ISDSG Institut für Sicherheit und Datenschutz im Gesundheitswesen

ExperSite

Das Magazin für Sicherheit und Datenschutz im Gesundheitswesen

Ausgabe 01 2018

DS-GVO wenn nicht jetzt, wann dann?

Diese Sofortmaßnahmen sollten jetzt noch auf Ihrer Agenda stehen.

Akademie
Seminare, Workshops, Veranstaltungen

Datenschutz oder Täterschutz
Ein schmaler Grat bei der Datenauswertung

Informationssicherheit leben
St. Marien-Krankenhaus Siegen bildet Taskforce

Akademie

Wir bilden Sie aus und fördern den Branchenaustausch für Datenschutz- und Informationssicherheit. Sie sind auf der Suche nach den richtigen Seminaren und Workshops? Dann werfen Sie einen Blick auf unsere Auswahl an Seminaren, Workshops und Tagungen.

SEMINARE

Europäische Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung ist für die meisten Gesundheitseinrichtungen ein Großprojekt. Um das Thema Awareness erfolgreich zu bewerkstelligen sind Praxisseminare unabdingbar. Wir bieten Ihnen:

- Grundlagenschulung für Mitarbeiter und Führungskräfte
- DS-GVO für IT-Fachkräfte
- Informationssicherheit für Datenschutzbeauftragte

… usw.

Kompaktseminar Datenschutz

Der Einstieg in den Beruf des Datenschutzbeauftragten ist nicht immer leicht. Neben einer Vielzahl von gesetzlichen Anforderungen sind auch persönliche und branchenspezifische Kenntnisse mitzubringen. Mit unserem Kompaktkurs Datenschutz erlangen Sie alle Grundlagen, die Sie als Datenschutzbeauftragter benötigen, um erfolgreich in Ihren beruflichen Alltag zu starten. An vier Terminen erhalten Sie das notwendige Expertenwissen, um als gesetzlich geforderter Datenschutzbeauftragter unternehmensintern wie -extern agieren zu können. Neben juristischen und informationstechnologischen Kenntnissen steht dabei u. a. der Ausbau kommunikativer sowie betriebswirtschaftlicher Kompetenzen auf dem Lehrplan.

DER NÄCHSTE KURS FINDET IN DÜSSELDORF GANZTÄGIG AN VIER AUFEINANDERFOLGENDEN FREITAGEN STATT:

- **Der nächste Start ist für Mai 2018 geplant**

Der Kurs findet jeweils von 09.00 bis 16.30 Uhr statt und schließt mit einer schriftlichen Prüfung ab.

Datenschutzbeauftragter (IOM)

Ob es um den verstärkten Einsatz von Social Media in Unternehmen oder aber technische Entwicklungen geht, die Mitarbeitern auch außerhalb des Büros den Zugriff auf Unternehmensinterna ermöglichen – das Thema Datenschutz wird in der Wirtschaftswelt immer wichtiger. Doch was gilt es bei der Nutzung und Verarbeitung personenbezogener Daten für Unternehmen und Einrichtungen zu beachten?

Im Rahmen des zehntägigen berufsbegleitenden Zertifikatslehrgangs »Datenschutzbeauftragte/-r« erlangen die Teilnehmer das notwendige Expertenwissen, um als gesetzlich geforderter Datenschutzbeauftragter unternehmensintern wie -extern agieren zu können. Neben juristischen und informationstechnologischen Kenntnissen steht dabei u. a. die Erweiterung kommunikativer sowie betriebswirtschaftlicher Kompetenzen auf dem Lehrplan.

BEGINN:
09.10.2018 IN ESSEN

Individuelle Workshops für Ihre Einrichtung

Selbstverständlich lassen wir Ihnen gerne ein individuelles Angebot für ein auf Ihre Bedürfnisse abgestimmtes Schulungskonzept zukommen, zum Beispiel aus den Bereichen:

- Auftragsverarbeitung
- DS-GVO
- Mitarbeiterschulungen
- Datenschutz
- Informationssicherheit

Inhalt

Bald ist es so weit. Die DS-GVO kommt.

