Rödl & Partner

Potenziale nutzen

Fokus Gesundheits- und Sozialwirtschaft

Informationen für Entscheider im Bereich Gesundheits- und Sozialwirtschaft

Ausgabe: Dezember 2018 – www.roedl.de

Lesen Sie in dieser Ausgabe:

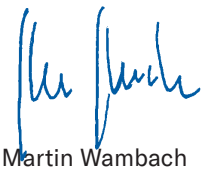
Liebe Leserin, lieber Leser,

ein ereignisreiches Jahr 2018 neigt sich dem Ende entgegen. Ein Top-Thema des Jahres war sicherlich die DSGVO. Ein halbes Jahr nach dem rechtswirksamen Inkrafttreten der EU-Datenschutzgrundverordnung könnte der derzeitige Zustand als „Ruhe vor dem Sturm“ bezeichnet werden. Doch wird diese Ruhe anhalten? Das erste große Bußgeld wurde jüngst in Portugal gegen ein Krankenhaus verhängt – entspannt aufatmen kann man daher wohl noch nicht. Zudem haben nach wie vor viele Unternehmen ihre Hausaufgaben noch nicht vollumfänglich gemacht. Es gibt viele Lücken bei den rechtsverbindlichen Auflagen, viele Prozesse sind aktuell noch schleppend und viele Mitarbeiter sind unzureichend geschult … Man muss kein Spezialist sein, um zu sehen, dass 2019 noch einige Herausforderungen auf die unternehmerische Welt zukommen.

Was wird das neue Jahr für die Gesundheits- und Sozialwirtschaft bereithalten? Einige große Themen sind bereits bekannt, wie zum Beispiel das „Baby“ unseres Gesundheitsministers Jens Spahn: das Pflegestärkungsgesetz. Viel wird versprochen durch diese gesetzliche Neuerung: mehr Unterstützung für pflegende Angehörige, Personaluntergrenzen, attraktivere Ausbildung, grundsätzlich mehr Personal. Wir dürfen gespannt sein, wie sich diese Vorhaben in der Realität für Krankenhäuser, Betreiber, Pfleger, Gepflegte und alle Beteiligten auswirken wird. Außerdem hat auch die Digitalisierung wieder ein neues To-do im Gepäck: Ab November 2019 müssen viele Unternehmen in der Lage sein, sogenannte X-Rechnungen empfangen zu können. Wer hier jetzt denkt, ein normales E-Mail-Postfach würde für den Empfang, die Verarbeitung und Dokumentation ausreichen, der irrt sich leider. Wir können uns also einer Sache sicher sein: Langweilig wird es nicht!

Doch zunächst wünschen wir Ihnen und Ihren Familien eine besinnliche Weihnachtszeit und einen ruhigen Jahresausklang.

Bis zum nächsten Jahr!



Martin Wambach
Geschäftsführender Partner

Bernd Vogel
Partner

Assurance & IT

› Elektronische Rechnungsverarbeitung wird Pflicht: Sind Sie vorbereitet?

Von Jana Wollmann und Jürgen Schwestka

Woher kommt die Pflicht?

Durch die EU-Richtlinie 2014/55/EU werden alle öffentlichen Auftraggeber dazu verpflichtet, elektronische Rechnungen empfangen und verarbeiten zu können. In Deutschland beschloss der IT-Planungsrat am 22. Juni 2017, dass öffentliche Auftraggeber zukünftig den Standard XRechnung empfangen und verarbeiten können müssen.

Dieser basiert auf einer nationalen Ausgestaltung der europäischen Norm CEN 1693. Es erfolgt dabei die Datenübertragung nur noch als strukturierter Datensatz oder als hybride Rechnung, sofern die Rechnung den rechtlichen Vorgaben entspricht. Im Sinne der EU-Richtlinie sind eine eingescannte Papierrechnung, eine reine PDF-Datei ohne strukturierte Daten oder eine Bilddatei keine elektronischen Rechnungen.

Wer ist davon betroffen?

Von der Umstellung sind zunächst einmal die obersten Bundesbehörden betroffen. Für sie treten die entsprechenden Vorschriften ab dem 27. November 2018 in Kraft.

Für alle anderen öffentlichen Auftraggeber tritt die Verpflichtung erst ab dem 27. November 2019 in Kraft (§ 11 Abs. 1 u. 2 E-Rech-VO).

Nach § 2 Abs. 6 E-Rech-VO sind „subzentrale öffentliche Auftraggeber“ alle (sonstigen) öffentlichen Auftraggeber, die keine obersten Bundesbehörden oder Verfassungsorgane des Bundes sind. Wer der öffentliche Auftraggeber ist, wird dabei im § 99 Nr. 1-4 GWB geregelt. Danach sind öffentliche Auftraggeber:

1. Gebietskörperschaften, sowie deren Sondervermögen; hierzu zählen vor allem Länder, Landkreise, Gemeinden und deren Sondervermögen (Beispiele: kommunale Eigenbetriebe oder nicht-rechtsfähige Stiftungen).
2. Andere juristische Personen des öffentlichen und des privaten Rechts, die zu dem besonderen Zweck gegründet wurden, im Allgemeininteresse liegende Aufgaben nichtgewerblicher Art zu erfüllen, sofern
   - sie überwiegend von Stellen nach Nummer 1 oder 3 einzeln oder gemeinsam durch Beteiligung oder auf sonstige Weise finanziert werden,
   - ihre Leitung der Aufsicht durch Stellen nach Nummer 1 oder 3 unterliegt oder
   - mehr als die Hälfte der Mitglieder eines ihrer zur Geschäftsführung oder zur Aufsicht berufenen Organe durch Stellen nach Nummer 1 oder 3 bestimmt worden sind.
3. Verbände, deren Mitglieder unter Nummer 1 oder 2 fallen; Hierunter fallen z. B. rechtsfähige Verbände, aber auch Kooperationen in Form von Arbeits- oder Einkaufsgemeinschaften.
4. Natürliche oder juristische Personen des privaten Rechts sowie juristische Personen des öffentlichen Rechts, soweit sie nicht unter Nummer 2 fallen, in den Fällen, in denen sie für Tiefbaumaßnahmen, für die Errichtung von Krankenhäusern, Sport-, Erholungs- oder Freizeiteinrichtungen, Schul-, Hochschul- oder Verwaltungsgebäuden oder für damit in Verbindung stehende Dienstleistungen und Wettbewerbe von Stellen, die unter die Nummern 1, 2 oder 3 fallen, Mittel erhalten, mit denen diese Vorhaben zu mehr als 50 Prozent subventioniert werden.

Dabei umfasst der Begriff der Errichtung auch Rekonstruktionen, Modernisierungen, Sanierungen, Erweiterungen sowie alle sonstigen baulichen Änderungen.

Der Begriff des Krankenhauses umfasst alle Einrichtungen, die der Erbringung medizinischer (Akut-)Versorgung dienen. Des Weiteren sind hierunter auch solche Einrichtungen zu subsumieren, die medizinische Leistungen erbringen und zumindest bestimmte Personengruppen stationär aufnehmen können. Zuletzt fällt hierunter auch jede Einrichtung, die eine nicht lediglich unerhebliche medizinische Versorgung gewährleistet, beispielsweise Alters- und Pflegeheime, Hospize oder Einrichtungen zur Betreuung und medizinischen Versorgung von Behinderten.

Was bedeutet dies für Öffentliche Auftraggeber?

Öffentliche Auftraggeber müssen ab dem 27. November 2019 Rechnungen in elektronischer Form im Format XRechnung empfangen und verarbeiten können. Hierbei handelt es sich um xml-Dateien, die die Rechnungsinformationen in strukturierter Form enthalten. Das Auslesen der Rechnungsinformationen per Texterkennung (OCR) und die anschließende Interpretation entfallen damit zukünftig, denn für jedes Datenfeld der XRechnung ist eindeutig definiert, was es bedeutet. Das Fehlerrisiko wird damit geringer.

Die E-Rech-VO schreibt in § 4 Absatz 3 vor, dass für die Übermittlung von elektronischen Rechnungen die Nutzung eines Verwaltungsportals vorgegeben ist. Auf Bundesebene wird eine zentrale Rechnungseingangsplattform entwickelt, die es ermöglichen soll, den elektronischen Rechnungseingang zu bewältigen.

Darüber hinaus soll aber sogar auf Bundesebene der Rechnungsempfang per E-Mail möglich sein. Weiterhin gibt es neben der XRechnung auch hybride Formate wie ZUGFeRD 2.0. Diese bestehen aus einer PDF-Datei mit eingebundenen strukturierten Rechnungsinformationen (XML). Die Besonderheit ist hierbei, dass die Rechnung sowohl die bildlichen Informationen wie eine klassische PDF-Rechnung enthält und gleichzeitig die Rechnung in Übereinstimmung mit der Norm CEN 1693. Allerdings muss sichergestellt werden, dass die beiden Rechnungen übereinstimmen und es muss nachvollziehbar sein, auf Basis welcher Rechnungsinformation die Buchung erfolgte.

Archivierung und Aufbewahrung von elektronischen Rechnungen richten sich nach den Vorgaben des UStG, der Abgabenordnung sowie der GoBD (BMF vom 14. November 2014). Elektronische Rechnungen sind demnach vom Steuerpflichtigen über die gesetzliche Aufbewahrungsfrist von mindestens 10 Jahren aufzubewahren. Über diesen Zeitraum sind die Echtheit der Herkunft, die Unversehrtheit des Inhalts und die Lesbarkeit der Rechnung zu gewährleisten.

