der letzten Seite.

→ Wirtschaftsprüfung

Pflegebudget

Aktuelle Änderungen und Hinweise

von Tino Schwabe und Christiane Kraus

Die Rahmenbedingungen zur Ermittlung des Pflegebudgets ändern sich stetig. Neben klärenden Schiedsstellenentscheiden hat sich nun auch der Gesetzgeber des Themas noch einmal angenommen und mit dem Gesundheitsversorgungsweiterentwicklungsgesetz einige gravierende Änderungen auf den Weg gebracht. Wir stellen Ihnen die wichtigsten Änderungen sowie weitere wichtige Sachverhalte im folgenden Text dar.

Das Pflegebudget ist seit seiner Einführung in einem ständigen Wandel. Nun trat als neueste Änderung das Gesetz zur Weiterentwicklung der Gesundheitsversorgung (Gesundheitsversorgungsweiterentwicklungsgesetz – GVWG) am 20.7.2021 in Kraft. Dieses Gesetz hat neben weiteren Thematiken auch die Anpassung des Pflegebudgets im Blick. Soweit noch keine Vereinbarung für das Jahr 2020 zwischen dem Krankenhausträger und den Kostenträgern bis zum 20.7.2021 erfolgte, gelten die Änderungen des GVWGs auch rückwirkend für das Pflegebudget 2020.

Konkret werden folgende Regelungen durch das GVWG getroffen:

1. NUTZUNG DER ANLAGEN DER ZWEITEN ÄNDERUNGSVEREINBARUNG

Die Anwendung der aktuellen Anlagen ist somit keine Empfehlung mehr, sondern, sollte noch keine Vereinbarung vorliegen, auch für das Jahr 2020 verbindlich anzuwenden. In diesen Anlagen werden die Rubriken „Sonstige Berufe“ und „Ohne Berufsausbildung“ detaillierter behandelt. Somit fallen aus diesen Rubriken die Medizinischen Fachangestellten, anästhesietechnischen Assistenten, Notfallsanitäter sowie Pflege- und Sozialassistenten und können vollständig angesetzt werden, solange diese Berufsgruppen typisch pflegerische Tätigkeiten erbringen.

2. ANSATZ DER GESAMTEN PFLEGEVOLLKRÄFTE UND PFLEGEPERSONALKOSTEN

Nach § 6a Abs. 3 Nr. 1 und 2 KHEntgG sind nun die jahresdurchschnittliche Stellenbesetzung der Pflegevollkräfte sowie die Pflegepersonalkosten insgesamt, gegliedert nach Berufsbezeichnungen, anzugeben. Dies bedeutet, dass keine Nebenrechnungen vorab auf Basis von Kostenstellen durchgeführt werden dürfen. Es sind somit alle Abzugspositionen, die das jeweilige Haus betreffen, in den dafür vorgesehenen Positionen zu befüllen. Eine Abgrenzung des Personals, das nicht im Anwendungsbereich des KHEntgGs tätig ist, erfolgt erst durch den Eintrag in den Zeilen 7 ff der Anlage.

3. AUSWEIS DER ANERKENNUNGSPRAKTIKANTEN

Ausländische Pflegekräfte, die sich in der Anerkennungsphase nach dem Fachkräfteeinwanderungsgesetz befinden, sind nicht in der Rubrik „ohne Berufsabschluss“ anzusetzen, sondern entsprechend der behördlichen Bestätigung in der jeweiligen Berufsgruppe zu berücksichtigen. Sie werden dann in der Anlage der pflegebudgetrelevanten Kosten als Davon-Position der jeweiligen Berufsgruppe ausgewiesen.

4. DARLEGUNG ZUR ABGRENZUNG VON ERSTATTUNGEN UND ZULAGEN

Unter der neu hinzugefügten Abzugsposition „Sonstiges“ sind ausschließlich folgende Erträge und Erstattungen anzusetzen:

- erhaltene Erträge und Erstattungen von Dritten, wie Mutterschutz (U 2-Verfahren),
- berufliche Eingliederung,
- Kurzarbeitergeld,
- Quarantänemaßnahmen nach § 56 Infektionsschutzgesetz,
- Corona-Prämie für Pflegekräfte nach § 26a und § 26d KHG,
- Erstattungen durch die Vereinbarkeit von Pflege, Familie und Beruf nach § 4 Abs. 8a KHEntgG,
- Hygieneförderprogramm nach § 4 Abs. 9 KHEntgG sowie
- außertarifliche Tatbestände (bspw. Poolgelder).

5. 2018ER-REFERENZ

In Absatz 2 des § 6a KHEntgG wurde nun auch die 2018er-Referenz des Personals mit sonstigen Berufen und ohne Berufsabschlüsse gesetzlich verankert. Es ist somit die Anzahl der Vollkräfte ohne pflegerische Qualifikation des Jahres 2018 zugrundezulegen. Der Ansatz von pflegebudgetrelevantem Personal darüber hinaus ist nicht mehr zulässig.

6. PRÜFUNG DER ENTFALLENDEN ERLÖSE DES KRANKENHAUSES AUS DEN TAGESBEZOGENEN PFLEGEENTGELTEN

Es ist nun auch das vereinnahmte Pflegebudget zu testieren. Die auf das Vereinbarungsjahr entfallenden Erlöse des Krankenhauses aus den tagesbezogenen Pflegeentgelten nach § 7 Abs. 1 Satz 1 Nr. 6a KHEntgG sind vom Jahresabschlussprüfer zu prüfen. Es ist künftig dabei zu beachten, dass das jährliche Testat sich nicht nur auf ein Vereinbarungsjahr beziehen kann. Für das Geschäftsjahr 2021 werden mindestens 2 Jahre und für das Jahr 2022 wahrscheinlich sogar 3 Jahre zu testieren sein, da die meisten Krankenhäuser ihr Pflegebudget 2020 nicht bis zum Jahresende 2021 vereinnahmt haben werden. Dabei sind die Pflegeentgeltwerte nach ihren Budgetjahren zu differenzieren. Es muss daher die Möglichkeit geschaffen werden, die Pflegebewertungsrelationen nach genauen Zeiträumen auswerten zu können.

7. DOKUMENTATION

Zur Weiterentwicklung des Entgeltsystems hat der Krankenhausträger eine Dokumentation des vereinbarten Pflegebudgets einschließlich der jahresdurchschnittlichen Stellenbesetzung der Pflegevollkräfte gegliedert nach Berufsbezeichnungen aufzustellen. Aus dieser Dokumentation müssen die Höhe des Pflegebudgets sowie die wesentlichen Rechengrößen zur Herleitung der vereinbarten, im Pflegebudget zu berücksichtigenden Kosten (Pflegepersonalkosten, die pflegeentlastenden Maßnahmen, Ausgleiche für Mehr- und Minderkosten) und der Höhe des Pflegebudgets hervorgehen. Zur Umsetzung der neuen Dokumentationsverpflichtungen in Bezug auf das vereinbarte Pflegebudget werden die Vertragsparteien beauftragt, die bereits geschlossene Vereinbarung nach § 9 Abs. 1 Nr. 8 KHEntgG (Pflegebudgetverhandlungsvereinbarung) um weitere Regelungstatbestände zu ergänzen. Diese Dokumentationsvorgaben sind von den Vertragsparteien auf Ortsebene verbindlich zu verwenden, sobald die Vereinbarung in Kraft getreten ist.

8. VERÖFFENTLICHUNGSVERPFLICHTUNG DURCH DAS INEK

Um Transparenz herzustellen und den Vertragsparteien auf Bundesebene zu ermöglichen, ihrer Berichtspflicht nach § 17b Absatz 4 Satz 9 KHG nachzukommen, wurde die Veröffentlichungspflicht im Satz 6 des § 6a Abs. 3 KHEntgG aufgenommen. Die in den Sätzen 3 und 4 Nummer 1 bis 3 und 5 genannten Angaben des § 6a Abs. 3 KHEntgG sind krankenhausbezogen barrierefrei auf der Internetseite der InEK zu veröffentlichen. Das Krankenhaus hat dabei insbesondere die vereinbarten und die tatsächlich im Pflegebudget zu berücksichtigenden Daten zur Anzahl der Pflegevollkräfte, untergliedert nach Berufsgruppen, und der Pflegepersonalkosten in geeigneter Form zu veröffentlichen. Eine Veröffentlichung der übermittelten Dokumente ist hingegen nicht zulässig.

Für die Herleitung des Pflegebudgets 2021 sind darüber hinaus noch weitere Sachverhalte und Abzugspositionen zu beachten.

AUSSERTARIFLICHE TATBESTÄNDE

Hierunter fallen einerseits die schon refinanzierten Corona-Prämien nach § 26a und § 26d KHG. Ein besonderes Augenmerk ist hier auf die Prämie nach § 26a KHG zu legen, da einige Häuser einen Teil der Prämie aufgrund von technischen Problemen erst verspätet im Jahr 2021 ausgezahlt haben. Diese refinanzierte Auszahlung ist nun im Pflegebudget 2021 als Abzugsposition zu beachten. Ebenfalls ist die zweite Corona-Prämie nach § 26d KHG nicht im Pflegebudget anzusetzen.

Andererseits müssen auch die ausgezahlten Lohnarten auf außertarifliche Tatbestände geprüft werden. Dies beinhaltet insbesondere Prämien für das Programm „Mitarbeiter werben Mitarbeiter“, außertariflich gezahlte Zulagen, Zielvereinbarungen, Gutachtertätigkeiten und weitere freiwillig ausgezahlte Corona-Prämien etc. Die Lohnarten sind je Haus individuell zu prüfen.

ERHALTENE ERSTATTUNGEN

Insbesondere die Erstattungen für Quarantänemaßnahmen nach § 56 Infektionsschutzgesetz wurden zwar im Jahr 2020 schon beantragt, die wenigsten jedoch ausgezahlt. Da das Pflegebudget auf den Liquiditätsfluss abstellt, sind Erstattungen, die erst im Jahr 2021 für das Jahr 2020 eingehen, im Pflegebudget für das Jahr 2021 anzusetzen.

Ebenfalls müssen erhaltene Personalkostenerstattungen von den pflegebudgetrelevanten Kosten abgezogen werden, um eine Doppelfinanzierung zu vermeiden. Wurden zum Beispiel Personalkostenerstattungen zur Arbeitsförderung für Anerkennungspraktikanten nach SGB III § 81 und 82 erhalten, sind diese ebenfalls abzuziehen.

