DER SICHERE UMGANG MIT DATEN

Bewusstsein schaffen

Datenschutz ist nicht nur vom Gesetz her vorgeschrieben. Er kann darüber hinaus auch ein echtes Qualitätsmerkmal für eine Gesundheits- und Pflegeeinrichtung darstellen und die Kundenzufriedenheit positiv beeinflussen.

Der Datenschutz wird oft vernachlässigt. Er macht zusätzliche Arbeit, ist lästig und die Folgen schlechten Datenschutzes werden unterschätzt. Dabei sind diese Maßnahmen nicht nur gesetzlich vorgeschrieben, sie können auch die Qualität einer Einrichtung steigern und die Kundenzufriedenheit erhöhen. Im negativen Fall kann eine Datenschutzpanne sogar zur Insolvenz führen. Daten im Müll, auslesbare Datenträger auf dem Trödelmarkt, Kunden- und Patientendaten öffentlich zugänglich im Internet sowie Hackerangriffe auf ungeschützte EDV-Systeme – Pannen passieren immer wieder, trotz klarer gesetzlicher Vorgaben und streng definierter Strafen für einen falschen oder fahrlässigen Umgang mit persönlichen Daten. Laut einer Studie des Ponemon-Instituts im Auftrag des Softwareanbieters Symantec (2010) räumten 53 Prozent der befragten Unternehmen eine Datenpanne innerhalb der vorangegangenen zwölf Monate ein. Deutsche Firmen bezahlten 2009 durchschnittlich 2,58 Millionen Euro für die Aufklärung und Schadensbegrenzung von Datenschutzpannen. Die Dunkelziffer dürfte deutlich höher liegen. Gerade die Gesundheits- und Pflegebranche darf sich keine Datenverluste leisten, handelt es sich bei den erhobenen Daten doch nach § 3 Absatz 9 Bundesdatenschutzgesetz (BDSG) um „besondere Arten personenbezogener Daten“, die unter allen Umständen vor unerlaubtem Zugriff geschützt werden sie müssen. Kommen diese Daten abhanden oder werden sie missbraucht, ist das nicht nur finanziell kritisch. Schlimmer ist meist der allgemeine Vertrauensverlust, der damit einhergeht, denn dieser ist auch mit großem Aufwand kaum wieder gutzumachen.

WAS SPRICHT DAFÜR?	WAS SPRICHT DAGEGEN?
Rechtliche und technische Expertisen sind sofort abrufbar. Sie müssen keinen Mitarbeiter freistellen, damit er sich in die Materie einarbeiten kann. Das kann Zeit und Geld sparen.	Es fallen zusätzliche Kosten für die Dienstleistung an (Honorar).
Ein Spezialist kennt die Datenschutz-Schwachstellen von Gesundheitsbetrieben und hat Erfahrung mit Lösungsstrategien.	Ein externer Datenschutzexperte muss in vorhandene Strukturen eingeführt werden. Zudem benötigt er einen Ansprechpartner im Betrieb. Dies kann zu Reibungsverlusten führen.
Ein Externer ist weder in Betriebsabläufen gefangen noch beeinflusst von innerbetrieblicher Teamdynamik. Diese Neutralität ermöglicht eine effiziente Arbeit – frei von Interessenkonflikten und Betriebsblindheit.	Ein Externer prüft und organisiert die Datenschutzstrategie, ist aber danach nur punktuell vor Ort, um die korrekte Umsetzung im Alltag zu prüfen. Hier sind klare Vereinbarungen und Verträge nötig.
Fehlerhaft aufgesetzte Datenschutzprozesse und Schulungen liegen in der Verantwortlichkeit des Externen, nicht mehr in Ihrem Haus.	Mitarbeiter können den Externen als bedrohlich (Jobverlust) oder als lästig (zusätzliche Arbeit) empfinden. Dies kann die konsequente Mitarbeit in Datenschutzfragen erschweren.
Kosten sind kalkulierbar, denn Aufwendungen für Weiterbildungen, Beschaffung von Fachliteratur, Kosten für Dienstausfälle, Vertretungen oder Neubestellung eines innerbetrieblichen Beauftragten entfallen.	Zwischen IT-Abteilung und externem Datenschutzbeauftragten kann es zum Kompetenzgerangel kommen. Für ein respektvolles Miteinander sind klare Kommunikationsstrategie und Definition der Verantwortlichkeiten nötig.
Sie schließen einen befristeten Vertrag ab. Im Gegensatz dazu genießt ein interner Beauftragter während seiner Funktion und auch noch ein Jahr nach Entbindung von der Aufgabe erweiterten Kündigungsschutz.	Nicht jeder Externe ist für jedes Unternehmen geeignet. Achten Sie bei der Auswahl auf fachliche und menschliche Kompetenzen. Ein externer Spezialist muss zu Ihren Mitarbeitern passen. Sonst bleibt der Erfolg aus.