Im Falle von ZUGFeRD 2.0 oder sonstigen CEN-konformen elektronischen Rechnungen, die per E-Mail übermittelt werden, wird ein revisionssicheres elektronisches Archiv inkl. Workflowsteuerung zur Prüfung und Freigabe der Belege benötigt. Ein Ausdruck der elektronischen Rechnung und Archivierung in Papierform wäre ein Medienbruch und somit nicht GoBD-konform.

Welche Pflichten ergeben sich als Dienstleister/Lieferant Öffentlicher Auftraggeber?

Alle Lieferanten der Öffentlichen Auftraggeber werden verpflichtet, elektronische Rechnungen auszustellen und zu übermitteln (§ 3 E-Rech-VO). Die Verpflichtung hierzu besteht ab dem 27. November 2020 (§ 11 Abs. 3 E-Rech-VO).

Hierbei muss es sich nicht nur um die Lieferung von Waren handeln, sondern es betrifft auch die Erbringung von Dienstleistungen. Voraussetzung für die Verpflichtung ist, dass die Beauftragung durch den Öffentlichen Auftraggeber erfolgte.

Kontakt für weitere Informationen:

Jana Wollmann
Rechtsanwältin
Tel.: +49 (2 21) 94 99 09-436
E-Mail: jana.wollmann@roedl.com

Jürgen Schwestka
Diplom-Kaufmann (Univ.), IT-Security-Manager/Auditor, CISA, IT Auditor IDW
Tel.: +49 (9 11) 91 93-35 08
E-Mail: jürgen.schwestka@roedl.com

Assurance & IT

› Prüfnachweis Kritische Infrastrukturen (KRITIS) nach § 8a BSIG

Von Jürgen Schwestka

Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) ist am 25. Juli 2015 als Artikelgesetz in Kraft getreten. Als Kernbestandteil sehen die neu eingefügten §§ 8a und 8b des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz/BSIG) vor, dass informationstechnische Systeme, die für die Funktionsfähigkeit von Kritischen Infrastrukturen maßgeblich sind, von den jeweiligen Betreibern durch die Umsetzung von angemessenen organisatorischen und technischen Vorkehrungen abzusichern sind und dass erhebliche IT-Vorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden sind.

Spiegelbildlich zu den besonderen Pflichten ergeben sich aus den §§ 3 Absatz 3 und 8b Absatz 2 Nummer 4 BSIG für Betreiber Kritischer Infrastrukturen besondere Rechte. Diese beinhalten insbesondere die privilegierte Beratung und Information durch das BSI.

Nach § 2 Absatz 10 Nummer 1 in Verbindung mit § 10 Absatz 1 Satz 1 BSIG ist zu bestimmen, welche Anlagen in den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen als Kritische Infrastrukturen gelten.

Mit der am 3. Mai 2016 in Kraft getretenen BSI-Kritisverordnung (BSI-KritisV) wurden bereits die Festlegungen zur Bestimmung Kritischer Infrastrukturen in den Sektoren Energie, Wasser, Ernährung und Informationstechnik und Telekommunikation (IKT) getroffen. Die noch ausstehenden Festlegungen für die Sektoren Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr wurden am 30. Juni 2017 mit der „Ersten Verordnung zur Änderung der BSI-Kritisverordnung“ getroffen.

Was sind Kritische Infrastrukturen?

Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen einträten.

In Deutschland werden folgende Sektoren (und Branchen) den Kritischen Infrastrukturen zugeordnet:

- Transport und Verkehr (Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik)
- Informationstechnik und Telekommunikation
- Finanz- und Versicherungswesen (Banken, Versicherungen, Finanzdienstleister, Börsen)
- Staat und Verwaltung (Regierung und Verwaltung, Parlament, Justizeinrichtungen, Notfall- und Rettungswesen einschließlich Katastrophenschutz)
- Ernährung (Ernährungswirtschaft, Lebensmittelhandel)
- Wasser (öffentliche Wasserversorgung, öffentliche Abwasserbeseitigung)
- Gesundheit (medizinische Versorgung, Arzneimittel und Impfstoffe, Labore)
- Energie (Elektrizität, Mineralöl, Gas)
- Medien und Kultur (Rundfunk – Fernsehen und Radio), gedruckte und elektronische Presse, Kulturgut, symbolträchtige Bauwerke)

Als Kritische Infrastrukturen gelten aber nicht die Unternehmen oder Abteilungen als Gesamtheit, sondern einzelne technische Anlagen, die eine für die Bevölkerung kritische (Dienst-) Leistung erbringen. Um als kritisch zu gelten, muss diese Anlage einen bestimmten Schwellwert überschreiten. Anlagen unterhalb dieses Schwellwerts müssen zum heutigen Zeitpunkt noch nicht beachtet werden. Im Bereich Gesundheit sehen die Schwellwerte u. a. wie folgt aus:

- 30.000 vollstationäre Fälle pro / Jahr
- Herstellung oder Abgabe von Medizinprodukten mit einem Umsatz von mehr als 90.680.000 Euro pro Jahr
- 34.000 in Verkehr gebrachte Blutkonserven pro Jahr

Zum Schutz der Bevölkerung muss somit sichergestellt werden, dass kritische Dienstleistungen uneingeschränkt zur Verfügung stehen. Es ist daher davon auszugehen, dass in den kommenden Jahren der Schwellwert nach unten angepasst wird, um eine breitere Basis als Kritische Infrastruktur zu definieren und somit mehr Versorgungssicherheit zu ermöglichen.

Was müssen Betreiber Kritischer Infrastrukturen beachten?

Mit Ausnahme von „Staat und Verwaltung“ sowie „Medien und Kultur“ müssen diese Sektoren ihre Vorkehrungen (siehe § 8a (1) BSIG) nach Stand der Technik zur Vermeidung von Störungen gegenüber dem BSI nachweisen. Dieser Nachweis ist alle 2 Jahre zu erbringen.

Eine Zertifizierung nach ISO 27.001 ist hierbei nicht ausreichend, da bei einer ISO-Zertifizierung bestimmte Risiken in Kauf genommen werden können, bei einer Kritischen Infrastruktur dies aber explizit ausgeschlossen ist. Auch müssen der Geltungsbereich (Scope) der ISO-Zertifizierung und der Kritischen Infrastruktur nicht deckungsgleich sind.

Was ist der Geltungsbereich der Prüfung?

Der Definition des Scopes kommt eine große Bedeutung zu. Der Scope umfasst die informationstechnischen Systeme, Komponenten und Prozesse, Rollen sowie Personen, die für die Funktionsfähigkeit der vom Betreiber betriebenen Kritischen Infrastruktur maßgeblich sind oder auf diese Einfluss haben.

Zum Geltungsbereich gehören immer die Systeme, Komponenten und Prozesse

- der kritischen Dienstleistung (kDL),
- die die kDL direkt unterstützen und
- von denen die kDL indirekt abhängig ist,

z. B. bei deren Ausfall, Störung oder Angriff es zu einer Beeinträchtigung der kDL kommen könnte.

Der Scope sollte zum einen nicht zu groß gewählt werden, da sich hierdurch automatisch der Aufwand für den Prüfnachweis nach § 8a BSIG deutlich erhöht und zum anderen darf er aber auch nicht zu klein gewählt sein, um nicht Kritische Infrastrukturen zu vergessen.

Es bietet sich daher an, eine vorgelagerte Beurteilung des Geltungsbereiches im Rahmen einer GAP-Analyse durchzuführen. Dabei wird beurteilt, ob der Geltungsbereich sinnvoll gewählt wurde und ob für die darin enthaltenen Kritischen Dienstleistungen geeignete Maßnahmen vorhanden sind. Auf diese Weise kann vorab beurteilt werden, in welchen Bereichen noch Handlungsbedarf besteht, sodass dieser bis zur eigentlichen Prüfung behoben werden kann.

Was sind die Kriterien für die Prüfung?

Ein großes Problem ist zum aktuellen Zeitpunkt, dass es bis auf den Bereich Wasser noch keinen einheitlichen Branchenstandard gibt, den man vergleichsweise prüfen könnte. Es ist aber davon auszugehen, dass die Berichte aufgrund fehlender offizieller Prüfkriterien und einer größeren Anzahl von Prüfstellen extrem unterschiedlich ausfallen und sich auch bei Häusern vergleichbarer Art unterscheiden werden.

Da bisher nur für eine Branche ein einheitlicher Branchenstandard existiert, entwickelt Rödl & Partner derzeit in Zusammenarbeit mit dem Institut der Wirtschaftsprüfer (IDW) und dem BSI einen Prüfkriterienkatalog ergänzend zum IDW Prüfungsstandard 860, der für die einzelnen Bereiche Soll-Vorgaben definiert und als Mindeststandard für KRITIS-Prüfungen gelten soll. So soll sichergestellt werden, dass die Prüfungen auch bei unterschiedlichen Prüfgesellschaften vergleichbar sind und ein gewisses Mindestniveau erfüllen.

Wie sollte man im Rahmen einer KRITIS-Prüfung vorgehen?