DARLEGUNG DES PFLEGERISCHEN ANTEILS

Aus den bisherigen Schiedsstellensprüchen ist ersichtlich, dass der pflegerische Anteil bestimmter Berufsgruppe substantiiert dargelegt werden muss. Dies betrifft insbesondere Berufsgruppen, die von ihrem klassischen Berufsbild primär keine pflegerischen Leistungen absolvieren, wie Physio- oder Ergotherapeuten. Es ist daher essenziell die pflegerischen Anteile detailliert mit Tätigkeitsbeschreibungen zu belegen und den Verhandlungspartnern sowie den Prüfern darzulegen.

ANSATZ DER LEIHARBEITNEHMER

Hierbei sollten die erbrachten Stunden der Leiharbeitnehmer dokumentiert werden. Eine Möglichkeit besteht darin, schon unter dem Jahr jegliche Rechnungen bei der Rechnungsprüfung in eine gesonderte Aufstellung aufzunehmen, in der die erbrachten Normalstunden sowie Zuschlagsstunden aufgelistet werden. Eine andere Option ist es, die Leiharbeitnehmer mit im Dienstplanprogramm zu führen und am Ende des Jahres die erbrachten Stunden auszuwerten. Es ist jedoch zu beachten, dass die Dienstplanverantwortlichen auch jegliche Ausfälle eintragen, um die wirklich erbrachten Stunden zu ermitteln.

Diese Stunden können sodann mit der internen Nettojahresarbeitszeit in Vollkräfte umgerechnet werden. Die Nettojahresarbeitszeit ergibt sich, indem der Ausfallfaktor des Pflegepersonals berechnet und von der Bruttojahresarbeitszeit abgezogen wird. Im Ausfallfaktor werden Urlaubs-, Krankheitstage sowie andere Ausfälle einbezogen. Ein realistischer Wert liegt für die Nettojahresarbeitszeit bei rund 1.580 Stunden.

Der Leiharbeitnehmer wird sodann entsprechend in den Haustarif eingruppiert. Der ermittelte gesamte Stundenwert, also inklusive der Zuschlagsstunden, wird mit den Bruttopersonalkosten pro Stunde ohne Zuschläge multipliziert. Die Bruttopersonalkosten ergeben sich, indem das Grundentgelt der entsprechenden Tarif- und Entwicklungsstufe mit dem Arbeitgeberanteil addiert wird.

ABGRENZUNG VON ERSTATTUNGEN DURCH DIE DEUTSCHE STIFTUNG FÜR ORGANSPENDE

Des Weiteren ist zu beachten, dass bei den Erstattungen der Deutschen Stiftung für Organtransplantation geringe Anteile für pflegerische Leistungen erstattet werden können. Sollten somit Transplantationen durchgeführt und pflegerische Leistungen durch die Deutsche Stiftung für Organtransplantation erstattet worden sein, sind diese von den pflegebudgetrelevanten Kosten abzuziehen, um eine Doppelfinanzierung zu vermeiden.

FESTLEGUNGEN GEMÄSS § 6A ABS. 3 SATZ 7 KHENTGG

Die InEK hat Anfang September 2021 mit dem Spitzenverband Bund der Krankenkassen Maßnahmen im Fall einer nicht fristgerechten Vorlage der Bestätigung des Jahresabschlussprüfers festgelegt. Dabei liegt ein Versäumnis vor, wenn die Daten nicht fristgerecht an die InEK übermittelt werden. Eine Datenübermittlung gilt als nicht fristgerecht, wenn keine Daten, unvollständige Daten oder objektiv falsche Daten übermittelt worden sind. Von unvollständigen Daten spricht man, wenn das Testat vom Jahresabschlussprüfer nicht alle Angaben nach § 6a Abs. 3 Satz Nr. 1 bis 5 enthält. Offenkundige Rechenfehler, nachträgliche Korrekturen des Krankenhausträgers oder eine Einschränkung des Jahresabschlussprüfers werden als eine objektiv falsche Datenübermittlung gewertet. Die Rechtsfolgen einer nicht fristgerechten Datenübermittlung sind für ein Krankenhaus erheblich. Die Strafzahlung beträgt mindestens 20.000 Euro und höchstens 400.000 Euro. Des Weiteren veröffentlicht die InEK fortlaufend monatlich aktualisiert auf ihrer Internetseite, welche Krankenhäuser die Daten im Sinne dieser Festlegung nicht oder nicht fristgerecht übermittelt haben.

Mit dem GVWG steigt der Bürokratisierungsaufwand für die Krankenhäuser weiter an und dies gilt nicht nur für das Pflegebudget. Wir können Ihnen daher nur empfehlen, sich frühzeitig mit der Thematik auseinanderzusetzen, um sich optimal auf die künftige Testierung vorzubereiten. Die Erstellung eines Leitfadens oder Handbuchs zur Herleitung des Pflegebudgets, was wir auch frühzeitig angeregt hatten, ist mit diesem Gesetz fast unausweichlich, um für die künftigen Verhandlungen bestens vorbereitet zu sein.

Gerne stehen wir Ihnen für weitere Fragen und Unterstützung mit unserem interdisziplinären Team zur Verfügung.

Quellen:

Gesetz zur Weiterentwicklung der Gesundheitsversorgung (Gesundheitsversorgungsweiterentwicklungsgesetz – GVWG).

Festlegungen gemäß § 6a Abs. 3 Satz 7 KHEntgG im Benehmen mit dem Spitzenverband Bund der Krankenkassen vom 9.9.2021 (www.g-drg.de).

Kontakt für weitere Informationen

Tino Schwabe
Steuerberater, Wirtschaftsprüfer
T +49 911 9193 3651
E tino.schwabe@roedl.com

Christiane Kraus
B.A. Betriebswirtschaft
T +49 911 9193 3706
E christiane.kraus@roedl.com

→ Datenschutz

Das Patientendatenschutzgesetz

Sind alle Krankenhäuser nun Kritis-Betreiber?

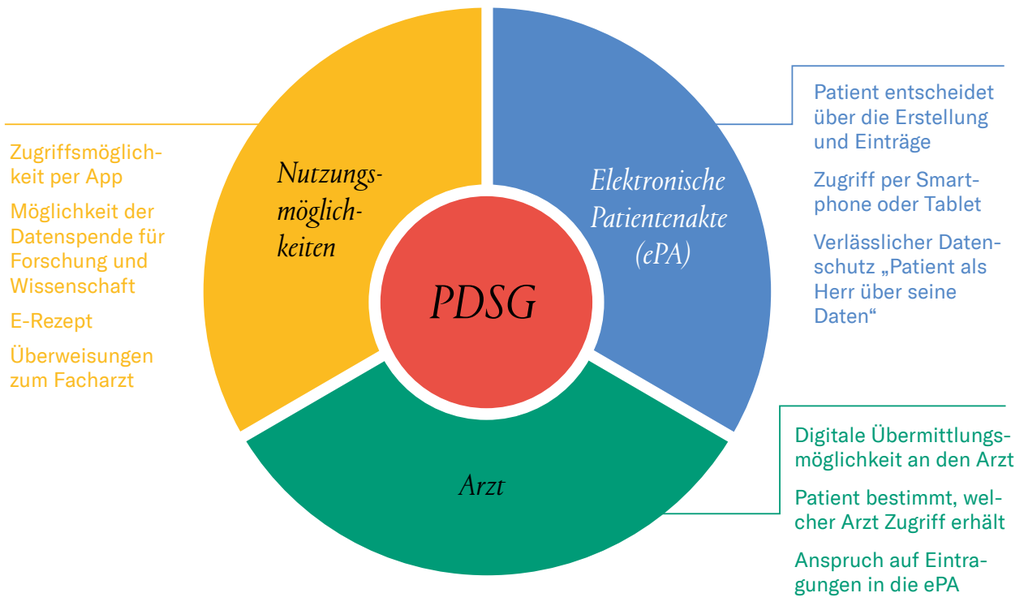
von Jürgen Schwestka und Norman Lenger-Bauchowitz, LL.M.

Datenschutz und Datensicherheit bekommen mit dem am 14.10.2020 verabschiedeten und zum Anfang des Jahres 2021 in Kraft getretenen Patientendatenschutzgesetz (PDSG) eine noch höhere Bedeutung für Krankenhausbetreiber. Im Spannungsverhältnis von Digitalisierung des Gesundheitswesens und Sicherheit von Patientendaten müssen praktikable und verlässliche Lösungen in der Gesundheitswirtschaft entwickelt werden. Diesem Spannungsverhältnis trägt der Beitrag Rechnung.

Mit dem am 14.10.2020 verabschiedeten und zum Anfang des Jahres 2021 in Kraft getretenen Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur – kurz: Patientendatenschutzgesetz (PDSG) soll die Digitalisierung des Gesundheitswesens in Deutschland weiter vorangetrieben werden. Neben den Rahmenbedingungen für die elektronische Patientenakte beinhaltet es insbesondere Vorgaben hinsichtlich der Sicherheit von Patientendaten. Auf Krankenhäuser, Ärzte, Krankenkassen und andere Akteure des Gesundheitswesens kommen seitdem neue Herausforderungen in den Bereichen Datenschutz und Datensicherheit zu.

Das Patientendatenschutzgesetz regelt unterschiedliche Bereiche, die im Ergebnis alle das Recht des Patienten auf eine moderne Gesundheitsversorgung zum Ziel haben. Das bedeutet u. a., dass die Krankenkassen ihren Versicherten ab diesem Jahr eine elektronische Patientenakte (ePA) anbieten müssen. Gleichzeitig erhalten die Patienten einen Anspruch darauf, dass ihre Ärzte die entsprechenden Daten in die ePA eintragen. Zudem besteht ab 2022 auch die Möglichkeit, neben Befunden, Arztberichten oder Röntgenbildern den Impfausweis, den Mutterpass, das gelbe Untersuchungsheft für Kinder sowie das Zahn-Bonusheft in der elektronischen Patientenakte speichern zu lassen. Auch ein Krankenkassenwechsel soll unkompliziert möglich sein. Ab 2022 können die entsprechenden Daten aus der ePA übertragen werden.

Zusammenfassend ergibt sich daher folgendes Bild:



Dort, wo eine große Menge sensibler Daten gesammelt und verarbeitet wird, bedarf es selbstverständlich auch eines besonderen Schutzes.

Eine wesentliche Änderung bringt daher § 75c SGB V hinsichtlich der Anforderungen an die IT-Sicherheit in Krankenhäusern mit sich:

(Absatz 1, Satz 1) Ab dem 1. Januar 2022 sind 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.