Pro und Contra: Einsatz eines externen Datenschutzbeauftragten.

KRITISCHE PUNKTE IM DATENSCHUTZ

Datenschutz ist ein juristisch schwieriges Thema. Unterschiedliche Gesetzesvorgaben erschweren den sicheren Umgang mit den Datenschutzbestimmungen. Ob für das eigene Haus jeweils das Bundesdatenschutzgesetz (BDSG) gilt oder aber ein Landesdatenschutzgesetz (LDSG), Landeskrankenhausgesetze (LKHG), kirchliche Gesetze wie die Katholische Datenschutzordnung (KDO) oder das Datenschutzgesetz der Evangelischen Kirche Deutschlands (DSG EKD), ist Betroffenen nicht immer klar. Dies hat ganz praktische Auswirkungen, denn was z.B. in Hamburg datenschutzkonform ist, wird vielleicht in Bayern zum Problem.

Allen Datenschutzauflagen gemein ist, dass sie nicht greifen, wenn sie zwar professionell aufgesetzt sind, im Alltag aber nicht eingehalten werden. Ohne ein Bewusstsein für den Umgang mit sensiblen Kundeninformationen („Awareness“) sind Pannen programmiert. Auch die kriminelle Nutzung von Datensicherheitslecks (intern wie extern) oder „zwischenmenschliche“ Beeinflussungen, um an Informationen zu gelangen („Social Engineering“), sind nicht auszuschließen. Zu den größten Feinden des Datenschutzes und der Datensicherheit gehören:

- fehlende Sachkenntnis,
- nie hinterfragte Alltagsroutinen,
- Stress bei Arbeitsabläufen,
- Multitasking,
- unsichere oder halbherzige Techniklösungen,
- Nachlässigkeiten rund um das mobile Arbeiten,
- Konflikte mit Mitarbeitern an datenschutzrelevanten Schlüsselpositionen.

BASISELEMENTE FÜR GELUNGENEN DATENSCHUTZ

Das Bewusstsein für den Umgang mit Daten muss bei jedem einzelnen Mitarbeiter – von der Verwaltung und EDV-Abteilung über das Pflegepersonal bis hin zu den Ärzten – geschaffen werden. Dies beginnt bei der Einstellung und Einarbeitung eines

Mitarbeiters und reicht über eine mögliche Kündigung hinaus. Datenschutz muss in der gesamten Einrichtung höchste Priorität haben und gelebt werden. Dabei dürfen die nötigen Maßnahmen die täglichen Abläufe nicht stören. Im Gegenteil: Ein professioneller Datenschutz muss so konzipiert und in den Tätigkeiten verankert sein, dass er die Mitarbeiter bei der medizinischen Versorgung der Patienten unterstützt und keinen nennenswerten Zusatzaufwand bedeutet. Außerdem bedarf es eines verlässlichen und manipulationssicheren EDV-Systems.

Grundsätzlich muss sich die Datenerhebung und -verarbeitung im Sinne des § 3a BDSG auf ein Minimum beschränken (Datenvermeidung und -sparsamkeit) und – wo möglich – anonymisiert und pseudonymisiert werden. Zudem muss der Patient vorab über Freiwilligkeit, Umfang und Zweck der geplanten Verarbeitung seiner Daten informiert werden. Auf die Möglichkeit des Widerrufs seiner Einwilligung ist der Betroffene ebenfalls hinzuweisen (§ 4a Absatz 1 BDSG). Das der Datennutzung zugrunde liegende Prinzip heißt juristisch „Verbot mit Erlaubnisvorbehalt". Daraus ergibt sich, dass auf die schriftliche Form der Einwilligung zu achten ist. Dies gilt insbesondere, wenn persönliche Daten an Dritte übermittelt werden sollen.