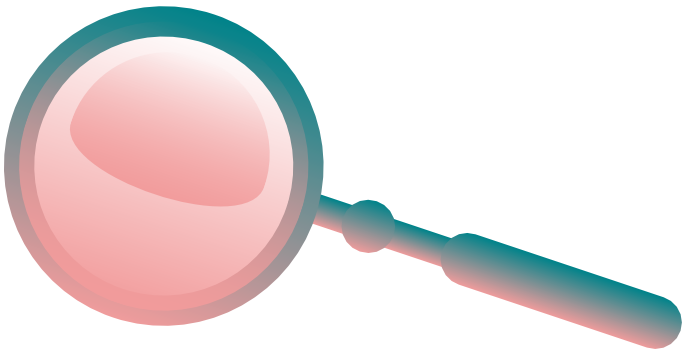
In einem ersten Schritt erfolgt die Prüfung des Geltungsbereiches. Im Idealfall ist dieser bereits im Rahmen einer GAP-Analyse untersucht worden, sodass es kurz vor der Meldefrist an das BSI zu keinen bösen Überraschungen kommen kann.

Im Gegensatz zur oberflächlichen GAP-Analyse erfolgt bei der eigentlichen Prüfung eine detaillierte Überprüfung, ob die einzelnen Anforderungen erfüllt sind. Eventuell gefundene Mängel müssen im Prüfungsbericht festgehalten und, sofern sie einen gewissen Schweregrad besitzen, an das BSI gemeldet werden.

Sind Sie von der Prüfpflicht betroffen, sollten Sie unbedingt einen ausführlichen Prüfungsbericht verlangen, in dem der Geltungsbereich, das Vorgehen in der Prüfung, die gefundenen Risiken und eine Bewertung des Prüfers genau und nachvollziehbar dargestellt sind. Nur dann ist im Falle eines Ausfalls der Kritischen Dienstleistung die Unternehmensführung in einer besseren Beweislage, dass alle festgestellten Punkte erkannt und angegangen wurden bzw. angegangen werden.

Kontakt für weitere Informationen:

Jürgen Schwestka
Diplom-Kaufmann (Univ.), IT-Security-Manager/Auditor,
CISA, IT Auditor IDW
Tel.: +49 (9 11) 91 93-35 08
E-Mail: jürgen.schwestka@roedl.com



Datenschutz

› Erleichterungen bei der Führung des Nachweises durch unabhängige Bescheinigungen zur Konformität des Datenschutzmanagements

Von Christoph Naucke

Mit Einführung der DSGVO wurden mehrere Schritte auf einmal vollzogen, die es in der Summe wesentlich anspruchsvoller für die Unternehmen machen, erheblichen Schaden von ihrem Unternehmen abzuwenden: Die Bußgeldvorschriften wurden drakonisch verschärft, im Falle einer Panne wird dem Betroffenen ein Recht auf Schadensersatz zugesichert, und gleichzeitig wird dem Verantwortlichen die Beweislast dafür auferlegt, rechtskonform gehandelt zu haben. Daher kommt dem Nachweis eines tatsächlich funktionierenden Datenschutz-Managements, möglichst in Form einer Referenz von unabhängiger Stelle, eine wachsende Bedeutung zu. Dafür eignen sich Bescheinigungen eines Wirtschaftsprüfers, beispielsweise eine IT-Prüfung außerhalb der Abschlussprüfung oder auch eine spezifische, fokussierte Prüfung der Datenschutz-Compliance.

Die gesetzlichen Vertreter einer Organisation sind dafür verantwortlich, Maßnahmen zu ergreifen, um das rechtskonforme Verhalten der Organisation zu gewährleisten. Anderenfalls besteht der Verdacht auf ein betriebliches Organisationsverschulden. Viele wissen dabei gar nicht, dass die Haftung auch solche gesetzlichen Vertreter trifft, die lediglich ehrenamtlich tätig sind. Es besteht also auch ein Risiko für den nebenamtlichen Vereinsvorstand! Dieser Grundsatz wurde in der EU Datenschutz-Grundverordnung dadurch unterstrichen, dass in Art. 5 Absatz 2 der Verantwortliche (also typischerweise das Unternehmen bzw. die Organisation) die Pflicht auferlegt bekommt, dass er die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nachweisen kann (faktische Beweislastumkehr).

Nachdem Ende September eine erneute massive Sicherheitslücke für Facebook-Nutzer bekannt wurde, wird aktuell über das erste empfindliche Bußgeld auf Basis der DSGVO spekuliert. Unternehmen der Sozial- und Gesundheitswirtschaft verarbeiten oft in großem Umfang sog. „besondere“, also besonders sensible Daten nach der Definition der DSGVO (u. a. Gesundheitsdaten, Art. 9). Es wäre kaum überraschend, wenn sich u. a. in diesem Bereich ein Tätigkeitsschwerpunkt der Landesdatenschutzbehörden entwickeln würde.

Der bayerische Landesbeauftragte für den Datenschutz schreibt beispielsweise schon in seinem Tätigkeitsbericht für das Jahr 2016 mit Bezug zum Art. 27 des Bayerischen Krankenhausgesetzes: „Gerade in Krankenhäusern entstehen zunehmend große Mengen an Daten, die die Gesundheit der Patientinnen und Patienten und damit deren intimsten Lebensbereich betreffen. Für diese Daten ist es durchaus angemessen, strengere Schutzmaßnahmen zu fordern. Durch die Beteiligung externer Stellen wird der Kreis derer größer, die mit sensiblen medizinischen Daten in Berührung kommen. Gleichzeitig sinken die direkten Einflussmöglichkeiten der Krankenhäuser auf den Umgang mit den Daten ihrer Patientinnen und Patienten. Das kann das Risiko von Datenmissbrauch und Datenverlust in einem besonders sensiblen Bereich erhöhen.“

Angesichts einer sehr anspruchsvollen Regelungsdichte der DSGVO und der zahlreichen weiteren einschlägigen Rechtsnormen wird auch der Nachweis der Konformität für die betroffenen Unternehmen erheblich anspruchsvoller. Zum Anforderungskatalog zählen beispielsweise:

- Der Nachweis angemessener technischer und organisatorischer Maßnahmen nach dem aktuellen Stand der Technik,
- der umfassende Nachweis der Verarbeitungstätigkeiten einschließlich des Nachweises, welchen Zweck diese erfüllen und auf welcher Rechtsgrundlage sie erfolgen,
- die zuverlässige Umsetzung der Auskunfts- und Löschungsrechte der Betroffenen,
- der Nachweis über die gegebenenfalls zuverlässige, fristgerechte Meldung einer Datenpanne,
- der Nachweis, dass Mitarbeiter zum Datenschutz verpflichtet und dass sie unterwiesen worden sind,
- die Vorlage der notwendigen Vereinbarungen zur Auftragsverarbeitung,
- der Nachweis, dass für die Datenweitergaben, für die Einwilligungserklärungen erforderlich sind, diese Einwilligungserklärungen systematisch eingeholt werden (in Krankenhäusern betrifft dies beispielsweise Übermittlungen an Vor- und Nachbehandler, Seelsorger, Pfortenauskunft, Angehörigenauskunft)
- der Nachweis, dass die Mitarbeiter im Bedarfsfall schnell prüfen können, ob die betreffende Einwilligung tatsächlich vorliegt,

- die Ermittlung der wichtigsten Datenschutzrisiken aus Betroffenensicht zur Auswahl derjenigen Verarbeitungstätigkeiten, für die eine Datenschutzfolgenabschätzung zu erstellen ist und schließlich
- die Vorlage der erforderlichen Datenschutzfolgenabschätzungen.

Nachweispflicht der DSGVO heißt nichts anderes als Datenschutz-Compliance-Management

Damit entsteht im Bereich Datenschutz nichts anderes als die Notwendigkeit, ein funktionierendes Compliance-Management, also ein Datenschutz-Compliance-Management, belegen zu können. Denn der Inhalt von Compliance ist genau durch die (nachgewiesene) Einhaltung gesetzlicher und interner Regelungen und Standards definiert. Bei der Übersetzung der notwendigerweise allgemein gehaltenen Anforderungen der DSGVO in die betriebliche Praxis spielen die für das Unternehmen und seine Prozesse angemessenen TOMs, die technischen und organisatorischen Maßnahmen also, eine zentrale Rolle. Hier gibt es branchen- und risikospezifische Anhaltspunkte, die man berücksichtigen sollte. Eine funktionierende Datenschutz-Compliance bedeutet, dass die tatsächliche Einhaltung der unternehmensbezogen definierten Standards nachgewiesen werden kann.

Die Bescheinigung eines Wirtschaftsprüfers über die Wirksamkeit eines Compliance-Management-Systems (CMS) bedeutet wertvolle Anhaltspunkte nach außen hin für den Fall, dass trotz aller Maßnahmen dennoch einmal etwas schiefläuft und eine Datenpanne geschieht. Das Institut der Wirtschaftsprüfer (IDW) hat mit dem Prüfungsstandard 980 einen Standard gesetzt, anhand dessen die Fragestellung nach der Wirksamkeit eines CMS beantwortet und als Ergebnis eine entsprechende Bescheinigung erlangt werden kann.