Neu ist in diesem Zusammenhang, dass die Umsetzung angemessener Maßnahmen im Bereich der Informationssicherheit nach dem Stand der Technik auch für kleinere Krankenhäuser verbindlich vorgegeben wird. Bisher waren ausschließlich Universitätskliniken und Maximalversorger als sog. kritische Infrastrukturen durch das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) betroffen. Kleinere Krankenhäuser stehen daher vor großen Herausforderungen, da neben technischen Anpassungen und Investitionen auch Anpassungen an interne Verfahren notwendig werden. Gleichzeitig ist die Personalausstattung in der Regel ohnehin angespannt und die Möglichkeiten Personal zu beschaffen und langfristig zu binden sind insbesondere im öffentlichen Bereich begrenzt. Neben dem Tages- und Projektgeschäft sowie der herausfordernden Anbindung an die Telematik-Infrastruktur gesellen sich nun verstärkt regulatorische Anforderungen zur Datensicherheit.

Umso wichtiger ist es, dieses Thema möglichst gezielt und ressourceneffizient anzugehen. Folgende Fragestellungen sind hierfür von Bedeutung:

- Wie laufen die Prozesse der medizinischen Versorgung ab und welche IT-Systeme werden dafür aktuell verwendet?
- Was sind die kritischen IT-Systeme und welchen Schutzbedarf haben sie derzeit?
- Wie sind die Systeme heute geschützt?
- Welche Maßnahmen müssen ergriffen werden, um einen ausreichenden gesetzeskonformen Schutz zu gewährleisten?

Zu beachten ist dabei, dass die Maßnahmen nicht zwingend technischer Natur sein müssen (z. B. Einführung neuer Systeme zur Absicherung). Häufig sind organisatorische Maßnahmen (z. B. Neugestaltung von Zugriffsrechten, Festlegung von Verantwortlichkeiten) sehr viel zielführender als große Investitionsmaßnahmen. Diese Maßnahmen sparen Zeit und andere Ressourcen. Welches jeweils die zielführendste Maßnahme ist, sollte gemeinsam mit Mitarbeitern der Krankenversorgung und der IT ermittelt werden. Datenschutz und Datensicherheit sind eine Unternehmensaufgabe, bei der abteilungsübergreifend zusammengearbeitet werden muss, um angemessene und effiziente Maßnahmen umzusetzen.

Koordinierende Stelle ist hier im Normalfall der Informationssicherheitsbeauftragte (ISB) des Krankenhauses. Dieser ist wesentlicher Bestandteil des Informationssicherheits-Management-Systems (ISMS). Der ISB muss mit einem ausreichenden Zeitbudget versehen werden, um seinen Aufgaben nachkommen zu können. Bei der Besetzung ist insbesondere darauf zu achten, dass Interessenskonflikte durch Überschneidungen mit anderen Tätigkeiten (z. B. gleichzeitige Leitung der IT-Abteilung) ausgeschlossen werden. Weiterhin empfiehlt es sich, bei der Auswahl auf Branchenerfahrung zu achten, denn es bedarf im Umgang mit Ärzten und dem Pflegepersonal erfahrungsgemäß der richtigen Ansätze, um auch unpopuläre, aber durchaus notwendige Sicherheitsmaßnahmen zu platzieren und durchsetzen zu können.

ABER WANN SIND DENN NUN ORGANISATORISCHE UND TECHNISCHE VORKEHRUNGEN ANGEMESSEN?

(Absatz 1, Satz 2) Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung des Krankenhauses oder der Sicherheit der verarbeiteten Patienteninformationen steht.

Kurzum:

Soviel wie nötig und so wenig wie möglich!

Von elementarer Bedeutung bei der Umsetzung von Maßnahmen ist dabei, dass die jeweiligen Schutzziele erreicht werden. Die Zauberformel lautet „VAPIBV“:

VERFÜGBARKEIT von Dienstleistungen, Funktionen eines Informationssystems, IT-System, IT-Netzinfrastruktur oder auch von Informationen ist dann gegeben, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

AUTHENTIZITÄT der Informationen ist sichergestellt, wenn sie von der angegebenen Quelle erstellt wurden.

PATIENTENSICHERHEIT als die Freiheit von unvertretbaren Risiken einer physischen Verletzung oder eines Schadens an der Gesundheit von Menschen. Dies schließt auch die Vermeidung einer nachhaltigen psychischen Belastung ein.

INTEGRITÄT bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.

BEHANDLUNGSEFFEKTIVITÄT stellt die wirksame Behandlung des Patienten unter Benutzung von Informationen und wirksamen Therapiemaßnahmen, ggf. auf Basis eines Informationsaustausches zwischen unterschiedlichen verantwortlichen Organisationseinheiten, sicher.

VERTRAULICHKEIT stellt den Schutz vor unbefugter Preisgabe von Informationen sicher. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in zulässiger Weise zugänglich sein.

Die Schutzziele Patientensicherheit und Behandlungseffektivität stammen aus dem branchenspezifischen Sicherheitsstandard (B3S) für die medizinische Versorgung in Krankenhäusern. Der B3S geht mit der Festlegung dieser Ziele über die Anforderungen einschlägiger Normen, wie dem BSI Grundschutz, deutlich hinaus. Mit Blick auf die wesentlichen Ziele eines Krankenhauses und das Wohl von Patienten ist dies jedoch zielführend und nachvollziehbar.

Eine rein wirtschaftliche Betrachtung bei der Planung von Maßnahmen ist nicht ausreichend. Die Umsetzung einer Maßnahme darf nicht aus dem Grund unterbleiben, weil sie beispielsweise „zu teuer“ ist. Es muss dabei immer abgewogen werden, welche Risiken durch Unterlassung von Maßnahmen auf die Schutzziele bestehen und ob ein angemessener Schutz besteht.

(Absatz 1, Satz 3) Die informationstechnischen Systeme sind spätestens alle 2 Jahre an den aktuellen Stand der Technik anzupassen.

Die Umsetzung des Stands der Technik orientiert sich an den Vorgaben des BSI-Gesetzes, laut dem alle 2 Jahre ein entsprechender Nachweis gefordert ist.

Gegenüber Betreibern kritischer Infrastrukturen gibt es jedoch eine entscheidende Erleichterung: Der Stand der Technik ist zwar umzusetzen, die Umsetzung ist allerdings nicht – zwingend – gegenüber dem BSI nachzuweisen. Ein Nachweis der Umsetzung kann unter Umständen aber dennoch nützlich sein, z. B. bei Abschluss einer Cyber-Versicherung, als Nachweis der Wirksamkeit des Management-Systems für Informationssicherheit oder unter Compliance Gesichtspunkten.

WANN KANN MAN SICHER SEIN, DASS DIE VERPFLICHTUNGEN ERFÜLLT SIND?

(Absatz 2) Die Krankenhäuser können die Verpflichtungen nach Absatz 1 insbesondere erfüllen, indem sie einen branchenspezifischen Sicherheitsstandard für die informationstechnische Sicherheit der Gesundheitsversorgung im Krankenhaus in der jeweils gültigen Fassung anwenden, dessen Eignung vom Bundesamt für Sicherheit in der Informationstechnik nach § 8a Absatz 2 des BSI-Gesetzes festgestellt wurde.

Es gibt verschiedene Grundlagen, an denen sich die Krankenhäuser orientieren können, um die Verpflichtungen zur Datensicherheit strukturiert umzusetzen. Am bekanntesten sind dabei vermutlich die Norm ISO/IEC 27001 und der BSI IT-Grundschutz. Letzterer ist allerdings sehr formal, umfangreich und wenig prozessorientiert. Es lohnt sich daher, Verfahren am branchenspezifischen Sicherheitsstandard (B3S) „Medizinische Versorgung“, der vom Branchenarbeitskreis „Medizinische Versorgung“ erstellt wurde, auszurichten.

Weder das BSI-Gesetz noch die Kritis-Verordnung enthalten konkrete Maßnahmen innerhalb einer spezifischen Branche, um die im BSI-Gesetz abstrakt formulierten Anforderungen umzusetzen. Der branchenspezifische Sicherheitsstandard entspricht einer Interpretation für sinnvolle und notwendige Maßnahmen im Bereich der medizinischen Versorgung und bietet durch die Freigabe des BSI Sicherheit. Die Aufrechterhaltung des Versorgungsniveaus der kritischen Infrastruktur steht stets im Mittelpunkt der Maßnahmen. Hierfür ist ein Informationssicherheits-Management-System (ISMS) obligatorisch. Wesentlicher Bestandteil des Managementsystems ist die Risikoverwaltung. Es sind strukturierte Verfahren für die Identifikation, Bewertung und Überwachung von Risiken im Bereich der Informationssicherheit zu etablieren und aufrechtzuerhalten. Neben dem Risikomanagement enthält der B3S außerdem die folgenden Bereiche:

- Informationssicherheits-Management-System (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

WER IST VON DEN NEUREGELUNGEN NICHT BETROFFEN?

(Absatz 3) Die Verpflichtung nach Absatz 1 gilt für alle Krankenhäuser, soweit sie nicht ohnehin als Betreiber kritischer Infrastrukturen gemäß § 8a des BSI-Gesetzes angemessene technische Vorkehrungen zu treffen haben.

Für Kritis-Häuser ergeben sich durch § 75c SGB V keine Änderungen, da sie bereits ohnehin durch das BSI-Gesetz zur Umsetzung des Stands der Technik verpflichtet sind.

Durch das Patientendatenschutzgesetz sollen im Ergebnis alle Krankenhäuser auf das Schutzniveau von Kritis-Häusern kommen, unabhängig von der Fallzahl (sog. Kritis-light). Derzeit definiert die Kritis-Verordnung lediglich Krankenhäuser mit einer jährlichen Zahl von mindestens 30.000 vollstationären Fällen als kritische Infrastrukturen.

Zum aktuellen Zeitpunkt ist für Nicht-Kritis-Häuser kein Nachweis über die Umsetzung im Rahmen von zweijährlichen Prüfungen gegenüber dem BSI geplant. Dabei handelt es sich jedoch um eine Momentaufnahme. Seit Veröffentlichung der Kritis-Verordnung wird mit einer sukzessiven Erweiterung des Kreises der Betreiber kritischer Infrastrukturen durch Senkung der Schwellenwerte gerechnet. Nichtsdestotrotz sollte die Geschäftsleitung über eine freiwillige Prüfung, beispielsweise auf Basis des branchenspezifischen Sicherheitsstandards, nachdenken. Hierdurch können wesentliche Schwachstellen und Angriffspunkte frühzeitig aufgedeckt und nachgebessert werden. Einen Ausfall der medizinischen IT-Systeme können und dürfen sich große wie kleine Krankenhäuser nicht erlauben. Gut, wenn man vorher nachweislich durch ein Audit Auswirkungen und Wahrscheinlichkeiten von Schadensereignissen auf ein akzeptables Maß reduzieren konnte. Sollten dennoch umfangreichere IT-Investitionen notwendig werden, kein Problem. Das Krankenhauszukunftsgesetz (KHZG) sieht in einem der Förderprogramme vor, dass Projekte zur Beschaffung, Errichtung, Erweiterung oder Entwicklung informationstechnischer oder kommunikationstechnischer Anlagen, Systeme oder Verfahren unterstützt werden. Gleiches gilt für die Modernisierung der vorhandenen Systeme. Förderungen nach § 12a Abs. 1 S. 4 Nr. 3 des KHZGs (Vorhaben zur Verbesserung der informationstechnischen Sicherheit der Krankenhäuser aus dem Strukturfond) sind sogar vorrangig.