DER BETRIEBLICHE DATENSCHUTZBEAUFTRAGTE

Ein konsequenter Datenschutz steht und fällt auch mit der Person des betrieblichen Datenschutzbeauftragten, denn dieser überprüft Abläufe, identifiziert Sicherheitslücken und muss eine langfristige Datenschutzstrategie entwickeln und durchsetzen. Ob der gesetzlich vorgeschriebene Datenschutzbeauftragte eines Unternehmens intern bestellt wird oder ob man auf einen externen Sachverständigen zurückgreift, bleibt jeder Einrichtung überlassen. Wesentlich für die Bekleidung dieser Position sind die Zuverlässigkeit der bestellten Person, eine nachweisbare, erhebliche und stets aktuelle juristische und technische Fachkenntnis und innerbetriebliche Durchsetzungskraft.

Wird ein Mitarbeiter intern für den Datenschutz bestellt, müssen ihm die für diese Aufgabe notwendigen zeitlichen Ressourcen zur Verfügung gestellt werden. Das bedeutet: Er ist für andere Aufgaben nicht mehr voll einsetzbar. Insbesondere zu Beginn der Tätigkeit sind auch Fachfortbildungen und eine großzügige Einarbeitungsphase zu gewähren. Zu den Aufgaben des Datenschutzbeauftragten zählen auch die Kontrollen zur Einhaltung der definierten Standards und die Schulung der Mitarbeiter.

SCHULUNGEN UND SCHULUNGSINHALTE

Jeder Mitarbeiter muss schon mit dem Einstieg in ein Unternehmen mit dem Thema konfrontiert werden – nämlich in Form einer schriftlichen Unterrichtung zu Datenschutz und Schweigepflicht. Die Hintergründe und Details sowie die in der jeweiligen Einrichtung gelebte Datenschutzpolitik werden am besten über gezielte Schulungsmaßnahmen vermittelt. Diese sollten nicht nur informieren, sondern auch zur Aufmerksamkeit motivieren. Klassische Schulungsinhalte sind:

- Informationen zum Sinn und Zweck von Datenschutzmaßnahmen, aktuelle Pannenszenarien,
- Überblick zu Gesetzesvorschriften und zur Haftung bei Datenschutzversäumnissen,
- Erläuterung von Patientenrechten im Hinblick auf den Datenschutz (Einwilligung, Widerspruchsrecht, Pfortensperren, Recht auf Akteneinsicht etc.),
- Klärung innerbetrieblicher Organisations- und Sicherheitsstrukturen,
- fachgruppenspezifische Informationen (Ärzte, IT-Abteilung, Verwaltung, Pflege etc.),
- Hinweise zur Dokumentation der Datennutzung (Verfahrensverzeichnis, Löschfristen etc.),
- Notfallstrategien und Fehlermanagement, wenn Datenschutzlücken wahrgenommen werden.

TECHNISCHE UNTERSTÜTZUNGSMÖGLICHKEITEN

Erfolgreicher Datenschutz muss menschliche Schwächen durch technische Hilfsmittel ausgleichen. Momentane Gedankenlosigkeit oder Ablenkung einzelner Mitarbeiter ist auch bei bester Schulung nicht immer vermeidbar. Da müssen intelligente Sicherheitssysteme greifen und eine falsche Nutzung von Daten, einen Datenverlust oder -missbrauch unmöglich machen; z.B.:

- elektronische Erinnerungen und Checklisten, die wesentliche Datenschutzvorgaben abfragen (Einwilligungen, Widersprüche etc.),
- EDV-Lösungen, die jedem Mitarbeiter einen individualisierten und strikt auf seine Befugnisse eingeschränkten Datenzugang ermöglichen (Zutritts-, Zugangs- und Zugriffskontrolle) und die Trennung von solchen Daten gewährleisten, die für unterschiedliche Zwecke erhoben wurden (Trennungsgebot),
- ein automatisiertes und kurz getaktetes Schließen von Programmen für den Fall, dass ein Mitarbeiter ungeplant einen Prozess unterbricht und sein Log-out darüber vergisst (Zugriffskontrolle),
- automatische Bildschirmschoner, die nach kurzen Pausen zur erneuten Passworteingabe oder zur Identifizierung per Daumenabdruck auffordern (Zugriffskontrolle),
- Dokumentationssysteme, die jede Datennutzung und -weitergabe mit einem Berechtigungsprofil abgleichen, Manipulationsversuche erfassen und jede Bewegung im EDV-System automatisch und nicht überschreibbar protokollieren (Zugriffs-, Weitergabe-, Eingabe- und Auftragskontrolle),
- Mechanismen, die ein versehentliches oder willentliches Löschen von Daten unmöglich machen (Eingabe- und Verfügbarkeitskontrolle).