ISDSG-Akademie 2

Das Team 4

Neuigkeiten 6
Wir räumen auf
10 Gerüchte rund um die DS-GVO

Schwerpunkt 8
Endspurt für Ihre Vorbereitungen auf die EU-Datenschutz-Grundverordnung
Diese Punkte sollten Sie unbedingt noch erledigen

Der Datenschutzbeauftragte 13
Das Intranet – ein Gestaltungsbeispiel
Datenschutz als Teil der Unternehmenskommunikation

Gastbeitrag 14
Datenschutzkonform:
Die Einwilligung im Entlassmanagement

Gastbeitrag 16
Daten- oder Täterschutz?!
Der schmale Grat der Datenauswertung

Informationssicherheit
Informationssicherheit vom Management bis ins Wohnzimmer 18
Ergebnisse aus der Initiative für Informationssicherheit im Gesundheitswesen

Gastbeitrag 20
Koordinationsteam Informationssicherheit
St. Marien-Krankenhaus Siegen lebt Informationssicherheit

Goldene Regeln 22
8. Goldene Regel: Flagge zeigen

EDITORIAL

Trendfaktor Datenschutz

Liebe Leserinnen, liebe Leser,

wann hatten Unternehmen das Thema Datenschutz so präsent vor Augen, wie es momentan der Fall ist? Die Newsfeeds füllen sich zunehmend mit dem aktuellen Trendthema: der EUROPÄISCHEN DATENSCHUTZGRUNDVERORDNUNG.

Das könnte uns Datenschützer kurz frohlocken lassen, weil unser Thema endlich Gehör findet – aber sind wir doch mal ehrlich: Wären da nicht der neue Bußgeldkatalog und das erweiterte Sanktionsrecht der Aufsichtsbehörden, würde niemanden interessieren, was sich auf Gesetzesebene entwickelt.

Ein vielleicht zu naiver Wunsch von mir: Das Bewusstsein für die Notwendigkeit von Datenschutz und den verantwortungsvollen Umgang mit dem digitalen Gold muss wachsen. Zum einen müssen wir wieder mehr Verantwortung für uns selbst (und unsere Daten) übernehmen, zum anderen sollten Unternehmen Themen wie Datenethik, Datenschutz und Informationssicherheit, kurz gesagt das Thema Compliance, verstärkt betrachten, denn: Wir sind alle in der Verantwortung.
Ihre

N. Richard

Nina Richard
Redaktionsleitung

Prof. Dr. Thomas Jäschke

Magnus Welz

Angelica Morina

Jan Domnik

Adrian Lingen

Maximilian Wölk

Nina Richard

Das Team

„Fachexpertise, Professionalität und Praxisnähe“, so lässt sich das ISDSG-Team beschreiben. Aufgrund unserer Kernkompetenzen in den Bereichen IT, Datenschutz und Sicherheit sowie jahrelanger Erfahrung im Gesundheitswesen können wir Ihnen ein breites Spektrum an Unterstützung anbieten, das sich genau an Ihren Bedürfnissen orientiert. Das ISDSG ist ein Dienstleistungsbereich der DATATREE AG.

Christine Thieme

Thorben Beer

Alexander Vogel

Bettina Sandrock

Susann Zorbach

Henning Mertes

Stefan Brandau

Fabian Rüter

Herwarth Reuter

DS-GVO wohin das Auge reicht

DIESE 10 GERÜCHTE HALTEN SICH HARTNÄCKIG RUND UM DIE DS-GVO

Es gibt genau ein Thema, das aktuell die Datenschutz-News dominiert und das ist die Datenschutz-Grundverordnung. Positiv, wenn es das Bewusstsein für das Thema stärkt. Negativ, wenn das Thema von ambitionierten Vertrieblern genutzt wird, um im besten Fall mit dem Kunden noch schnell auf den letzten Metern eine beträchtliche Summe Geld zu verdienen – am liebsten wird dabei das Verkaufsargument ANGST benutzt. Wir räumen daher mit den hartnäckigsten Gerüchten rund um die DS-GVO auf.

1. Bald ist es soweit: Die DS-GVO tritt im Mai diesen Jahres in Kraft …

FALSCH. Die Europäische Datenschutz-Grundverordnung wurde am 04. Mai 2016 im Amtsblatt der Europäischen Union veröffentlicht. Am 20. Veröffentlichungstag ist die Verordnung bereits in Kraft getreten – also am 24. Mai 2016.

Mit einer Übergangsfrist von zwei Jahren wird sie am 25.05.2018 zu geltendem Recht. Dies bedeutet, dass bis zu diesem Zeitpunkt Dokumente und Prozesse angepasst sein sollten.