Sprechen Sie uns gerne an. Unsere Experten, die auch über die Berechtigung nach § 21 KHSFV verfügen, sind gerne für Sie da!

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

Norman Lenger-Bauchowitz, LL.M.
Rechtsanwalt, Fachanwalt
für Steuerrecht, Zertifizierter
IT-Compliance Manager
T +49 911 9193 3713
E norman.lenger@roedl.com

→ Datenschutz

Cloudlösungen wie Microsoft 365 als Herausforderung für Krankenhäuser

von Christoph Naucke, Maximilian Dachlauer und Jonas Buckel

Viele für Unternehmen notwendige IT-Lösungen werden von den jeweiligen Herstellern strategisch nur noch als Cloudlösungen angeboten. Auch aus Sicht der anwendenden Unternehmen sind sie oft wesentlich attraktiver, beispielsweise unter Kostengesichtspunkten. Hinzu kommt der Prozessvorteil, den Cloudlösungen für das Arbeiten „von überall her" bieten und der nicht zuletzt durch die Pandemie zusätzlich massiv an Bedeutung gewonnen hat. Diese Überlegungen gelten für Unternehmen des Gesundheitssektors, insbesondere für Krankenhäuser, in gleichem Maße wie für jedes Unternehmen.

Zugleich bedeuten Cloudlösungen wie beispielsweise Microsoft 365 (MS 365) jedoch erhebliche datenschutzrechtliche Herausforderungen für die Unternehmen als Verantwortliche. Diese Herausforderungen sind für Krankenhäuser deswegen nochmals größer, weil sie zusätzlich zum allgemeinen Datenschutzrecht spezifischen Datenschutzvorgaben unterliegen, einerseits oftmals als öffentliche Stellen des betreffenden Bundeslandes, andererseits aus dem Landeskrankenhausrecht heraus.

Wie stellt sich die Rechtslage dar für Krankenhäuser, die auf den Einsatz von Cloudlösungen wie Microsoft 365 in ihrer IT-Infrastruktur nicht verzichten können oder auch wollen, und worauf sollte in jedem Fall geachtet werden?

VORGELAGERTES RISIKO EINER FEHLENDEN RECHTSGRUNDLAGE BEACHTEN

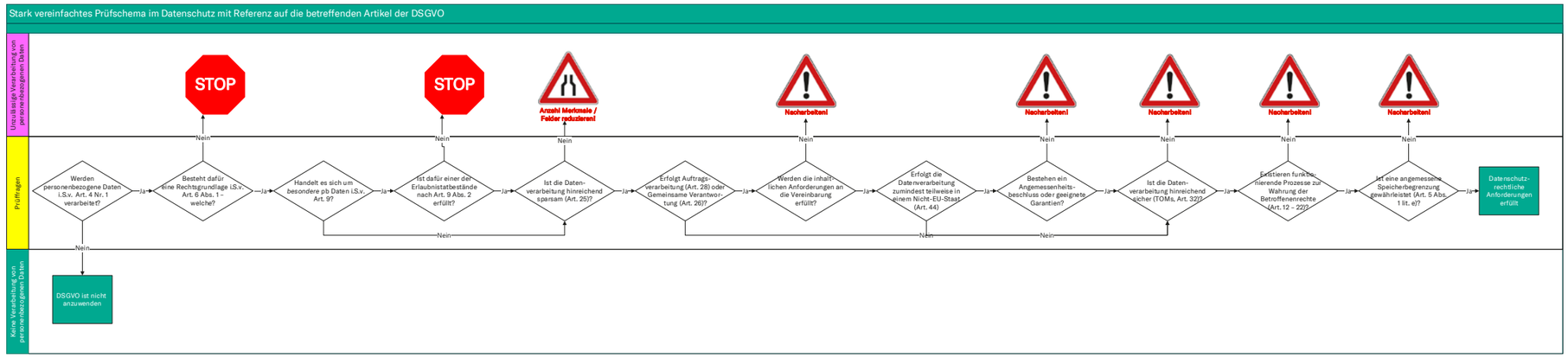
Es besteht u. a. die Gefahr, dass eine geplante oder auch bereits installierte Cloudlösung von den Datenschutzaufsichtsbehörden des betreffenden Bundeslandes deswegen als unzulässig eingestuft wird, weil für einzelne Verarbeitungsvorgänge, die durch den Dienstleister vorgesehen sind, die erforderliche Rechtsgrundlage i. S. v. Art. 6 Abs. 1 DSGVO fehlt. Als Beispiel ist hier das teilweise vorgesehene Recht des Anbieters zu nennen, die personenbezogenen Daten der Beschäftigten auch für Zwecke der Produktverbesserung zu nutzen.

VERSCHLÜSSELUNGSMASSNAHMEN ERSETZEN KEINE FEHLENDEN RECHTSGRUNDLAGEN

Bei den Diskussionen um möglicherweise fehlende Rechtsgrundlagen wird oft auf umfassende technische Maßnahmen verwiesen, die die Vertraulichkeit der personenbezogenen Daten gewährleisten sollen. Beispielsweise hört man das Argument, dass der Cloudanbieter im Fall einer Verschlüsselung nach dem Hold-Your-Own-Key-Standard ohnehin nur im Besitz nicht nutzbarer Daten („Datenschrott") sei, solange ihm dieser Schlüssel nicht offengelegt würde.

Richtig ist, dass die faktische „Unlesbarkeit" der personenbezogenen Daten, die beim Dienstleister gespeichert sind, sich auf das Ergebnis einer Erforderlichkeitsprüfung auswirken kann. Dennoch liegt einer möglichen Argumentation „technische Maßnahmen ersetzen Rechtsgrundlagen" ein Missverständnis zugrunde: Die Prüfung der Rechtsgrundlage ist in der Reihenfolge der Prüfschritte einer datenschutzkonformen Verarbeitung der Prüfung der Schutzmaßnahmen vorgelagert. Ein durch das Gesetz womöglich nicht gedeckter Verarbeitungszweck kann dadurch bildlich gesehen zu einem „Stoppschild" führen, noch bevor die Überprüfung angemessener technischer und organisatorischer Maßnahmen i.S.v. Art. 32 DSGVO relevant wird. In Bezug auf Verschlüsselung bedeutet dies: Verschlüsselung ist im Verständnis der DSGVO lediglich eine Form der erforderlichen technischen Maßnahmen (Art. 32 Abs. 1 lit. a). Dadurch macht der Gesetzgeber zugleich klar, dass Verschlüsselung gerade nicht dazu führt, dass die verschlüsselten Daten keine personenbezogenen Daten mehr wären und daher dem Datenschutz gar nicht unterfallen würden.

Abbildung: Die vereinfachte grafische Darstellung der datenschutzrechtlichen Prüfschritte veranschaulicht: Verschlüsselung als technische Maßnahme ersetzt keine ggf. fehlende Rechtsgrundlage.



VERARBEITUNG PERSONENBEZOGENER DATEN

Beim Einsatz von Microsoft 365 wird eine Vielzahl von personenbezogenen Daten verarbeitet. Hauptsächliche Betroffene sind die Beschäftigten des Verantwortlichen. In einem Krankenhaus können Patienten als weitere wichtige Betroffenenkategorie hinzutreten. Die Krankenhäuser müssen daher sowohl die Vorschriften der Datenschutz-Grundverordnung (DSGVO) in Verbindung mit dem Bundesdatenschutzgesetz (BDSG) bzw. den Landesdatenschutzgesetzen (LDSG) hinsichtlich der Verarbeitung der Beschäftigtendaten als auch die jeweiligen Regelungen aus den Landeskrankenhausgesetzen in Bezug auf die Verarbeitung von Patientendaten beachten.

MICROSOFT ALS AUFTRAGSVERARBEITER

Der Einsatz von Textverarbeitungsprogrammen und Kommunikationsplattformen als Cloudlösung fällt in aller Regel unter die Regeln der Auftragsverarbeitung im Sinne von Art. 28 DSGVO. Microsoft wird daher grundsätzlich als Auftragsverarbeiter des jeweiligen Krankenhauses tätig.

Da die Verarbeitungstätigkeit eines Auftragsverarbeiters datenschutzrechtlich in vielerlei Hinsicht so behandelt wird, als verarbeite der Verantwortliche selbst die personenbezogenen Daten, benötigt der Verantwortliche für den Einsatz eines Auftragsverarbeiters per se keine Rechtsgrundlage. Vielmehr genügt die Rechtsgrundlage, auf die der Verantwortliche selbst die Verarbeitungstätigkeit stützen kann. Im Fall von Beschäftigtendaten dürfte dies oftmals Art. 88 DSGVO i. V. m § 26 BDSG bzw. den jeweiligen Paragraphen in den LDSG sein. Freilich müssen dennoch die weiteren Regelungen über die Auftragsverarbeitung gem. Art. 28 DSGVO eingehalten werden: Es muss eine Vereinbarung zwischen Verantwortlichem und Auftragsverarbeiter geschlossen werden mit gewissen, gesetzlich vorgeschriebenen Mindestinhalten.

Die Verarbeitung von Beschäftigtendaten ist dann zulässig, wenn sie zur Durchführung des Beschäftigungsverhältnisses *erforderlich* ist. Im Rahmen der durchzuführenden Erforderlichkeitsprüfung kommt es darauf an, ob die Verarbeitung in der konkreten Situation das vom Verantwortlichen als Arbeitgeber gewählte mildeste Mittel ist, das heißt, ob die Persönlichkeitsrechte der Beschäftigten nur insoweit eingeschränkt werden, wie es für den Zweck der Verarbeitung notwendig ist. Ob die mit dem Arbeitsmittel Microsoft 365 als Cloudlösung eintretende Verarbeitung der Beschäftigtendaten das jeweils mildeste Mittel ist, erscheint schon deshalb zweifelhaft, weil bei der Übertragung der personenbezogenen Daten an Microsoft von einem Drittstaatentransfer in die USA ausgegangen werden muss und dadurch ein nach europäischem Recht übermäßiger Zugriff auf diese Daten durch US-Behörden nicht auszuschließen ist.