Esther Niederhammer

ONLINE EXKLUSIV

Literaturtipps:
- www.hcm-magazin.de

Internetipps:
- www.bsi.bund.de
- www.symantec.com
- www.ponemon.org

Downloads:
- Klassische Datenschutz-Schwachstellen

INTERVIEW MIT MARK RÜDLIN

„Dafür gibt es Fortbildungspunkte …“

***HCM:* Welches sind die häufigsten Fehler, die zu Pannen im Datenschutz führen?**
Rüdlin: Es sind meiner Erfahrung nach immer wieder die gleichen Probleme: fehlerhafte oder nicht vorhandene Einwilligungen zur Datenerhebung oder -verarbeitung, keine Regelungen oder Verträge zur Auftragsdatenverarbeitung, organisatorische Mängel und fehlerhaft oder gar nicht durchgeführte Schulungen. Die Hauptursache besteht darin, dass schlicht und ergreifend die Kenntnisse fehlen und Datenschutzaspekte nicht in die Tätigkeiten einbezogen werden. Erst wenn eine Datenschutzpanne auftritt oder jemand nachfragt, stellt man fest, dass in den Betriebsabläufen das Thema „Datenschutz“ nicht ausreichend durchdacht war.

***HCM:* Was sollte man bei Datenschutzproblemen tun?**
Rüdlin: Das ist in einer neuen Vorschrift klar geregelt: § 42a im BDSG schreibt vor, dass man eine Art Krisenorganisationsstruktur auf den Weg bringen muss. Mitarbeiter müssen darauf hingewiesen werden, dass sie einen Verdacht an eine hausinterne Datenschutzhotline melden. Diese leitet das Problem an die Geschäftsführung weiter, die wiederum unter Einbeziehung des Datenschutzbeauftragten eine Bewertung vornimmt, inwieweit zu reagieren ist. Manchmal muss man den gesetzlichen Vorgaben entsprechend die Betroffenen unterrichten, manchmal müssen auch die Aufsichtsbehörden informiert werden. Dies sollte immer so geschehen, auch um Schaden vom eigenen Unternehmen abzuwenden, der durch negative PR entstehen kann.

***HCM:* Wie lange dauert es, einen betrieblichen Datenschutz korrekt umzusetzen?**
Rüdlin: Das hängt von der Größe der Einrichtung und den Vorbedingungen ab. Zu Beginn ist eine Bestandsaufnahme nötig, wobei ein Audit hierfür mehrere Tage dauern kann, denn man muss sich erst einmal durch vorhandene Strukturen durcharbeiten. Die Umsetzung der Datenschutzstrategie, bis alle wichtigen Sachen auf den Weg gebracht sind und sich ein Haus relativ datenschutzkonform verhält, dauert nach meinen Erfahrungen etwa zwei Jahre. In der Zwischenzeit geht es darum, die Akzeptanz des Datenschutzes so weit in ein Haus hineinzutragen, dass die Maßnahmen von den Mitarbeitern angenommen werden. Optimal ist, wenn es Datenschutz-Arbeitsgruppen gibt. In einer Klinik ist es sinnvoll, dass jeweils Personen aus der ärztlichen Leitung, aus der IT-Leitung, aus der Personalabteilung, aus der Pflegedienstleitung und aus dem Betriebsrat alle zwei bis drei Monate zusammenkommen und sehen, welche datenschutzrelevanten Themen vorliegen.

PORTRÄT

Mark Rüdlin

Rechtsanwalt mit Schwerpunkten IT-, Software-, Vertrags- und Datenschutzrecht. Als betrieblicher Datenschutzbeauftragter prüft, konzeptioniert und schult er medizinische und andere soziale Einrichtungen in Datenschutzbelangen. Mitglied in der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD e.V.) und im Hamburger Anwaltsverein. **Kontakt:** ra@markruedlin.de

***HCM:* Ein externer Datenschutzbeauftragter kann eigentlich nur punktuell prüfen. Sollte er die Aufgabe der Kontrolle intern vergeben?**
Rüdlin: Es ist durchaus möglich, als Externer umfassend zu erkennen, was in den jeweiligen Einrichtungen praktisch passiert. Ich gehe z.B. regelmäßig ein bis zwei Stunden durch die Kliniken, für die ich arbeite, und schaue mir an, wie gearbeitet wird. Ich kenne ja die neuralgischen Punkte und weiß, worauf es sich lohnt, einen Blick zu werfen. Ich spreche Mitarbeiter an, wenn ich Situationen vorfinde, die ich als unbefriedigend empfinde.