2. Wenn Sie jetzt mit der Umsetzung der DS-GVO beginnen, haben Sie Ende Mai alles umgesetzt …

NEIN. Um alle Anforderungen der DS-GVO umzusetzen, gilt es mehr zu tun, als ein paar Dokumente anzupassen. Vielmehr geht es um „gelebten Datenschutz", Datenschutzprozesse und einen Qualitätsstandard für diesen Bereich. Kurz gesagt: ein Großprojekt, dessen Gesamtumsetzung nicht innerhalb von vier Wochen machbar ist. Jeder, der Ihnen etwas anderes erzählt, hat seinen Job nicht verstanden. ABER: Es ist auch nie zu spät, um noch anzufangen. Ergreifen Sie jetzt noch die wichtigsten Last-Minute-Maßnahmen, das Anpassen von Dokumenten, wie AV-Verträge, Behandlungsverträge, Verpflichtung auf das Datengeheimnis usw.

3. Es ist kein anderes Gesetz mehr gültig und es gilt nur noch die Datenschutz-Grundverordnung …

FALSCH. Die DS-GVO ersetzt die Datenschutzrichtlinie 95/46/EG aus dem Jahr 1995, die zusammen mit den erlassenen national geltenden Umsetzungsgesetzen (Deutschland: BDSG) galt. Im Gegensatz hierzu gilt die DS-GVO unmittelbar, eine Umsetzung in national gültiges Recht ist nicht notwendig. Allerdings existiert eine Vielzahl von Öffnungsklauseln, die es erlauben, konkrete Regelungen auf nationaler Ebene zu treffen. Hier gilt demnach das BDSG-neu.

Ebenso arbeiten gerade alle Beteiligten auf Länderebene an der Anpassung der Landesdatenschutzgesetze. Außerdem ist mit Anpassungen der Spezialgesetze zu rechnen.

4. Sie brauchen ein Datenschutzsiegel. Mit diesem Siegel wird die Aufsichtsbehörde nicht bei Ihnen klingeln …

FALSCH. Mit der Datenschutz-Grundverordnung wird erstmalig das Thema Zertifizierung auf Gesetzesebene aufgegriffen. „(...) Die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. (Art. 42 DS-GVO)"

Diese, und die folgenden Artikel der DS-GVO werden von unseriösen Stellen gerne genutzt, um Datenschutzsiegel zu verteilen. Achten Sie hier unbedingt auf die Qualität! Tatsächlich kann jedes Unternehmen nach eigenen Qualitätsstandards Siegel vergeben – tatsächlich ist aktuell nur die dakks staatliche Zertifizierungsstelle für den Bereich Datenschutz. By the Way: Achten Sie darauf, was zertifiziert ist.

5. Wenn Sie bis zum 25. Mai nicht alle Maßnahmen umgesetzt haben, können Sie den Laden zumachen …

NEIN. Die Aufsichtsbehörden haben eine erweiterte Kompetenz in Bezug auf die Durchsetzung von Sanktionen und werden diese auch durchsetzen. Nehmen Sie sich deshalb zuerst die Prozesse vor, die die Verarbeitung von besonders schützenswerten Daten umfassen.

PS: Achten Sie auch darauf, dass das Thema DS-GVO von Ihren Wettbewerbern genutzt werden kann, um Sie zu schädigen – der ein oder andere Abmahnanwalt steht bestimmt schon in den Startlöchern.

6. Sie brauchen keinen Datenschutzbeauftragten …

FALSCH. Hier bleibt es beim Alten – haben Sie zehn oder mehr Personen, die personenbezogene Daten verarbeiten, müssen Sie einen Datenschutzbeauftragten bestellen – dieser kann intern oder extern benannt werden. Eine Benennungsurkunde ist nicht mehr notwendig. Der Datenschutzbeauftragte muss eine Vielzahl von Kenntnisse mitbringen.

7. Mit der DS-GVO wird der Datenschutz neu erfunden …

EIN GANZ KLARES NEIN. Was die DS-GVO anstrebt, ist das Angleichen des Europäischen Datenschutzniveaus, um den Schutz von personenbezogenen Daten und zudem einen freien Datenverkehr innerhalb des Europäischen Binnenmarktes zu ermöglichen. Im Vergleich zu manch anderen europäischen Ländern kann sich Deutschland als Vorreiter bezeichnen. Unsere Datenschutzgesetze waren schon vor der Datenschutz-Grundverordnung auf einem hohen Niveau. Grundsätzlich wird der Datenschutz allerdings nicht neu erfunden. Unternehmen, die bereits vorher ein sehr hohes Datenschutzniveau hatten, werden auch zukünftig weniger Herausforderungen zu bewältigen haben, als es schlecht aufgestellte Unternehmen haben.