Gleiche Überlegungen gelten für die vorzunehmende Abwägung zwischen den berechtigten Interessen des Verantwortlichen und den Persönlichkeitsrechten der Beschäftigten, wenn man die Verarbeitung auf Art. 6 Abs. 1 lit. f DSGVO stützen möchte. Wichtig zu beachten ist für Krankenhäuser jedoch: Diese Möglichkeit entfällt im Falle von Krankenhäusern, da sie öffentliche Stellen sind.

Hinsichtlich Patientendaten ist die Rechtslage noch einmal komplizierter. Die datenschutzrechtliche Zulässigkeit der Verarbeitung von Patientendaten regeln die jeweiligen Landeskrankenhausgesetze. Ob und wie Krankenhäuser Patientendaten durch einen Auftragsverarbeiter verarbeiten lassen dürfen, ist stark reglementiert. Oftmals dürfen medizinische Daten nur durch das Krankenhaus selbst oder durch ein anderes Krankenhaus verarbeitet werden.

MICROSOFT ALS EIGENER VERANTWORTLICHER

Im Falle des Einsatzes von MS 365 wird Microsoft jedoch nicht nur als Auftragsverarbeiter tätig und verfolgt insoweit nicht ausschließlich die Zwecke des Verantwortlichen. Ausweislich des Nachtrags zum Datenschutz für Online-Dienste aus Dezember 2020[1] lässt sich Microsoft erlauben, bestimmte personenbezogene Daten auch für legitime Geschäftsinteressen von Microsoft zu verarbeiten. Hier verfolgt Microsoft eigene Zwecke und ist in Bezug auf diese Zwecke nicht mehr Auftragsverarbeiter des jeweiligen Krankenhauses, sondern eigener Verantwortlicher. In der Folge bedarf das Krankenhaus einer Rechtsgrundlage für die Übermittlung der Beschäftigtendaten an Microsoft als eigenen Verantwortlichen.

Als problematisch anzusehen ist hierbei, dass die Übermittlung von Beschäftigtendaten an Microsoft als eigenen Verantwortlichen nicht zu Zwecken der Durchführung des Arbeitsverhältnisses stattfindet, sondern für die eigenen Geschäftsinteressen von Microsoft. Art. 88 DSGVO i. V m § 26 BDSG bzw. den jeweiligen Paragraphen in den LDSG scheidet daher als Rechtsgrundlage aus. Die vorzunehmende Interessenabwägung im Rahmen von Art. 6 Abs. 1 lit. f DSGVO wird aus oben genannten Gründen ebenfalls ergeben, dass sich der Arbeitgeber regelmäßig nicht auf ein berechtigtes Interesse stützen kann, ein Arbeitsmittel einzusetzen, das damit verbunden ist, dass personenbezogene Daten zu Geschäftsinteressen des Dienstleisters in ein Drittland übertragen werden, in dem ein nach europäischem Recht übermäßiger Zugriff auf diese Daten durch staatliche Behörden des Drittlands nicht auszuschließen ist. Gleiches gilt für die Klassifizierung der Geschäftsinteressen von Microsoft als Drittinteresse im Sinne von Art. 6 Abs. 1 lit. f DSGVO. Wieder zu beachten ist an dieser Stelle, dass für Krankenhäuser, die datenschutzrechtlich öffentliche Stellen sind, das berechtigte Interesse nach Art. 6 Abs.1 lit. f DSGVO als Rechtsgrundlage von vornherein nicht in Betracht kommt. Letztere ist jedoch in der Anwendungspraxis naturgemäß unbeliebt, da sie einen erheblichen Verwaltungsaufwand sowie Folgeprobleme nach sich zieht (ggf. fehlende Handlungsoptionen des Arbeitgebers im Falle der Verweigerung bzw. des Widerrufs einer Einwilligung).

Auch die Übermittlung von Patientendaten an Microsoft zu deren eigenen Geschäftsinteressen dient nicht der Behandlung von Patienten, weshalb die Landeskrankenhausgesetze in der Regel ebenfalls keine Rechtsgrundlage für die Übermittlung bieten.

ÜBERMITTLUNG IN EIN DRITTLAND

Eine Übermittlung personenbezogener Daten an ein Drittland ist nur zulässig, wenn der Verantwortliche – neben den sonstigen Bestimmungen der DSGVO – die Vorschriften des 5. Kapitels der DSGVO, d. h. die Vorschriften gem. Art. 44 ff. DSGVO einhält.

Eine Drittlandübermittlung ist danach zum einen zulässig, wenn ein sog. Angemessenheitsbeschluss der EU-Kommission zu dem Drittland, in das personenbezogene Daten übermittelt werden, vorliegt. Das vom EuGH „gekippte“ Privacy Shield war ein solcher Teil-Angemessenheitsbeschluss in Bezug auf Datentransfers in die USA.

Falls kein Angemessenheitsbeschluss vorliegt, darf ein Verantwortlicher personenbezogene Daten an ein Drittland zum anderen übermitteln, sofern der Verantwortliche geeignete Garantien vorgesehen hat und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Diese geeigneten Garantien können auch in den Standarddatenschutzklauseln bestehen.

Die „neuen“ Standarddatenschutzklauseln traten am 27.6.2021 in Kraft. Die bislang noch geltenden „alten“ Standarddatenschutzklauseln werden mit Wirkung vom 27.9.2021 aufgehoben und können für neue Verträge keine wirksame Garantie für einen rechtmäßigen Drittstaatendatenverkehr mehr darstellen. Für Verträge, die vor dem 27.9.2021 auf Grundlage der alten Standardvertragsklauseln geschlossen wurden, wird eine Übergangsfrist bis zum 27.12.022 gewährt.

Die Problematik, dass US-Behörden im Rahmen des Cloud Acts gegebenenfalls in unverhältnismäßiger Weise auf personenbezogene Daten zugreifen können, wird jedoch auch durch die „neuen“ Standarddatenschutzklauseln nicht vollständig gelöst, denn diese können als zivilrechtlicher Vertrag freilich keine Bindungswirkung für ausländische Behörden entfalten. Es müssen daher zusätzliche Maßnahmen getroffen werden, um einen Zugriff der US-Behörden zu vermeiden.

VORNAHME GEEIGNETER TECHNISCHER UND ORGANISATORISCHER MASSNAHMEN ZUR RISIKOREDUZIERUNG

Das Risiko eines datenschutzwidrigen Einsatzes von MS 365 kann durch die Vornahme geeigneter technischer und organisatorischer Maßnahmen zwar nicht gänzlich ausgeschlossen, jedoch zumindest reduziert werden.

[1] https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

Im Idealfall sollte der Datenfluss derjenigen personenbezogenen Daten, bei denen sich Microsoft vorbehält, sie als eigener Verantwortlicher zu verarbeiten, möglichst effektiv unterbunden werden. Es sollte daher zum einen eine vertragliche Konstruktion gewählt werden, bei der es Microsoft untersagt wird, personenbezogene Daten außerhalb des Auftragsverarbeitungsverhältnisses auch zu eigenen Zwecken zu verarbeiten. Hierbei sollte die eigene Verhandlungsposition nicht unterschätzt werden: Vor Abschluss des Lizenzvertrages besteht mitunter mehr Verhandlungsspielraum als vermutet.

Zum anderen sollten aber auch auf technischer Ebene Maßnahmen etabliert werden, mithilfe derer der Datenfluss an Microsoft als eigener Verantwortlicher möglichst effektiv verhindert wird. Dies kann beispielsweise bereits an der Firewall geschehen oder durch das Setzen bestimmter Gruppenrichtlinieneinstellungen.

Zur Minimierung des Risikos eines datenschutzwidrigen Zugriffs von US-Behörden sollten alle personenbezogenen Daten an Microsoft nur derart verschlüsselt übertragen werden, dass ein Zugriff von Microsoft auf Klardaten sowohl bei der Übertragung als auch bei der Speicherung oder deren Erstellung verhindert wird. Dies hätte auch zur Konsequenz, dass die Erforderlichkeitsprüfung im Rahmen der Prüfung der Rechtsgrundlage für die Verarbeitung der Beschäftigtendaten zugunsten des Arbeitgebers ausgehen dürfte und MS 365 als Arbeitsmittel datenschutzrechtlich zulässig eingesetzt werden könnte.

Die Möglichkeiten, bei der Konfiguration von MS 365 technische und organisatorische Maßnahmen zur Wahrung der Vertraulichkeit der Daten zu treffen, sind vielfältig und auch für erfahrene Administratoren nur schwer überschaubar. Gleichzeitig sollte auch bedacht werden, dass die werksseitige Standardkonfiguration von MS 365 keine optimale Ausschöpfung der Möglichkeiten zur Erhöhung der Vertraulichkeit bedeutet. Im Vorfeld der Installation sollten also sämtliche Einstellungen kritisch überprüft, hinterfragt und angepasst werden. In dem Zusammenhang ist auch das Minimalprinzip zu nennen: Alle MS 365-Anwendungen, Funktionen, Features etc., deren Verwendung nicht tatsächlich erforderlich ist, sollten auch ausgeschaltet werden.

ERFORDERLICHKEIT EINER DATENSCHUTZFOLGENABSCHÄTZUNG

In jedem Fall ist vorab eine Datenschutzfolgenabschätzung gemäß Art. 35 DSGVO durchzuführen, da im Rahmen des Einsatzes von MS 365 vertrauliche Daten schutzbedürftiger Personen (Beschäftigter und Patienten) verarbeitet werden können und ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nicht auszuschließen ist.

UNVOLLSTÄNDIGES FACHWISSEN FÜHRT ZU ERHÖHTEN RISIKEN

Soweit nicht auf interne Mitarbeiter mit breitem Rechtswissen sowie fundierter Erfahrung bei MS 365-Einführungen zurückgegriffen werden kann, ist gerade für Krankenhäuser sowie Unternehmen der Forschungs-, der Gesundheits- und der Sozialwirtschaft eine datenschutzrechtliche Beratung und externe Unterstützung bei einer geplanten Migration auf MS 365 dringend zu empfehlen.