***HCM:* Wie gehen Sie vor, können Sie das konkretisieren?**
Rüdlin: Manchmal stehen die Patientenaktenwagen mitten auf dem Flur. Ich blättere in den Akten und prüfe, wie lange es braucht, bis ich angesprochen werde. Oder ich ziehe mir einen Blaumann an und versuche, einen Rechner oder irgendwelche Unterlagen wegzutragen – und warte darauf, dass ich zur Ordnung gerufen oder zumindest gefragt werde, ob und von wem ich dazu legitimiert worden bin. Zur Prüfung der Beachtung von Pfortensperren bitte ich auch Dritte zu versuchen, ob sie an der Pforte über solche Patienten Auskünfte erhalten können, die einer Auskunftserteilung widersprochen haben. Neulich habe ich in einem Krankenhaus geprüft, wer alles auf eine elektronische Patientenakte zugegriffen hatte und ob diese Leute tatsächlich mit der Behandlung eines speziellen Patienten betraut waren. Manchmal laufe ich auch nachts durch ein Haus, mit dem ich einen Vertrag habe. Meist sind die Stationen nur minimal besetzt, keiner ist zu sehen. Manchmal steht aber die Stationszimmertür auf und im Rechner ist jemand eingeloggt. Da gucken die Betroffenen dann schon, wenn ich ihnen eine Akte vor die Nase halte, die ich vom Tisch genommen habe, und sage: „Ich hätte jetzt auch ein Privatdetektiv sein können.“

Foto: Esther Niederhammer

***HCM:* Welche Konsequenzen hat das für Mitarbeiter, die nachlässig waren?**
Rüdlin: Oft reicht es, die Betreffenden in ein Gespräch zu verwickeln und zu fragen: „Machen Sie das eigentlich immer so? Kann man das nicht anders machen?“ So etwas ergibt durchaus Sinn, gerade wenn ich weiß, dass nach mehrmaligen Ansagen das gewünschte Ergebnis noch nicht erreicht ist. Es trägt dazu bei, dass die Hintergründe solcher Auflagen ins Bewusstsein kommen und dass Maßnahmen künftig auch entsprechend umgesetzt werden. Datenschutz darf nicht als lästig empfunden, sondern muss als sinnvoll erkannt werden und Teil des Ablaufes sein. Sonst funktioniert er nicht.

***HCM:* Über welche Kanäle funktioniert die Vermittlung von Datenschutzansagen am besten?**
Rüdlin: Ich beschreite mehrere Wege. Es ist wichtig, die Mitarbeiter regelmäßig zu schulen, je nach Haus im Abstand zwischen einem und fünf Jahren. In den Einrichtungen, in denen ich arbeite, müssen die Mitarbeiter nachweisen, dass sie an Datenschutz-Schulungsveranstaltungen teilgenommen haben, entweder intern oder extern. Die Häuser selbst müssen ihre Mitarbeiter für solche Schulungen freistellen. Dafür gibt es Fortbildungspunkte, sowohl für Pflegekräfte als auch für Ärzte. Ich stelle auch Unterlagen im Intranet zur Verfügung. Zudem schreibe ich regelmäßig kleine Artikel in den Hauszeitschriften oder mache dort Werbung dafür, dass ich auf offene Fragen gerne angesprochen werden kann. Von den Einrichtungen, in denen die Thematik gut angenommen wird, bekomme ich regelmäßig Anfragen.

***HCM:* Geraten Sie als externer Datenschutzbeauftragter auch mal in Konflikte mit der IT-Abteilung? Man kann sich da ein Kompetenzgerangel vorstellen.**
Rüdlin: Nein, eigentlich passiert das nie. Die IT-Abteilungen freuen sich meist, wenn sie unterstützt werden. Es gibt ein paar wenige „Hardliner“ mit Tunnelblick, denen es manchmal schwerfällt, aber da kommt man argumentativ ganz gut dagegen an. Gerade für die IT ist es ein Aspekt der Sicherheit, dass sie wissen, worauf es bei Datenschutzauflagen im Detail ankommt. Ich erlebe also eher, dass meine Präsenz gut angenommen wird. Psychologische Aspekte spielen da natürlich eine Rolle. Wenn ich als Besserwisser durch die Gegend laufe, dann bekomme ich, was ich verdiene – nämlich Ablehnung. Wenn ich versuche, mich in die Arbeitssituation der Betroffenen hineinzudenken und nicht diktiere, was wir machen, sondern Vorschläge unterbreite und für Lösungen werbe, dann erreiche ich große Akzeptanz.