Die Prüfung des CMS nach diesem Prüfungsstandard 980 kann auf bestimmte Unternehmensfunktionen eingeschränkt werden. Deshalb eignet sich der Standard u. a. gut dafür, eine gezielte Prüfung des Datenschutz-Compliance-Managementsystems mit anschließender Bescheinigung durchzuführen. Die Prüfung kann als Konzeptions-, als Angemessenheits- oder als Wirksamkeitsprüfung definiert werden. Ziel einer umfassenden Wirksamkeitsprüfung ist es festzustellen, ob die definierten Grundsätze und Maßnahmen gemäß der Konzeption des CMS angemessen sind, ob sie zu einem bestimmten Zeitpunkt implementiert und in einem zu bestimmenden Prüfungszeitraum auch wirksam waren. Für den Fall einer spezifischen Datenschutz-CMS-Prüfung umfasst diese sowohl organisatorische als auch technische Aspekte eines Datenschutz-CMS.

Bescheinigung der Datenschutz-Compliance in einem abgrenzbaren IT-System: PS 860 als Alternative zum PS 980

Wenn eine Bescheinigung mit Bezug zu bestimmten IT-Systemen angestrebt wird, eignet sich eine Prüfung nach dem IDW Prüfungsstandard 860 für IT-Prüfungen außerhalb der Abschlussprüfung. Mit dem neu erschienenen IDW Prüfungshinweis 9.860.1 konkretisiert das IDW die Prüfkriterien im Rahmen solcher Prüfungen nach dem IDW PS 860 mit Blick auf datenschutzspezifische Besonderheiten. Die Prüfung kann als Angemessenheitsprüfung und als Wirksamkeitsprüfung gestaltet werden. Ziel einer Angemessenheitsprüfung ist es festzustellen, ob die angewandten Grundsätze, Verfahren und Maßnahmen geeignet sind, die durch das IDW erstellten Kriterien einzuhalten und ob sie zum relevanten Prüfzeitpunkt im Unternehmen implementiert sind. Ziel der Wirksamkeitsprüfung ist über die Angemessenheitsprüfung hinaus zu beurteilen, ob die in der Erklärung zum IT-System dargestellten Grundsätze, Verfahren und Maßnahmen des zu prüfenden IT-Systems in dem zu prüfenden Zeitraum wirksam gewesen sind.

Da sich das Datenschutz-Management-System des Unternehmens letztlich in der Gesamtheit dieser Grundsätze, Verfahren und Maßnahmen manifestiert, wird mit der Prüfung daher eine externe, unabhängige Aussage zur Angemessenheit, zum Stand der Implementierung sowie gegebenenfalls zur Wirksamkeit des Datenschutz-Management-Systems im Unternehmen getroffen. Sie kann daher ebenfalls ein wertvoller Baustein bei der Führung des Nachweises sein, den die DSGVO vom Verantwortlichen fordert.

Aufgrund der Ausrichtung des zugrundeliegenden IDW PS 860 für IT-Prüfungen sind Prüfungen nach diesem Standard naturgemäß besonders dafür geeignet, Sicherheit über die Angemessenheit und den Implementierungsstand der notwendigen Schutzmaßnahmen (technische und organisatorische Maßnahmen, TOMs) zu erlangen. Damit steht ein zusätzliches Werkzeug mit gegebenenfalls besonderem Schwerpunkt auf die TOMs und zur Erlangung einer entsprechenden Bescheinigung zur Verfügung.

Welche Kriterien im Rahmen einer Angemessenheitsprüfung heranzuziehen sind, ergibt sich zunächst aus den in der DSGVO sowie dem BDSG dargestellten Grundsätzen. Hierauf aufbauend hat das IDW einen Anforderungskatalog entwickelt, der diese Grundsätze im Zusammenhang mit der Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen konkretisiert. Im Ergebnis sind die von den gesetzlichen Vertretern des Unternehmens getroffenen Grundsätze, Verfahren und Maßnahmen den rechtlichen Kriterien gegenüberzustellen und auf ihre Angemessenheit und gegebenenfalls Wirksamkeit hin zu überprüfen. Diese Überprüfung kann

durch eine geeignete Aufbau- und Funktionsprüfung erfolgen. Darüber hinaus ist eine Risikobeurteilung durchzuführen.

Bescheinigungen aufgrund von Prüfungen, die als CMS-Prüfungen (PS 980) oder auch als Systemprüfungen (PS 860) ausgestaltet sind, unterliegen, genau wie andere Testate und Bescheinigungen eines Wirtschaftsprüfers, der Berufspflicht der Unabhängigkeit. Gleichzeitig unterstützt der Prüfungsprozess oftmals beim Aufdecken und Beseitigen noch unbemerkter Schwachstellen und bietet damit im Anschluss an die Prüfung eine wesentlich verbesserte Ausgangslage, um den Nachweis der Einhaltung der Grundsätze der DSGVO zu führen.

Kontakt für weitere Informationen:

Christoph Naucke
Betriebswirt (BA), Compliance Officer,
zertifizierter Datenschutzbeauftragter DSB
Tel.: +49 (9 11) 91 93-36 28
E-Mail: christoph.naucke@roedl.com

Datenschutz

› E-Health: Ist der professionelle Einsatz von Gesundheits-Apps im ärztlichen Bereich aufgrund der neuen Datenschutzgrundverordnung nur noch ein Wunschdenken?

Von Christoph Naucke und Lana Dachlauer-Baron

Der datenschutzkonforme Einsatz von Gesundheits-Apps durch niedergelassene Ärzte und durch Krankenhaus-Ärzte erweist sich auf den ersten Blick als schwierig, da die Apps zu erheblichen rechtlichen Risiken führen können. Die Regelungen der EU-Datenschutzgrundverordnung bestimmen die Anforderungen an den Umgang mit solchen Apps und sollten genau beachtet werden.

Gesundheits-Apps sind heutzutage auch in der ärztlichen Diagnose und Therapie kaum noch aus dem Alltag wegzudenken. Immer mehr Krankenhäuser möchten die fortschreitende Digitalisierung und die mit ihr einhergehende Effizienz für sich nutzen. Kein Wunder, dass sich Krankenhäuser häufig für die Einführung solcher Apps entscheiden. Im Bereich der Patientenversorgung lässt sich eine Reihe von Beispielen finden: So kann der behandelnde Arzt mittels eines ausgerüsteten Handys die Wundheilung analysieren, fürs eigene Auge vergrößern und in Echtzeit an ein anderes Endgerät zur weiteren Beobachtung oder an die jeweilige Station schicken. Bei akut oder schwer erkrankten Patienten können aktuelle Informationen über deren Vitaldaten von Bedeutung sein.

Rechtfertigen die Chancen die damit einhergehenden Datenschutz-Risiken?

Die Vorteile des Einsatzes liegen klar auf der Hand: Hervorragende Vernetzungsmöglichkeiten und damit einhergehende gesteigerte Effizienz und Kostenreduktion durch individuell zugeschnittene Versorgung. Im Mittelpunkt steht dabei das Sammeln, Senden sowie Verarbeiten patientenbezogener Daten in Echtzeit. Der Nachteil: ein Graus für alle Datenschützer angesichts der neuen EU-Datenschutzgrundverordnung, zumindest auf den ersten Blick.

Tatsächlich darf nicht außer Acht gelassen werden, dass es sich bei Gesundheitsdaten um hoch sensible Daten handelt, die einen besonderen Schutz erfordern. Solche Daten können für gewöhnlich über den Gesundheitszustand, Lebenswandel sowie über intimste Details umfassend Aufschluss geben.

Krankenhäuser müssen bei der Einführung solcher Gesundheits-Apps beachten, dass, dass hierbei personenbezogene Daten verarbeitet werden. Das bedeutet, dass die Vorschriften der EU-Datenschutzgrundverordnung Anwendung finden, sodass Krankenhäuser für den Einsatz solcher Apps eine Erlaubnisvorschrift aus der EU-Datenschutzgrundverordnung vorweisen müssen. Auch ist es erforderlich, die Einhaltung technischer und organisatorischer Maßnahmen gemäß der datenschutzrechtlichen Bestimmungen sicherzustellen. Zudem ergeben sich Informationspflichten gegenüber den Patienten.

Werden technische und organisatorische Maßnahmen nicht gewährleistet, kann es zu einer unbefugten Offenlegung der Daten kommen. Ebenfalls besteht die Gefahr, dass Datenflüsse nicht mehr kontrolliert werden können und hierdurch den betroffenen Patienten materielle und immaterielle Schäden entstehen. Nicht auszudenken sind die Folgen der unberechtigten Offenlegung von Krankheiten, beispielsweise gegenüber dem Arbeitgeber oder der Öffentlichkeit. Patientenbezogene Daten, die auf die Lebenserwartung schließen lassen, könnten für Kreditinstitute von Relevanz sein. Ebenfalls könnte es zu einer Flut an Spam-Nachrichten zu bestimmten Medikamenten oder Therapiemethoden kommen. Von erheblicher Bedeutung ist in diesem Zusammenhang auch das Interesse der Versicherungswirtschaft, da Gesundheitsinformationen in allen Personenversicherungssparten einen großen Einfluss auf die Risikoeinstufung und damit die Prämienhöhe oder gar den Ausschluss vom Versicherungsschutz haben. Schafft es also das Krankenhaus nicht, die Datenflüsse in der App unter seiner Kontrolle zu behalten, könnten die offengelegten Daten von verschiedenen Akteuren genutzt und vor allem ausgenutzt werden.