Wir unterstützen öffentliche Einrichtungen, Unternehmen der Sozial- und Gesundheitswirtschaft und der Forschung bei der Bewertung und der bestmöglichen Beherrschung datenschutzrechtlicher Risiken, die mit dem Einsatz von Cloudlösungen verbunden sind, sowie bei der Identifikation derjenigen technischen und organisatorischen Maßnahmen, die mindestens getroffen werden sollten, soweit die Einrichtung sich für die Einführung einer Cloudlösung entscheidet. Hierzu zählt im Bedarfsfall auch die Durchführung und Dokumentation einer erforderlichen Datenschutzfolgenabschätzung.

Kontakt für weitere Informationen

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

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

Verfahrensdokumentation

Die verkannte Notwendigkeit

von Ronny Oechsner und Christian Munker

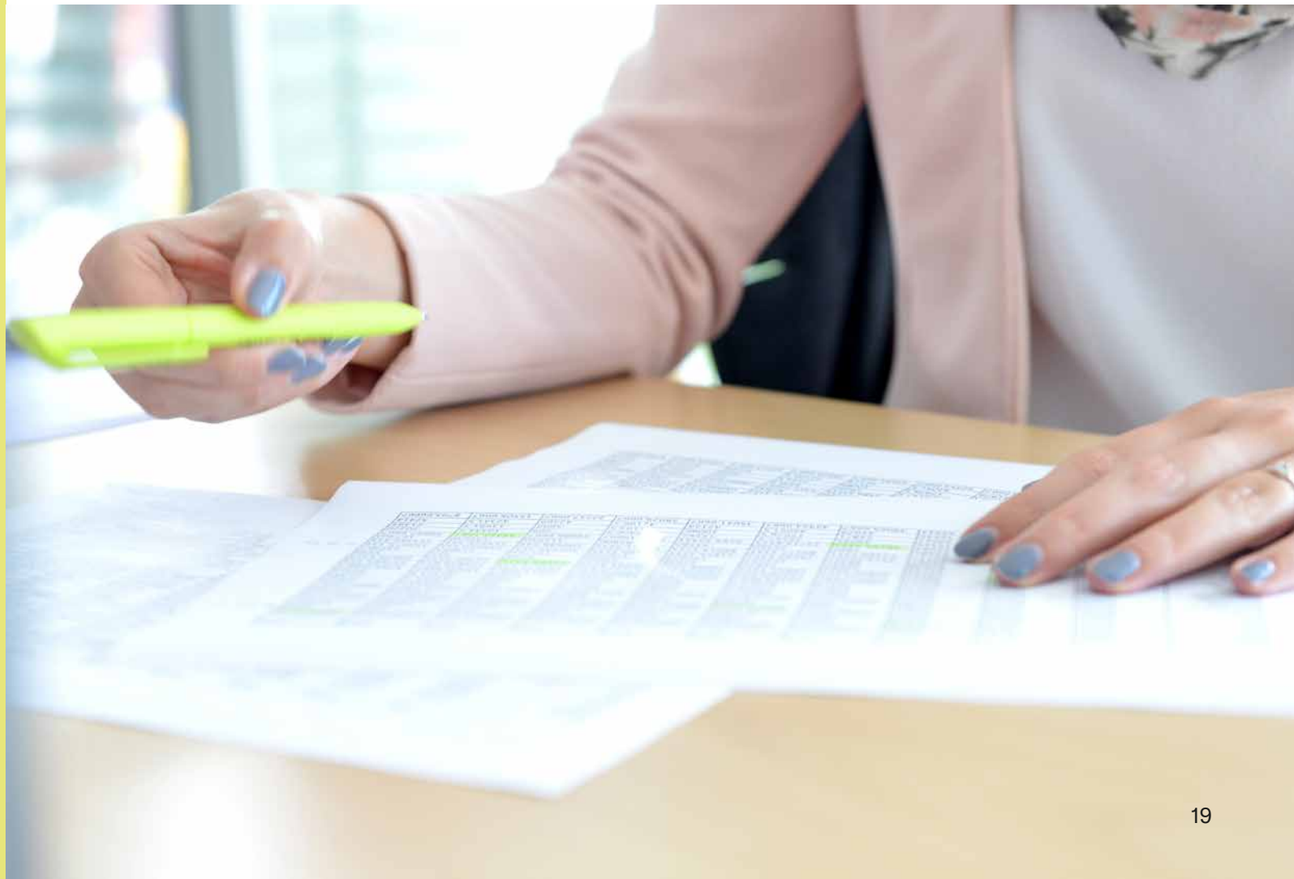
„Die Verfahrensdokumentation nach GoBD dient dazu, nachweisen zu können, dass die Anforderungen des Handelsgesetzbuches und der Abgabenordnung für die Erfassung, Verbuchung, Verarbeitung, Aufbewahrung und Entsorgung von Daten und Belegen erfüllt ist.“[1]

Was auf Wikipedia relativ unscheinbar formuliert ist, kann nach unserem Dafürhalten das nächste scharfe Schwert der Finanzverwaltung im Rahmen von steuerlichen Außenprüfungen werden.

Die Verpflichtung zur Erstellung und laufenden Aktualisierung von Verfahrensdokumentationen ergibt sich direkt aus den Grundsätzen zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff, den GoBD. Diese sind verpflichtend von jedem Unternehmer in Deutschland anzuwenden, egal ob Großkonzern, Mittelständler, Einzelunternehmer oder gemeinnützige Organisation.

Im Rahmen dieses Artikels möchten wir Ihnen einen Einblick in die Grundlagen dieses oft verkannten Themas bieten sowie die damit einhergehenden Risiken, aber auch Chancen darlegen.

[1] https://de.wikipedia.org/wiki/Verfahrensdokumentation.



RECHTLICHE GRUNDLAGEN

Bereits im Rahmen des umfangreichen Schreibens vom 14.11.2014 [2] zu den „neuen Grundsätzen der ordnungsgemäßen Buchführung“ hat das Bundesministerium der Finanzen (BMF) die Verfahrensdokumentation als Grundlage für eine gesetzeskonforme Buchführung aufgenommen. Die Grundsätze dieses Schreibens galten für Veranlagungszeiträume, die nach dem 31.12.2014 begonnen haben.

Somit besteht in der Regel bereits seit dem Jahr 2015 im Rahmen der steuerlichen Buchführungs- und Aufzeichnungspflichten die Notwendigkeit zur Erstellung einer Verfahrensdokumentation für DV-Systeme. Es handelt sich insoweit um keine neue Thematik. Noch heute wird das Thema in der Praxis an vielen Stellen unterschätzt.

Mit Datum vom 28.11.2019 veröffentlichte das BMF ein überarbeitetes Folgeschreiben, das das vorangegangene Schreiben vom 14.11.2014 ersetzt und mit Wirkung zum 1.1.2020 in Kraft trat.[3] Im Rahmen dieses Schreibens wurden die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (kurz: GoBD) weiterentwickelt und insbesondere an die neuen technischen Gegebenheiten angepasst.

Durch die stetige Weiterentwicklung der Grundsätze und vor allem die Erweiterung um den elektronischen Datenzugriff versteht sich die Finanzverwaltung als Treiber der Digitalisierung.

Hierbei werden bereits bestehende Regelungen zur Buchführungs- und Archivierungspflicht von Geschäftsdokumenten in Papierform Zug um Zug auf elektronische Dokumente ausgeweitet.

Die Erfüllung der besonderen gesetzlichen Anforderungen an eine GoBD-konforme Software und Belegerfassung rückt zukünftig verstärkt in den Fokus von Betriebsprüfungen. Die Verantwortung der Ordnungsmäßigkeit liegt hierbei beim Steuerpflichtigen und ist nicht delegierbar.

Aus dem BMF-Schreiben lässt sich als Kriterium für die GoBD-Konformität der Buchführung unter anderem die Erstellung und Aufbewahrung einer Verfahrensdokumentation ableiten.

WAS IST EINE VERFAHRENSDOKUMENTATION?

Eine Verfahrensdokumentation dient im Wesentlichen als Nachweis über die Einhaltung der Grundsätze der ordnungsgemäßen Buchführung im Unternehmen.

In Bezug auf die eingesetzten DV-Systeme fordert das BMF eine Verfahrensdokumentation, in Bezug auf übrige Verfahren ist eine solche sicherlich zu empfehlen.

Das Bundesministerium gibt dabei keine formale Gestaltung vor. Vielmehr kann jeder Unternehmer selbst entscheiden, wie er die Dokumentation nach den eigenen unternehmensinternen Bedürfnissen erstellt.

Die Verfahrensdokumentation beschreibt dabei den organisatorisch und technisch gewollten Prozess, z. B. bei elektronischen Dokumenten von der Entstehung der Information über die Indizierung, Verarbeitung und Speicherung, dem eindeutigen Wiederfinden und der maschinellen Auswertbarkeit, der Absicherung gegen Verlust und Verfälschung und der Reproduktion.

DIE NOTWENDIGEN INHALTE

Mit Blick auf den notwendigen Inhalt gibt das Bundesministerium für Finanzen vor, dass eine DV-Verfahrensdokumentation in der Regel aus

- einer allgemeinen Beschreibung,
- einer Anwenderdokumentation,
- einer technischen Systemdokumentation sowie
- einer Betriebsdokumentation

besteht.[4]

Für die Praxis kann es zudem empfehlenswert sein, u. a. folgende Inhalte im Rahmen der einzelnen Gliederungsabschnitte aufzunehmen:

- eine Unternehmensbeschreibung
- Nachweis der Mitarbeiterqualifikationen
- Arbeits- und Organisationsanweisungen
- vom Softwarehersteller bereitgestellte Handbücher und Schulungsunterlagen
- Beschreibung der IT-unterstützenden Aufgabenbereiche
- Aufgaben der eingesetzten Datenverarbeitungssysteme, Programme, Module und Infrastrukturkomponenten
- Auflistung der Schnittstellen
- programminterne Vorschriften zur Generierung der Buchungen
- Beschreibung der technischen Verarbeitungsregeln
- Auflistung und Beschreibung der erzeugten Protokolle
- Datensicherungen und Notfallszenarien

Der Unternehmer hat für den gesamten Zeitraum der steuerlichen Aufbewahrungsfrist zu gewährleisten, dass das in der Dokumentation beschriebene Verfahren dem in der Praxis eingesetzten Verfahren voll entspricht. Hierbei gilt es auch zu beachten, dass die Verfahrensdokumentation ebenfalls unter die steuerlichen Aufbewahrungspflichten und -fristen fällt. Die Aufbewahrungsfrist für die Verfahrensdokumentation läuft jedoch nicht ab, soweit und solang die Aufbewahrungsfrist für die Unterlagen noch nicht abgelaufen ist, zu deren Verständnis sie erforderlich ist.