***HCM:* Stichwort „mobiles Arbeiten“: Viele Ärzte nutzen heute ein Smartphone. Es wird auch von zu Hause gearbeitet. Hat sich dadurch die Situation für den Datenschutz verschärft?**
Rüdlin: Nicht wenn man gesellschaftliche und technische Änderungen zur Kenntnis nimmt und diese Situationen technisch und organisatorisch löst, dass man z.B. sichere Verbindungen schafft, nur bestimmte Geräte ausgibt oder manipulationsfreie Home-Office-Arbeitsplätze einrichtet. Und dass die entsprechenden Verantwortlichen die Hoheit bekommen, zu prüfen, ob mit den Geräten sachgemäß umgegangen wird. Ein ziemlicher Hype derzeit ist ja, dass man mit dem Smartphone arbeitet und direkten Zugang auf die Krankenhausinformationssysteme bekommt. Hier müssen Sicherheitsschranken aufgestellt werden, die man nicht umgehen kann. Parallel dazu ist es sinnvoll, organisatorische Maßnahmen zu treffen, damit es einschlägige Betriebs- und Individualvereinbarungen mit den Betreffenden gibt, dass ihnen ganz klar ist, was sie dürfen oder eben nicht. Bleiben noch die klassischen Pannen, dass z.B. jemand mit dem Notebook durch die Gegend fährt, auf dem sich Daten lokal befinden, und man dann mal eben schnell auf dem Heimweg am Supermarkt hält – und wenn man zurückkommt, hat man eine eingeschlagene Scheibe und ein Notebook weniger. Hier hilft nur, dass die Mitarbeiter entsprechend sensibilisiert sind und wissen: So etwas kann ich nicht machen.

***HCM:* Es sind aber schon Patientendaten bei Facebook aufgetaucht, weil ein Arzt sein Adressbuch dort abgeglichen hatte.**
Rüdlin: Dieser Arzt hat seine Sorgfaltspflicht verletzt. Es ist wichtig, dass die sozialen Netzwerke und auch der Umgang mit dem Internet hausintern als Themen wahrgenommen werden und dass es verbindliche Vorgaben gibt, wie damit umzugehen ist. Bei mir ist fester Bestandteil in Schulungen, dass man die wichtigen Benimmregeln im Umgang mit sozialen Netzwerken und dem Internet erläutert und auf Quellen verweist, bei denen man sich weiter informieren kann.

***HCM:* Wie sollten Schulungen angelegt sein?**
Rüdlin: Ich empfehle allgemeine Schulungen und solche, die speziell auf den jeweiligen Arbeitskontext ausgerichtet sind. Eine Basisschulung dauert etwa eine Stunde. Wenn man Rückfragen ermöglichen will, sind anderthalb Stunden besser. Im Übrigen ist es sinnvoll, manche Bereiche besonders zu betrachten. Inhaltlich unterscheiden sich die Schulungen, die sich speziell an Pflegekräfte, an Therapeuten oder an Sozialarbeiter in sozialen Einrichtungen richten, nachhaltig. Auch Ärzte, Abrechnungs-, Personal- und IT-Abteilungen haben einen besonderen Informationsbedarf und spezielle Fragestellungen.

***HCM:* Was haben die DIN ISO 9001 oder die KTQ-Zertifizierung, die dem Qualitätsmanagement zuzuordnen sind, mit dem Datenschutz zu tun?**
Rüdlin: Diese Norm ist eine von vielen Möglichkeiten, um über zertifizierte Verfahren eine gewisse Qualität in einer Einrichtung zu gewährleisten, auch indem regelmäßige Berichte zu verfassen sind. Die gesetzliche Vorgabe ist § 137 SGB V. Der Datenschutz ist ein Teil davon, erstaunlicherweise aber nicht standardisiert. Oft bekomme ich den Eindruck, es hängt sehr davon ab, welche persönlichen Hintergründe verschiedene Auditoren zu diesem Thema mitbringen. Das ist deutlich ausbaufähig.

ESTHER NIEDERHAMMER

Freie Fachjournalistin, 2004 bis 2007 Mitarbeiterin in der ambulanten Altenpflege,
Kontakt: kontakt@esther-niederhammer.de