Angesichts der dargestellten Szenarien wird schnell deutlich, dass bereits bei der Konzeption einer solchen App, aber auch bei deren Einsatz durch den Verantwortlichen besonders auf die datenschutzrechtlichen Aspekte, also auf geeignete technische und organisatorische Maßnahmen geachtet werden muss.

Wie schaut es derzeit auf dem Markt der Gesundheits-Apps im professionellen Kontext tatsächlich aus?

Derzeit existiert ein breites Spektrum an Gesundheits-Apps mit Einsatzmöglichkeiten im professionellen Kontext. Im Vergleich zu herkömmlichen medizinischen Geräten zur Unterstützung in der Diagnostik stellen die Gesundheits-Apps nur selten Medizinprodukte dar. Dies ist deswegen wichtig, weil sich Hersteller von Medizinprodukten den besonderen Anforderungen des Medizinproduktgesetzes und zahlreichen weiteren Rechtsverordnungen unterwerfen müssen.

Dabei sind Medizinprodukte gemäß § 3 Nr. 1 MPG alle einzeln oder miteinander verbunden verwendeten Instrumente, Software (...) oder andere Gegenstände einschließlich der vom Hersteller speziell zur Anwendung für diagnostische oder therapeutische Zwecke bestimmten und für ein einwandfreies Funktionieren des Medizinproduktes eingesetzten Software. Zudem muss der Hersteller den Zweck des Medizinprodukts ganz klar auf die Vorsorge, Diagnostik und Therapie ausrichten (siehe § 3 Nr. 1 MPG). Sobald also der Hersteller den vorgenannten Zweck bestimmt hat, unterliegen Apps den strengen Zertifizierungsanforderungen des MPG, sodass eine staatliche Kontrolle über das Inverkehrbringen der Apps gewährleistet ist. Während des Zertifizierungsprozesses werden jedoch die datenschutzrechtlichen Aspekte des Öfteren kaum hinreichend berücksichtigt, ebenfalls wird eine Prüfung von Übertragungswegen oder Netzkomponenten nicht vorgenommen. Das bedeutet, dass aus einer bestehenden Zertifizierung nach MPG nicht zwangsläufig auch auf die vollständige Einhaltung datenschutzrechtlicher Bestimmungen geschlossen werden kann.

Zusätzlich zu der Beurteilung, ob eine Klassifizierung der jeweiligen App als ein Medizinprodukt vorliegt, stellt sich die Frage, welche datenschutzrechtlichen Maßnahmen bislang ergriffen wurden.

Gemäß einiger vorliegender Studien zeichnet sich ein eher düsteres Bild ab: Auf der einen Seite sind fehlende oder fehlerhafte Verschlüsselung, ungeschützte Übertragung von Daten, Vermischung der Daten aus verschiedenen Quellen sowie mangelhafte Anonymisierung der Daten an der Tagesordnung. Auf der anderen Seite sind es oft die Krankenhäuser selbst, die ihre Patienten über die Nutzung solcher Apps nicht hinreichend informieren. Denn die Verwendung der App bedeutet ja unter Umständen auch, dass die betreffenden Daten an einen Dritten übertragen werden. Hinzu kommt oft auch die Unwissenheit der Ärzte, dass der Einsatz solcher Apps der vorherigen Rücksprache mit der Krankenhausleitung bedarf. Denn auch im Falle einer eigenmächtigen Nutzung der App durch den Krankenhausarzt bleibt das Krankenhaus für den Einsatz am Patienten datenschutzrechtlich verantwortlich und haftet ihm gegenüber.

Trotz der aufgezeigten datenschutzrechtlichen Schwierigkeiten bei der Nutzung von Gesundheits-Apps in Diagnose und Therapie ist eine rechtskonforme Nutzung unter Beachtung folgender Aspekte und Fragestellungen weiterhin möglich:

- Zunächst einmal muss eine Rechtsgrundlage bestehen, die die Nutzung der jeweiligen App erlaubt. Dabei kommt vor allem eine Einwilligung des Patienten oder eine Auftragsverarbeitung zwischen dem Krankenhaus und dem App-Hersteller in Betracht.
- Liegt ein schlüssiges Datenschutzkonzept seitens des Herstellers und des Krankenhauses vor? Besteht ein ausreichender Schutz der betreffenden personenbezogenen Daten, die als besonders sensibel anzusehen sind?
- Ist gegebenenfalls auch eine Datenschutzfolgenabschätzung erfolgt?
- Werden die wichtigsten datenschutzrechtlichen Grundsätze wie Transparenz und größtmögliche Datensparsamkeit eingehalten?
- In jedem Fall muss zur Einhaltung der gesetzlichen Vorgaben das Bewusstsein auf Hersteller- und Anwenderseite (Krankenhaus und Ärzte) für Qualitäts- und Datenschutzaspekte geschaffen und geschärft werden.

Kontakt für weitere Informationen:

Christoph Naucke
Betriebswirt (BA), Compliance Officer,
zertifizierter Datenschutzbeauftragter DSB
Tel.: +49 (9 11) 91 93-36 28
E-Mail: christoph.naucke@roedl.com

Lana Dachlauer-Baron
Rechtsanwältin, Datenschutzbeauftragte
Tel.: +49 (9 11) 91 93-35 23
E-Mail: lana.dachlauer-baron@roedl.com

Betriebswirtschaft

› Festlegung von Pflegepersonaluntergrenzen in pflegesensitiven Bereichen – Ein Überblick zur PpUGV

Von Magdalena Pieger

Am 11. Oktober 2018 trat die Pflegepersonaluntergrenzen-Verordnung (PpUGV) in Kraft. Die PpUGV definiert zum einen pflegesensitive Bereiche und legt andererseits Untergrenzen für die personelle Besetzung dieser Bereiche fest, die ab dem 1. Januar 2019 gültig sind.

Zur Verbesserung der Personalsituation in der Pflege wurden nach § 137i Abs. 1 SGB V der GKV-Spitzenverband und die DKG beauftragt, bis zum 30. Juni 2018 mit Wirkung zum 1. Januar 2019 Pflegepersonaluntergrenzen für festzulegende pflegesensitive Bereiche im Krankenhaus zu vereinbaren. Diese Verhandlungen sind jedoch gescheitert, sodass die Vorgaben durch Rechtsverordnung durch das Bundesministerium für Gesundheit erlassen wurden. Ziel der PpUGV ist die Sicherung des Patientenschutzes und der Qualität der pflegerischen Patientenversorgung in Krankenhäusern.

Die Regelungen der PpUGV sind bis zum Wirksamwerden einer Vereinbarung über Pflegepersonaluntergrenzen in pflegesensitiven Bereichen der DKG und dem GKV-Spitzenverband gültig. Dies ist jedoch frühestens ab dem 1. Januar 2020 möglich.

Pflegesensitive Bereiche und Grenzwerte

Gemäß PpUGV werden die Bereiche als pflegesensitiv festgelegt, in denen Leistungen der Intensivmedizin, Geriatrie, Unfallchirurgie, Kardiologie, Neurologie und Herzchirurgie erbracht werden. Für die Neurologie und Herzchirurgie wurden durch die PpUGV jedoch vorerst keine Pflegepersonaluntergrenzen festgelegt.

Die Pflegepersonaluntergrenzen werden im Verhältnis von Pflegekräften und Patientenzahl angegeben. Dabei wird zwischen Tag- und Nachtschichten differenziert. Weiter werden Grenzwerte der Anteile von Pflegehilfskräften an der Gesamtzahl der Pflegekräfte festgelegt, die nicht überschritten werden dürfen. Folgende Untergrenzen und Grenzwerte je Bereich wurden festgelegt:

	Tagschicht	Nachtschicht
Intensiv (bis 2020)	2,5:1	3,5:1
Intensiv (ab 2021)	2:1	3:1
Anteil Hilfskräfte	8 %	8 %
Geriatrie	10:1	20:1
Anteil Hilfskräfte	20 %	40 %
Unfallchirurgie	10:1	20:1
Anteil Hilfskräfte	10 %	15 %
Kardiologie	12:1	24:1
Anteil Hilfskräfte	10 %	15 %

Bei interdisziplinär belegten Stationen gilt die Untergrenze mit der jeweils niedrigeren Patientenzahl pro Pflegekraft.

Mitteilungspflicht und Ausnahmetatbestände

Die PpUGV nennt jedoch auch Ausnahmetatbestände, bei denen eine Unterschreitung der Pflegepersonaluntergrenzen zulässig ist. Bei kurzfristigen krankheitsbedingten Personalausfällen, die über das übliche Maß hinausgehen oder bei starken Erhöhungen der Patientenzahlen durch beispielsweise Epidemien oder Großschadensereignisse müssen Pflegepersonaluntergrenzen nicht eingehalten werden.

Zur Überprüfung der Einhaltung der Pflegepersonaluntergrenzen sind dabei Durchschnittswerte der Personalbesetzung über die einzelnen Monate hinweg differenziert nach Stationen und Schichten zu bilden. Die Krankenhäuser müssen den jeweiligen Vertragsparteien und dem Institut für das Entgeltsystem im Krankenhaus (InEK) quartalsweise die Anzahl der Schichten mitteilen, in denen die festgelegten Pflegepersonaluntergrenzen nicht eingehalten wurden.