AUSGEWÄHLTE EINZELFRAGEN

GIBT ES BEFREIUNGEN?

Ein klares Nein! Durch die Ausweitung der GoBD auch auf steuerliche Aufzeichnungen betreffen die Vorschriften nicht nur buchführungspflichtige Unternehmer, sondern auch solche, die ihren Gewinn nach Einnahmen-Überschuss-Rechnung ermitteln. Auch kennen die GoBD keine Befreiungen oder Erleichterungen für „kleine“ Unternehmer.

TRÄGT DER UNTERNEHMER NUR EINEN EINMALIGEN ERSTELLUNGSAUFWAND?

Ebenfalls ein klares Nein! Da die Verfahrensdokumentation wie vorstehend beschrieben die tatsächliche und gelebte Praxis schriftlich und nachprüfbar abbilden soll, ist die Verfahrensdokumentation dementsprechend auch an sich ändernde Sachverhalte anzupassen.

Die Änderungen müssen hierbei historisch nachvollziehbar sein, was der Unternehmer am besten durch eine Versionisierung seiner Verfahrensdokumentation erreicht.

WER KANN HELFEN?

Wir verfügen über eine ausgeprägte Expertise im Bereich der Erfordernisse der GoBD und der steuerlich geforderten Dokumentationen und unterstützen Sie gerne bei der konkreten Ausgestaltung Ihrer Verfahrensdokumentationen, in Abhängigkeit von der Komplexität Ihrer Geschäftstätigkeit und der Organisationsstruktur sowie der eingesetzten EDV-Systeme.

FAZIT: DIE VERFAHRENSDOKUMENTATION ALS CHANCE

Auch wenn die Erstellung und laufende Aktualisierung der steuerlich notwendigen Verfahrensdokumentation sicherlich einen nicht unerheblichen Aufwand bedeutet, sollten Unternehmer die Verfahrensdokumentation nicht als notwendiges Übel, sondern auch als Chance betrachten.

Denn durch die Dokumentation ergibt sich so die Möglichkeit, Schwachstellen im Geschäftsprozess oder im organisatorischen Ablauf zu entdecken und zu beheben. Auch ist die Verfahrensdokumentation (in Auszügen) eine hervorragende Anleitung für neue Kollegen, um die Arbeitsweise im Bereich der Buchführung kennenzulernen.

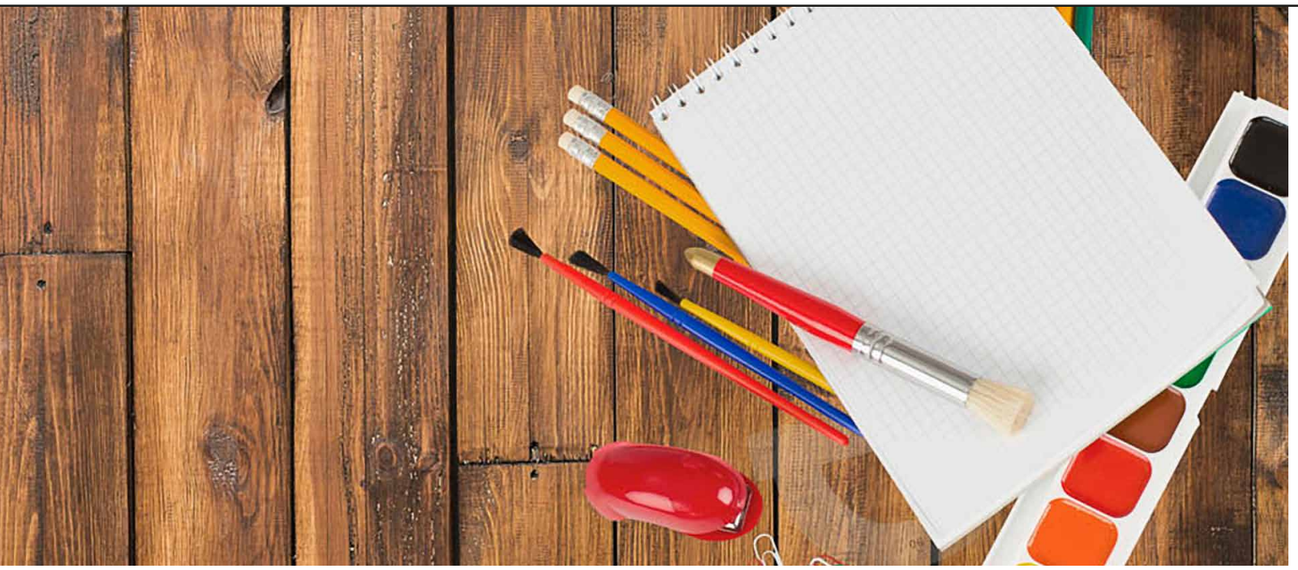
Und nicht zuletzt kann die Verfahrensdokumentation auch als längst überfälliger Einstieg in den Digitalisierungsprozess verstanden werden, weil sie aufzeigen kann, wo im Unternehmen die Digitalisierung noch hakt und wo sie verbesserungsfähig ist.

[2] BMF-Schreiben vom 14.11.2014 (GZ: IV A 4 - S 0316/13/10003).
[3] BMF-Schreiben vom 28.11.2019 (GZ: IV A 4 - S 0316/19/10003 : 001).
[4] Vgl. BMF-Schreiben vom 28.11.2019, RZ 153.

Kontakt für weitere Informationen

Ronny Oechsner
Steuerberater
T +49 221 949 909 439
E ronny.oechsner@roedl.com

Christian Munker
Steuerberater
T +49 911 9193 3688
E christian.munker@roedl.com



→ Compliance

Ein Tax Compliance Management-System ist mehr als ein paar Checklisten – Teil 2

oder: Praxisprobleme bei der Festlegung des Tax Compliance-Ziels

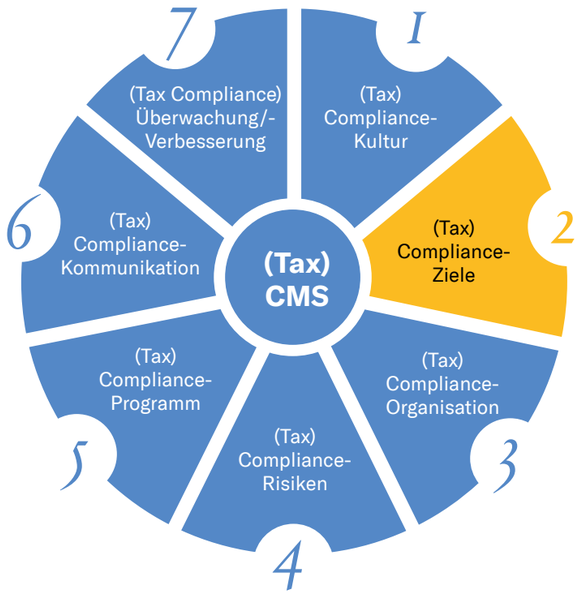
von Anka Neudert und Christoph Naucke

In unserem ersten Artikel „Teil 1" dieser Reihe haben wir einige allgemeine Erläuterungen zum Tax CMS gegeben die aus der Beratungspraxis stammen und den theoretischen Hintergrund beleuchteten. Daher soll ab diesem zweiten Teil die konkrete Umsetzung in der Praxis eine größere Rolle spielen.

Anhand von Beispielen soll gezeigt werden, wo bei der Ausgestaltung eines Tax CMS praktische Probleme liegen können, die insbesondere bei gemeinnützigen Unternehmen oder auch bei juristischen Personen öffentlichen Rechts zum Tragen kommen.

Dieser Artikel beschäftigt sich mit der Schwierigkeit, das korrekte Tax Compliance-Ziel zu definieren.

Weitere Teile, die Schwierigkeiten bei den übrigen Grundelementen eines TCMS beleuchten, folgen.



TAX COMPLIANCE-ZIELE, REGELN UND REGELVERSTÖSSE

Vermeintlich ist die Festlegung der Tax Compliance-Ziele reine Formsache. Beim genaueren Hinsehen stellt sich jedoch heraus, dass es sehr wohl einen Unterschied macht, wie das Tax Compliance-Ziel genau definiert ist und vor allem auch, welche Schwierigkeit es in der Praxis bereitet, ein wirklich sinnvolles Tax Compliance-Ziel zu definieren.

Das folgende Beispiel soll dies verdeutlichen:

Variante 1:

„Ziel unseres TCMS ist die Erfüllung sämtlicher steuerlicher Pflichten und die Einhaltung der Steuergesetze. Steuerliche Regelverstöße sollen in jedem Fall vermieden werden."

Problem bei einer derartigen Formulierung ist, dass erst erläutert werden müsste, was im Unternehmen als steuerlicher Regelverstoß angesehen wird. Zum einen können damit – in umfassendem Sinne - alle Regeln gemeint sein, die negative Folgen mit Bezug zum Bereich „Tax" vermeiden sollen. Zum anderen könnten aber auch nur solche Verstöße gemeint sein, die strafrechtliche Konsequenzen oder Reputationsschäden zur Folge hätten:

Hierdurch wird deutlich, dass auch für den steuerlichen Bereich Regeln aufgestellt werden müssen, die jeder Mitarbeiter versteht und befolgen kann. Formulierungen wie „Während der Arbeitszeit darf kein Alkohol konsumiert werden", die ebenfalls eine – zwar nicht steuerliche – Regel für das gesamte Unternehmen darstellen, sind einfach und verständlich und können daher ohne Weiteres von jedem Mitarbeiter befolgt werden.

Tax Compliance-Risiken: Verstöße gegen „einzuhaltende Regeln"

MAXIMUM
Regeln, die sämtliche mögliche negative Folgen mit Bezug zum Bereich „Tax" vermeiden

AUFFASSUNG DER FINANZVERWALTUNG
Falls nicht (klar) vorhanden: Auffassung der Finanzverwaltung antizipieren

Was sind die konkret einzuhaltenden Regeln?

MINIMUM
Regeln, die (nur) steuerstrafrechtliche Folgen und/oder Reputationsschäden mit Bezug zum Bereich „Tax" vermeiden

GESETZLICHE VORSCHRIFTEN
(Achtung: häufig Auslegungsfrage!)

wirkt gegen

- Steuernachzahlungen zzgl. Zinsen
- Steuerstrafrechtliche Risiken
- andere „steuerliche Strafzahlungen" (Verspätungszuschläge)
- Reputationsschäden
- Geldbußen gemäß § 30 OWiG

wirkt gegen

- Steuerstrafrechtliche Risiken
- andere „steuerliche Strafzahlungen" (Verspätungszuschläge)
- Reputationsschäden
- Geldbußen gemäß § 30 OWiG
- Risiko der Steuernachzahlung zzgl. Zinsen (als Unternehmens-Risiko) bleibt bestehen!