Die Krankenhäuser riskieren Vergütungsabschläge, wenn die Untergrenzen unterschritten werden. Diese Vergütungsabschläge werden allerdings bis zum 31. März 2019 nicht erhoben. Die Höhe sowie die nähere Ausgestaltung der Vergütungsabschläge ist jedoch noch nicht erfolgt. Die nähere Ausgestaltung von Sanktionen und Vergütungsabschlägen bei Nichteinhaltung der Pflegepersonaluntergrenzen sowie die Festlegung von Pflegepersonaluntergrenzen für die Neurologie und Herzchirurgie soll durch die DKG und den GKV-Spitzenverband erfolgen.

Vermeidung von Personalverlagerungseffekten

Mit der Festlegung von Pflegepersonaluntergrenzen für ausgewählte Bereiche eines Krankenhauses besteht die Gefahr von Personalverlagerungseffekten aus oder in nicht geregelte Bereiche. Abweichend zur Forderung nach § 137i Abs. 1 S. 4 SGB V nennt die PpUGV keine geeigneten Maßnahmen, um Personalverlagerungseffekte zu vermeiden.

Die Einführung der Pflegepersonaluntergrenzen in pflegesensitiven Bereichen wird jedoch von einem sog. „Ganzhausansatz“ begleitet. Um die Pflegequalität und die Sicherheit der Patienten im gesamten Krankenhaus sicherzustellen, soll künftig ein „Pflegepersonalquotient“ je Krankenhaus bestimmt werden, der nicht unterschritten werden darf. Der Pflegepersonalquotient bildet das Verhältnis von eingesetztem Pflegepersonal zum individuellen Pflegeaufwand eines Krankenhauses ab. Die Einführung des Pflegepersonalquotienten ist Bestandteil des Pflegepersonal-Stärkungsgesetzes (PpSG), das voraussichtlich zum 1. Januar 2019 in Kraft treten soll.

Kontakt für weitere Informationen:

Magdalena Pieger
B.A. Betriebswirtschaft
Tel.: +49 (9 11) 91 93-36 78
E-Mail: magdalena.pieger@roedl.com

Rechtsberatung

› 3 kritische Faktoren bei Verträgen zu klinischen Prüfungen nach dem Arzneimittelgesetz AMG

Von Norman Lenger und Laura Maria Hoven

Klinische Prüfungen sind für die Entwicklung und Zulassung von Arzneimitteln ein unverzichtbarer Bestandteil. Sie sind dazu bestimmt, die Wirksamkeit von neuen Arzneimitteln nachzuweisen und deren Verträglichkeit festzustellen. Die klinischen Prüfungen finden statt, bevor das Arzneimittel auf den Markt kommt. Bis eine klinische Prüfung beginnen kann, müssen die Vertragsparteien oft umfangreiche Verhandlungsrunden durchführen, da einheitliche Mindeststandards weder in der Industrie noch bei den unterschiedlichen Forschungseinrichtungen existieren. Ein großes Problem im Rahmen der Vertragsverhandlungen stellt daher die zeitliche Komponente dar, die regelmäßig zum kritischen Faktor wird. Dies ist insoweit bemerkenswert, da die entsprechenden Zeitverzögerungen bei den immer gleichen Vertragspunkten auftreten.

Keine einheitlichen Standards

Wie bereits oben ausgeführt, existieren einheitliche Minimalstandards für den erforderlichen Vertragsinhalt nicht. Zwar gibt es von der Deutschen Hochschuldmedizin, dem KKS-Netzwerk und dem Verband der forschenden Pharma-Unternehmen gemeinsam herausgebrachte „Empfehlungen für die Vertragsverhandlungen von klinischen Studien“. Diese dienen jedoch nur als Orientierung und Ausgangspunkt für die Vertragsverhandlung und sind keine fest vorgeschriebenen Standards. Um zu verhindern, dass Patienten zu spät oder gar nicht in eine Studie eingeschlossen werden, ist diese zeitliche Komponente aus einem prozessualen Blickwinkel zu betrachten. Neben dem materiellen Vertragsinhalt ist eine gut strukturierte Verhandlungsführung wesentlicher Erfolgsfaktor für eine maximale Zeit- und damit Kostenersparnis, die im Ergebnis nicht nur zur Einhaltung des gewünschten Initiierungstermins sondern auch zur Effizienz in der Prüfungsdurchführung führt.

Drei kritische Faktoren: Vorbereitung – Absprachen - Verhandlungsrunden

Um Ihnen einen kleinen Überblick über eine optimale Verhandlungsstruktur zu geben, werden nachfolgend ein paar der notwendigen Punkte anhand von drei relevanten Vertragsinhalten dargestellt:

1. Vorbereitung ist das A & O

Bevor es zur inhaltlichen Überprüfung des eingereichten Vertragstemplates kommt, ist es sinnvoll, einige Vorbereitungen zu treffen. Darunter fällt zunächst das Abfragen der wesentlichen Parameter wie der geplante Initiierungstermin, die Anforderungen sämtlicher zum Vertrag gehörender Anlagen und die konkreten Ansprechpartner sowohl aufseiten des Vertragspartners als auch der Studienkoordination. Wesentlicher Bestandteil dessen ist ebenfalls das Prüfprotokoll.

2. Interne Absprache: geschlossenes Auftreten nach außen

Bei der Vertragsprüfung kann ein unnötiges mehrfaches Austauschen des Vertragswerks zwischen den verhandelnden Parteien dadurch vermindert werden, dass die oft streitigen Vertragsinhalte vorab intern bei jedem Vertragspartner geklärt werden. Dies hat den Vorteil, dass der den Vertrag aushandelnde Sachbearbeiter weiß, was die internen Minimalstandards sind, auf die er in den Verhandlungsrunden bestehen muss und wie groß sein Verhandlungsspielraum ist. Letztlich stärkt ein solches Vorgehen die Verhandlungsposition und bedeutet neben Zeit- auch Geldersparnis.

Drei Beispiele für vorab zu klärende Mindeststandards sind das geistige Eigentum, die Haftungsklauseln und die Beachtung des AGB-Rechts.

– Geistiges Eigentum

Hinsichtlich der Klausel über das geistige Eigentum sollte vorab Rücksprache mit dem Prüfarzt gehalten werden. Möchte der Prüfarzt, dass das Eigentum an möglicherweise entstehenden Arbeitsergebnissen in jedem Fall auf seinen Arbeitgeber übertragen wird? Oftmals wird vom Vertragspartner eine zusätzliche Vergütung für diese Übertragung von Arbeitsergebnissen verlangt. Hier sollte mit dem Prüfarzt abgeklärt werden, ob dafür Budget einkalkuliert wurde und auch tatsächlich zur Verfügung steht.

Es sollte weiter vorab geklärt werden, wem die Nutzungsrechte zustehen sollen und wie diese ausgestaltet sein sollen, zum Beispiel ob diese ausschließlich, unbefristet oder beschränkt zur Verfügung gestellt werden sollen.

– Haftungsklauseln

Eines der wichtigsten Themen ist die Berücksichtigung von Haftungsklauseln. Hier ist vorab zu klären, ob es bereits interne Vorgaben zum Umgang mit Haftungklauseln gibt. Gibt es zum Beispiel einen Beschluss der Führungsebene, wonach die Haftung immer nach den gesetzlichen Regelungen zu erfolgen hat?

Gibt es interne Risikobewertungsmechanismen, nach denen geregelt ist, auf welche Haftungsregelung man sich in bestimmten Verträgen einlassen darf?

Gibt es solche internen Vorgaben nicht, kann durch Rücksprache mit dem Prüfarzt vorab geklärt werden, ob Haftungsfreistellungen oder Haftungsbegrenzungen zugelassen werden sollen. Wenn dies der Fall ist, kann schon vor Eintritt in die Vertragsverhandlung geklärt werden, ob die zu gewährende Haftungsbegrenzung der Art oder der Höhe nach erfolgen soll.

– Berücksichtigung des Rechts über die allgemeinen Geschäftsbedingungen, § 305 ff. BGB

Der Anwendungsbereich der AGB-Kontrolle wird durch § 305 Abs. 1 BGB bestimmt. Danach sind Vertragsbedingungen als Allgemeine Geschäftsbedingungen zu qualifizieren, wenn sie drei Kriterien erfüllen:

- von einer Vertragspartei gestellt
- mit Mehrfachverwendungsabsicht und
- fehlendes Aushandeln „im Einzelnen“.

Die Maßstäbe, die die Vorschriften für die Inhaltskontrolle von allgemeinen Geschäftsbedingungen vorsehen, sind streng. Das gilt auch für den unternehmerischen Rechtsverkehr. Obwohl hier die Klauselverbote der §§ 308, 309 BGB keine Anwendung finden, misst der Bundesgerichtshof (BGH) ihnen Indizwirkung bei und unterwirft somit B2C- und B2B-Verträge in vielerlei Hinsicht denselben Maßstäben. Welche Folgen dies hat, lässt sich am Beispiel der soeben erörterten Haftungsbeschränkungen veranschaulichen. Nach ständiger Rechtsprechung des BGH setzt deren Wirksamkeit voraus, dass sie die Ersatzfähigkeit des vertragstypischen, vorhersehbaren Schadens unberührt lassen. Ausgenommen von der „Vorhersehbarkeitsformel“ ist lediglich die Haftung wegen nichtwesentlicher Vertragspflichten. Weitere Restriktionen folgen aus § 309 Nr. 7 Buchst. b BGB, der ein Freizeichnungsverbot für die Haftung für grobe Fahrlässigkeit und Vorsatz vorsieht und dem auch im unternehmerischen Rechtsverkehr Indizwirkung zukommen soll. Auch wenn sich der BGH insoweit nicht klar positioniert hat, folgt daraus wohl, dass die Haftung wegen grober Fahrlässigkeit und Vorsatzes gar nicht, das heißt noch nicht mal nach Maßgabe der Vorhersehbarkeitsformel eingeschränkt werden kann. Frei beschränkbar bleibt demnach allein die – praktisch wohl kaum relevante – Haftung wegen einfach fahrlässiger Verletzungen nichtwesentlicher Vertragspflichten.

Effektive Haftungsbeschränkungen sind auf dieser Grundlage schwierig und daher präzise zu formulieren.

3. Eigentliche Verhandlungsphase

Nachdem alle Klauseln des Vertrages durchleuchtet, überprüft und an den zu verhandelnden Stellen kommentiert wurden, steht die Nachbereitung an. Es empfiehlt sich, direkt Kontakt mit dem jeweiligen Ansprechpartner beim Vertragspartner aufzunehmen, den Vertrag anzukündigen und die zeitliche Vorstellung hinsichtlich der Vertragsfinalisierung mitzuteilen.

Die aufgeführten Beispiele können anhand des dargestellten Schemas bei allen Vertragsklauseln durchgeführt werden, die für die Verhandlung von Verträgen für klinische Studien nach dem AMG relevant sind.

Benötigen Sie Unterstützung, sprechen Sie uns an. Wir helfen Ihnen mit unserer Expertise gerne weiter!

Kontakt für weitere Informationen:

Norman Lenger LL.M.
Rechtsanwalt, Fachanwalt für Steuerrecht,
Zertifizierter Compliance Officer
Tel.: +49 (2 21) 94 99 09-518
E-Mail: norman.lenger@roedl.com

Laura Maria Hoven
Rechtsanwältin
Tel.: +49 (2 21) 94 99 09-429
E-Mail: laura.hoven@roedl.com

Natürlich können die dargestellten Hinweise nur einen ersten Überblick vermitteln und auf einige wichtige kritische Punkte hinweisen. In der Praxis sind immer auch die Besonderheiten Ihrer Einrichtung zu berücksichtigen: Eine ausführlichere, um weitere Punkte ergänzte Checkliste finden Sie unter:
http://bit.ly/checkliste-vertraege

Wirtschaftsprüfung

› Der neue Bestätigungsvermerk – Erweiterte Berichterstattung des Abschlussprüfers

Von Jan-Claas Hille und Simone Müller

Der im Rahmen der Abschlussprüfung erteilte Bestätigungsvermerk erfuhr eine grundlegende Änderung. Bei den Unternehmen von öffentlichem Interesse (Puplic Interest Entities, PIE) erfolgte die Anpassung bereits für das Geschäftsjahr 2017 und wird nun auch für die Non-PIEs ab dem Geschäftsjahr 2018 verpflichtend. Zentrale Neuerung ist die Aufnahme der wesentlichen Prüfungssachverhalte (key audit matters = KAMs), die für die PIEs verpflichtend und für die Non-PIEs optional erfolgt.

Der Bestätigungsvermerk erfuhr eine grundlegende Änderung infolge der neuen Anforderungen der EU-Abschlussprüfungsverordnung (EU-APrVO) und der damit einhergehenden Änderung in den internationalen und nationalen Prüfungsstandards. Der bisherige kurze und standardisierte Bestätigungsvermerk, das sogenannte „Formeltestat", wird um weitergehende Detailerläuterungen ergänzt. **Der neue Bestätigungsvermerk wird durch die Neuerungen einen deutlich größeren Umfang erhalten.** In Folge werden sich die Bestätigungsvermerke für Unternehmen von öffentlichem Interesse (Puplic Interest Entities, PIE) von solchen für Abschlüsse von Non-PIE-Unternehmen unterscheiden.

Zu Beginn des Jahres wurden die IDW Prüfungsstandards der sog. IDW PS 400er-Reihe veröffentlicht. Auch wenn sich die Vorgaben der EU vorrangig an PIEs wenden, soll ein allzu weites Auseinanderfallen der Regulierungen zur gesetzlichen Abschlussprüfung vermieden werden. Bei den sogenannten PIEs handelt es sich um Unternehmen, deren übertragbare Wertpapiere zum Handel auf einem geregelten Markt zugelassen sind, Kreditinstitute, Versicherungsunternehmen sowie Unternehmen, die von den Mitgliedstaaten als Unternehmen von öffentlichem Interesse bestimmt werden.

Hinsichtlich des Anwendungszeitpunktes ist anzumerken, dass die Anwendung für die Abschlussprüfung von den sogenannten PIEs bereits für den Berichtszeitraum mit Beginn nach dem 16. Juni 2016 erfolgte. Für alle anderen Unternehmen erfolgt die Anwendung dagegen erst für Berichtszeiträume mit Beginn am oder nach dem 15. Dezember 2017. Bei kalenderjahrgleichen Geschäftsjahren (1. Januar bis 31. Dezember) käme damit der nach § 322 HGB neu zu erteilende Bestätigungsvermerk erstmals für Jahresabschlüsse zum 31. Dezember 2018 zur Anwendung.

Der neue IDW PS 400 gibt das Rahmenkonzept vor und regelt den Normalfall des uneingeschränkten Prüfungsurteils. Die ergänzenden Standards regeln die Modifikationen des Prüfungsurteils (IDW PS 405) beispielsweise wenn Einwendungen zu erheben sind oder Prüfungshemmnisse vorliegen und es zu einem eingeschränkten oder versagten Prüfungsurteil kommen kann. Hierzu kann es kommen, wenn beispielsweise die Anhangangaben unvollständig sind, Gewinnverwendungsregeln verletzt wurden oder mangelhafte Bestandsnachweise bei Vermögensgegenständen vorliegen. Die möglichen Hinweise des Abschlussprüfers von besonderen Sachverhalten werden in IDW PS 406 dargestellt. Ein besonderer Sachverhalt, der im Bestätigungsvermerk hervorzuheben ist, kann beispielsweise ein bedeutsames Ereignis sein, das zwischen dem Abschlussstichtag und dem Datum des Bestätigungsvermerks eingetreten ist. Die Mitteilung besonders wichtiger Prüfungssachverhalte (KAMs) im Bestätigungsvermerk ist in IDW PS 401 geregelt.

Ziel dieser Neuerung ist es, die Kommunikation zwischen dem Abschlussprüfer und den Abschlussadressaten zu verbessern, die Aussagekraft des Bestätigungsvermerks zu erhöhen, indem mehr Transparenz über die durchgeführte Abschlussprüfung geschaffen wird, sowie eine international einheitliche Berichterstattung sicherzustellen.

Zentrale Merkmale der künftigen Berichterstattung:

- **Strukturelle Änderungen mit vorangestelltem Prüfungsurteil**
- **detailliertere Gliederung des Bestätigungsvermerk**
- **ergänzende Anforderungen zum Bestätigungsvermerks für PIEs sowie Non-PIEs**

Die Struktur des neuen Bestätigungsvermerks soll nach den Standardentwürfen des Hauptfachausschusses für alle Unternehmen identisch sein, um eine Zwei-Klassen-Prüfung zu vermeiden. Der neue Bestätigungsvermerk ist zweigeteilt dargestellt. Der erste Teil beinhaltet den Vermerk über die Prüfung des Abschlusses. Dieser beginnt mit der Darstellung des Prüfungsurteils und der Beschreibung der Grundlagen für dieses Urteil. Die Abschnitte zur Verantwortung von Vorstand und Aufsichtsrat für den Abschluss sowie zur Verantwortung des Abschlussprüfers für die Prüfung sind umfangreicher als bisher darzustellen. Der zweite Teil enthält weitere Berichterstattungserfordernisse, insbesondere den Vermerk über die Prüfung des

Lageberichts. Hier ist ebenfalls das Prüfungsurteil vorzustellen, gefolgt von Ausführungen zur Grundlage für das Prüfungsurteil und der Beschreibung der Verantwortlichkeiten.

Ergänzend zu dieser erweiterten Berichterstattung in Bestätigungsvermerken existiert die Darstellung der besonders wichtigen Prüfungssachverhalte, der sogenannten key audit matters (KAMs). Die KAMs stellen die Sachverhalte dar, die nach pflichtgemäßem Ermessen des Abschlussprüfers bei der Prüfung des Abschlusses des aktuellen Geschäftsjahres am bedeutsamsten waren. Sie werden aus den Sachverhalten abgeleitet, die mit dem Aufsichtsrat bzw. Prüfungsausschuss erörtert wurden.

Bei den PIEs ist die Aufnahme der KAMs verpflichtend, wohingegen bei den Non-PIEs gemäß IDW PS 401 die Aufnahme der KAMs freiwillig erfolgt und im Vorhinein ausdrücklich schriftlich im Auftragsbestätigungsschreiben vereinbart werden muss.