Es ist jedoch deutlich schwieriger, auch für den steuerlichen Bereich allgemeine Regeln zu definieren, die jeder Mitarbeiter befolgen kann. Stellt man beispielsweise die Regel „Steuergesetze sind zu befolgen“, auf, führt dies dazu, dass trotz oder vielleicht sogar wegen steuerlichem Sachverstand im Unternehmen eine praktische Umsetzung schwierig sein kann.

Gerade im Bereich der Gemeinnützigkeit sind die Gesetzesformulierungen teilweise so unscharf, dass eine Umsetzung in der Praxis aus dem reinen Gesetzeswortlaut zum Teil nicht möglich ist.

Beispielsweise ist der Begriff „wirtschaftlicher Geschäftsbetrieb“, der zur Steuerpflicht im Bereich der Körperschaftsteuer und Gewerbsteuer auch bei gemeinnützigen Einrichtungen führt, zunächst nur eine sehr abstrakte gesetzliche Regelung:

Gesetz:

Ein wirtschaftlicher Geschäftsbetrieb ist eine selbstständige nachhaltige Tätigkeit, durch die Einnahmen oder andere wirtschaftliche Vorteile erzielt werden und die über den Rahmen einer Vermögensverwaltung hinausgeht. Die Absicht, Gewinn zu erzielen, ist nicht erforderlich. (§ 14 AO)

Zur praktischen Umsetzung ist daher zwingend eine Entscheidung in Bezug auf die Interpretation nötig, wobei diese Unterstützung in der Regel – gewissermaßen indirekt – durch die Finanzverwaltung erfolgt. Die von der Finanzverwaltung verfassten Steuerrichtlinien sind eigentlich zunächst nur bindend für die Finanzverwaltung selbst, werden häufig aber gleichlautend auch von den Steuerpflichtigen angewendet. Neben den Richtlinien erlässt die Finanzverwaltung (Bundesfinanzministerium oder auch die Finanzverwaltungen der einzelnen Bundesländer) auch regelmäßig einzelne Schreiben zu bestimmten steuerlichen Sachverhalten. So wird z. B. in einem solchen Schreiben genauer erläutert, wann wirtschaftliche Geschäftsbetriebe bei Krankenhäusern vorliegen:

Finanzverwaltung:

Wirtschaftliche Geschäftsbetriebe bei Krankenhäusern, Verfügung der ODF Frankfurt am Main vom 20.6.2016, Auszug:
2. Personal- und Sachmittelgestellung an eine private Klinik bzw. an eine ärztliche Gemeinschaftspraxis
Auch hinsichtlich der Personal- und Sachmittelgestellung an Dritte ist ein steuerpflichtiger wiG anzunehmen.

Von daher könnte es sich anbieten, das Tax Compliance-Ziel wie folgt zu konkretisieren:

Variante 2:

„Ziel unseres TCMS ist die Erfüllung sämtlicher steuerlicher Pflichten und die Einhaltung der Steuergesetze. Steuerliche Regelverstöße sollen in jedem Fall vermieden werden. Hierzu sind Anweisungen der Finanzverwaltung (Steuererlasse, Steuerrichtlinien, sonstige BMF-Schreiben) zwingend zu befolgen.“

Auch eine derartige Konkretisierung des Zieles führt jedoch in der Praxis zu 2 Problemkreisen:

1. Die Steuergesetzgebung wird immer umfassender und komplexer, auch die Verlautbarungen der Finanzverwaltung zu den einzelnen Paragraphen werden umfangreicher und auch komplizierter. Es ist daher sehr wahrscheinlich, dass einzelnen Mitarbeitern, die mit steuerlichen Aufgaben betraut sind, hier unbeabsichtigte Fehler in der Anwendung der Vorgaben der Finanzverwaltung unterlaufen und daher häufig Compliance-Verstöße auftreten, die auch entsprechend als Compliance-Verstöße mit allen festgelegten Folgen (i. d. R. Meldewege zur Geschäftsführung) zu ahnden wären. Ob dies gewollt und in der Praxis umsetzbar ist, muss bei Festlegung des Ziels bedacht werden.
2. Durch die Vorgabe, sämtliche Anweisungen der Finanzverwaltung auf allen Ebenen im Unternehmen zwingend befolgen zu müssen, würde sich das Unternehmen auch gewisser steuerlicher Chancen berauben. Zumindest für die obere Leitungsebene muss daher die Möglichkeit gegeben sein, Entscheidungen zu treffen, die sich nicht an der momentanen Meinung der Finanzverwaltung orientieren. Denn die Einhaltung der Steuergesetze – die durch ein intaktes Tax CMS gewährleistet werden soll – beinhaltet nicht automatisch die Übernahme der Meinung der Finanzverwaltung in allen Fällen.

Folgende Fälle sind unter anderem denkbar, in denen Steuerpflichtige berechtigterweise abweichende bzw. eigene Auffassungen vertreten könnten:

Ein Gericht (Finanzgericht, Bundesfinanzhof) entscheidet abweichend von der derzeitigen Auffassung der Finanzverwaltung, ggf. veröffentlicht die Finanzverwaltung sogar einen sog. „Nichtanwendungserlass“, dass sie die Rechtsprechung nicht anwendet.

Es kann der Rechtsprechung gefolgt werden.

Weder Finanzverwaltung noch die sog. „herrschende Meinung“ haben einen klaren Rechtsstandpunkt.

Es kann der eigenen Rechtsauffassung gefolgt werden.

Ein klarer Rechtsstandpunkt der Finanzverwaltung oder eine herrschende Meinung in der Literatur sind vorhanden:

Es kann der eigenen Rechtsauffassung gefolgt werden. Die Abweichung muss aber gegenüber dem Finanzamt offengelegt werden.

Gerade im Bereich der gemeinnützigen Einrichtungen oder der juristischen Personen öffentlichen Rechts (Universitäten, Kirchen) gibt der reine Gesetzeswortlaut häufig keinen Aufschluss darüber, wie die praktische Umsetzung erfolgen kann (siehe obiges einfaches Beispiel vom „wirtschaftlichen Geschäftsbetrieb“). Hinweise der Finanzverwaltung sind daher die Regel.

Ob diese aber auf einen konkreten Sachverhalt anzuwenden sind, sollte zumindest kritisch geprüft werden.

Für das oben dargestellte Beispiel eines wirtschaftlichen Geschäftsbetriebes bei Krankenhäusern bedeutet dies Folgendes:

Zum einen ist bereits der Wortlaut der Verfügung der Finanzverwaltung nicht ganz eindeutig. Es ist nicht eindeutig erkennbar, ob mit „Personal- und Sachmittelgestellung an eine private Klinik“ sämtliche fremde Kliniken und Krankenhäuser gemeint sind oder nur tatsächlich „private“ Kliniken im umgangssprachlichen Sinn, also solche, die nicht gemeinnützig sind. Von daher ist nicht klar, ob die Personal- und Sachmittelgestellung an andere gemeinnützige Krankenhäuser nach Auffassung der Finanzverwaltung wirklich einen steuerpflichtigen wirtschaftlichen Geschäftsbetrieb darstellt.

Zudem kann man bei konsequenter Auslegung der Gesetze im Bereich der Gemeinnützigkeit zu dem Ergebnis kommen, dass eine Personal- und Sachmittelgestellung an andere gemeinnützige Einrichtungen nicht als steuerpflichtiger wirtschaftlicher Geschäftsbetrieb anzusehen ist. Hierzu gibt es auch Gerichtsentscheidungen, die dies unterstützen:

Gerichtsentscheidungen:

BFH im Jahr 2010: Personalgestellung kein wiGB, wenn gemeinnützige Einrichtung durch die Überlassung unmittelbar ihre satzungsmäßigen Zwecke verwirklicht

FG Münster im Jahr 2021 (Entscheidung des BFH steht noch aus): Personalgestellung an private ermächtigte Ärzte kein wiGB

Vielleicht wäre daher die Formulierung eines Tax Compliance-Ziels wie folgt denkbar:

Variante 3:

„Ziel unseres TCMS ist die Erfüllung sämtlicher steuerlicher Pflichten und die Einhaltung der Steuergesetze. Soweit aufgrund der Gemeinnützigkeit oder der Rechtsform Steuerbefreiungen oder -ermäßigungen eingeräumt werden, sollen diese möglichst umfassend genutzt werden.“

Das dargestellte Beispiel soll Folgendes verdeutlichen: Bereits bei der Festlegung des Tax Compliance-Ziels, spätestens aber bei Einrichtung der Tax Compliance-Organisation muss berücksichtigt werden, dass sich die Erfüllung der steuerlichen Pflichten immer auf verschiedenen Ebenen abspielt. Auf der einen Seite gibt es steuerliche „formale Regeln“, deren Einhaltung organisatorisch zu regeln ist (z. B. die rechtzeitige Abgabe von Steuererklärungen in allen Bereichen, die rechtzeitige Zahlung der Steuer, usw.). Auf der anderen Seite ist in einigen Bereichen eine unternehmensseitige Steuer-Policy zu bestimmen. Diese kann nicht oder zumindest nur bedingt von jenen Mitarbeitern getroffen werden, die sich um das steuerliche Tagesgeschäft kümmern und daher im Unternehmen als „die Steuerfachleute“ wahrgenommen werden. Denn in diesen Fällen ist mit der Entscheidung für oder gegen eine bestimmte Vorgehensweise bisweilen das Risiko eines Konflikts mit der Finanzverwaltung enthalten, dessen sich die gesetzlichen Vertreter bewusst sein sollten.

Der folgende Fokus-Beitrag in dieser Reihe wird sich daher mit Praxisproblemen der Tax Compliance-Organisation befassen.

Kontakt für weitere Informationen

Anka Neudert
Diplom-Kauffrau, Steuerberaterin,
zertifizierte Beraterin für Gemeinnützigkeit,
Certified Tax Compliance Officer
T +49 911 9193 3583
E anka.neudert@roedl.com

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

Nicht verpassen:

Ab 2022 ausschließlich in digitaler Form

Wir stellen zum nächsten Jahr die Print Version unseres Fokus Gesundheits- und Sozialwirtschaft ein. Selbstverständlich können Sie diesen als E-Mail Version weiterhin kostenfrei dreimal im Jahr beziehen:

Melden Sie sich direkt online dafür an:

www.roedl.de/newsletter-abonnieren

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
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