Die Darstellung der KAMs soll die relevanten Risikobereiche, die Art und Weise, wie der Abschlussprüfer durch entsprechende Prüfungshandlungen Prüfungssicherheit erlangt, sowie die Würdigung der Prüfungsergebnisse und etwaige Feststellungen enthalten. Diese Darstellung ist unternehmensindividuell vorzunehmen.

Bei der Festlegung der KAMs können erhöhte Fehlerrisiken aufgrund ermessensbehafteter Rechnungslegungs- und Bewertungsverfahren sowie komplexe Transaktionen im Geschäftsjahr eine Rolle spielen. Die Auswahl der KAMs ist im Rahmen der risikoorientierten Abschlussprüfung bereits bei der ersten Risikoanalyse in der Planungsphase auf Basis der unternehmensindividuellen Gegebenheiten vorläufig vorzunehmen. Es sind insbesondere die Sachverhalte auszuwählen, die ein erhöhtes Maß an Aufmerksamkeit vom Abschlussprüfer erfordern und über die er den Prüfungsausschuss bzw. den Aufsichtsrat informiert hat. Weiter ist im Bestätigungsvermerk auf Sachverhalte einzugehen, die in besonderem Maße erheblich für die Darstellung der Vermögens-, Finanz- und Ertragslage sind oder im betreffenden Geschäftsjahr einen besonders großen Prüfungsaufwand erfordert haben. Die Berichterstattung über die KAMs ist im Bestätigungsvermerk in einem eigenen Abschnitt vorzunehmen. Jedes KAM ist separat vorzustellen.

Die Beschreibung der KAMs beginnt mit der unternehmensindividuellen Darstellung des Risikos für den geprüften Jahres- und Konzernabschluss. Hierbei ist auf die einzelnen Abschlussposten bzw. Anhangangaben einzugehen, die von dem Fehlerrisiko betroffen sind. Es wird empfohlen, die Ursachen für mögliche Fehler in diesen Abschlussinformationen anzugeben. Im nächsten Schritt hat der Abschlussprüfer darauf einzugehen, durch welche Prüfungshandlungen er sich vergewissert hat, dass die jeweils geprüften Abschlussinformationen trotz der festgestellten Risiken keine wesentlichen Fehler enthalten. Abschließend sind die Ergebnisse und die bedeutendsten Schlussfolgerungen aus den zuvor beschriebenen Prüfungshandlungen zusammenfassend aufzuzeigen.

Die Neuregelungen sehen zudem vor, dass Querverweise auf Abschluss- und Anhangangaben sowie gegebenenfalls Lageberichte vorzunehmen sind, sofern diese für den geprüften Sachverhalt von Bedeutung sind. Dies kann dazu führen, dass die Angaben der gesetzlichen Vertreter künftig kritischer gelesen und analysiert sowie denen vergleichbarer Unternehmen gegenübergestellt werden.

Die neu eingeführte Berichterstattung über die besonders wichtigen Prüfungssachverhalte im Bestätigungsvermerk wird nicht nur für die Abschlussadressaten, sondern auch für den Prüfungsausschuss bzw. den Aufsichtsrat von besonderer Bedeutung sein. Da die abschließende Beurteilung darüber, welche Sachverhalte entscheidend für die Abschlussprüfung waren, meist erst zum Ende der Prüfung erfolgt und diese Phase vielfach zeitlich eng ist, empfehlen wir einen regelmäßigen Austausch mit dem Abschlussprüfer über die identifizierten KAMs und die hieraus resultierende Berichterstattung bereits im Verlauf der Prüfung, um den zeitlichen Aufwand für Diskussionen zum Ende der Prüfung hin zu begrenzen.

Kontakt für weitere Informationen:

Jan-Claas Hille
Wirtschaftsprüfer, Steuerberater, Diplom-Kaufmann
Tel.: +49 (2 21) 949 909-432
E-Mail: jan-claas.hille@roedl.com

Simone Müller
M.A. Medizinmanagement
Tel.: +49 (2 21) 94 99 09-434
E-Mail: simone.müller@roedl.com

Rödl & Partner intern

› Veranstaltungshinweise

Thema	**Revisionssichere Archivierung durch digitale Dokumentensteuerung richtig umsetzen**
Termin / Ort	29. Januar 2019 / Nürnberg

Thema	**Digital CHANGE Forum**
Termin / Ort	12. Februar 2019 / Nürnberg

ALTEN PFLEGE
Die Leitmesse 2019

SAVE THE DATE
2. – 4. April
Messezentrum
Nürnberg

CONSOZIAL 2018:

Wieder ist ein erfolgreicher Messebesuch auf der ConSozial in Nürnberg – die diesmal zum 20. Mal stattgefunden hat – zu Ende gegangen. Mit über 6.000 Besuchern aus Fach- und Führungsbereichen der Sozialbranche kann man die Jubiläumsveranstaltung ebenfalls als sehr erfolgreich bezeichnen. Wir möchten uns für eine Vielzahl an interessierten Besuchern an unserem Stand, gute Gespräche und erstklassiges Networking bedanken.

SAVE THE DATE
6. und 7. November 2019
in Nürnberg

Kontakt für weitere Informationen:

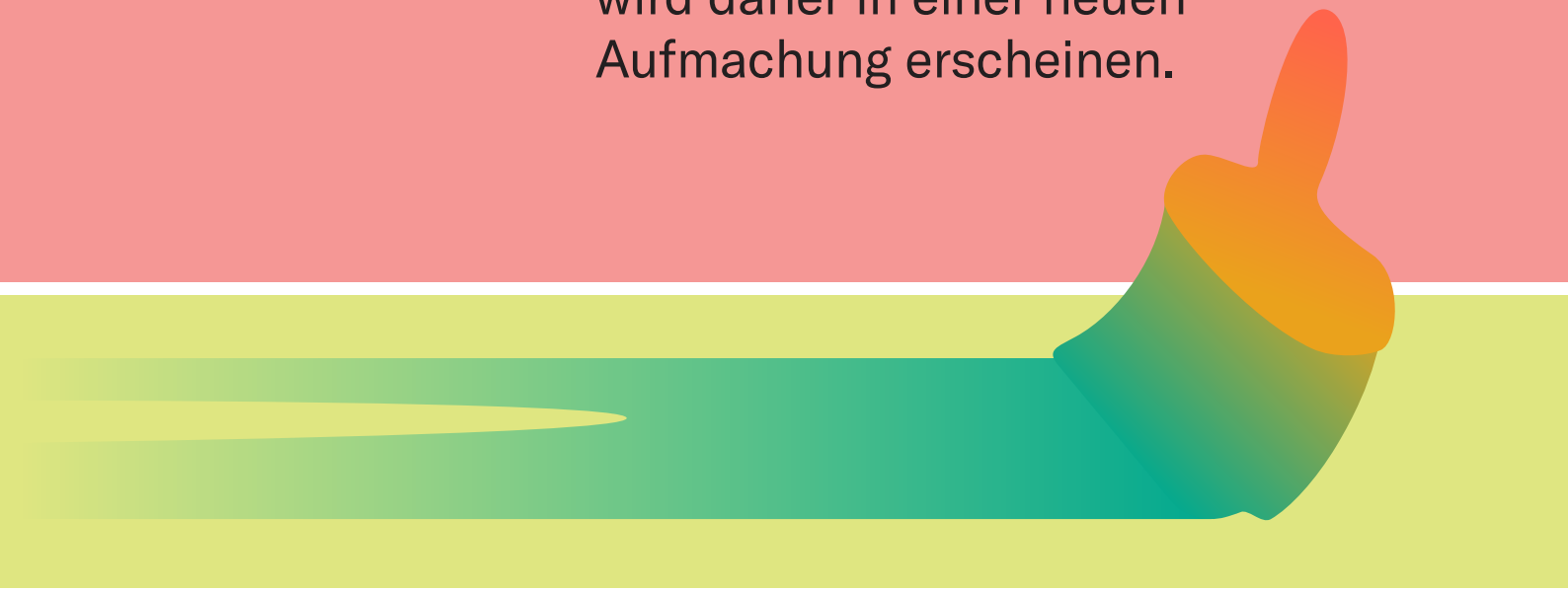
Klara John
Kauffrau für Marketingkommunikation
Tel.: +49 (9 11) 91 93-35 09
E-Mail: klara.john@roedl.com

FROHE WEIHNACHTEN

Wir wünschen Ihnen besinnliche Festtage
und ein frohes und erfolgreiches Jahr 2019.

NEUES DESIGN

Das neue Corporate Design von Rödl & Partner wird sich auch in unseren Newslettern widerspiegeln. Die nächste Ausgabe unseres Fokus Gesundheits- und Sozialwirtschaft wird daher in einer neuen Aufmachung erscheinen.



Impressum Fokus Gesundheits- und Sozialwirtschaft

Herausgeber: **Rödl & Partner GbR**
Äußere Sulzbacher Str. 100 | 90491 Nürnberg
Tel.: +49 (9 11) 91 93-35 04 | pmc@roedl.de

Verantwortlich
für den Inhalt: **Martin Wambach** – martin.wambach@roedl.com
Kranhaus 1, Im Zollhafen 18 | 50678 Köln
Bernd Vogel – bernd.vogel@roedl.com
Äußere Sulzbacher Str. 100 | 90491 Nürnberg

Layout/Satz: Andrea Kurz – andrea.kurz@roedl.com
Äußere Sulzbacher Str. 100 | 90491 Nürnberg