Grundlegende Änderungen betreffen beispielsweise:

- Soft- und Hardwareentwicklung und -einführung (Stichworte: privacy-by-design; privacy-by-default)
- Ausweitung der Personenrechte
- Meldepflichten bei Verletzungen
- Verschärfter Bußgeldkatalog
- Sicherheit der Verarbeitung von Daten
- Datenschutz-Managementsysteme

8. Es drohen Bußgelder in Höhe von 4 % des weltweit erzielten Umsatzes …

NEIN – gerne vergessen in der Gestaltung werden hier die zwei kleinen Wörter „bis zu“. Bei den 4 % oder 20 Mio. Euro handelt es sich um Maximalwerte, die in der Praxis je nach Schwere des Verstoßes angepasst werden.

9. Mit Software haben Sie im Handumdrehen ein Datenschutzmanagementsystem …

FALSCH. Mit der Einführung eines Datenschutz-Managementsystems ist keine spezielle Software gemeint. Natürlich können Prozesse ab einer gewissen Unternehmensgröße besser in einer Software abgebildet sein – es meint aber vielmehr ein System zur Qualitätssicherung, wie gelebte Prozesse usw. Eine Software ist allerdings nicht die Grundlage für Ihr Datenschutz-Managementsystem.

10. Nach der Übergangsfrist passiert doch sowieso nichts …

NEIN. Datenschutz ist durch die DS-GVO in einen komplett neuen Fokus gerückt. Die Aufsichtsbehörden werden mit Sicherheit aktiv werden. Unser Hinweis: Planen Sie das Projekt strukturiert, umfangreich und langfristig.

Endspurt für Ihre Vorb
EU-Datenschutz-Grund

ereitungen auf die verordnung

Der Countdown läuft, nur noch wenige Wochen – dann ist es soweit: Die Übergangsphase zur am 24. Mai 2016 in Kraft getretenen Datenschutz-Grundverordnung (DS-GVO) endet, sodass diese ab dem 25. Mai 2018 zwingend anzuwenden ist. Sie löst dann sowohl das alte Bundesdatenschutzgesetz (BDSG) ab als auch die EU-Datenschutzrichtlinie (Richtlinie 95/46/EG), auf der das BDSG basierte.

Zur Implementierung eines kompletten Datenschutz-Managementsystems ist die Zeit mittlerweile zu knapp, denn hierbei handelt es sich um ein Großprojekt, das nicht nur über gesetzliche Neuerungen informiert, sondern auch Prozesse innerhalb einer Organisation implementiert und lebt. Dennoch ist eine abwartende Haltung, in der Hoffnung, dass schon alles irgendwie gut geht, nicht der richtige Weg. Wir möchten Ihnen daher eine Reihe von wichtigen Last-Minute-Maßnahmen nennen, die Sie noch jetzt umsetzen sollten, um die ersten Schritte auf Ihrem Weg zur Datenschutzorganisation zu beschreiten.

Überarbeiten Sie Ihre Einwilligungen und Behandlungsverträge

Ihre vorliegenden Dokumente müssen an die neuen Rechtsnormen angepasst werden. Die DS-GVO räumt den Betroffenen deutlich umfassendere Informationsrechte ein, als dies gemäß BDSG der Fall war. Um als datenverarbeitende Stelle den Informationspflichten gerecht zu werden, müssen im Wesentlichen die folgenden Informationen angegeben werden:

- Name und Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters
- die Kontaktdaten des Datenschutzbeauftragten
- die jeweiligen Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie zusätzlich die Rechtsgrundlage für die Verarbeitung
- Darstellung der berechtigten Interessen, falls die Datenverarbeitung auf dem Tatbestand der Interessenabwägung beruht
- gegebenenfalls die Empfänger/Kategorien von Empfängern der Daten
- gegebenenfalls Informationen zur Datenübermittlung in Drittländer (Anforderungen beachten!)

Hierüber muss der Betroffene nicht direkt informiert werden, sondern die Informationen müssen nur zur Verfügung gestellt werden, sprich es reicht, wenn diese zum Beispiel im Internet oder in irgendeinem Aushang stehen.

Wichtig:

Die Mitteilung dieser Informationen hat gemäß Art. 13 DS-GVO sofort bei der Erhebung der Daten zu erfolgen. Prüfen Sie daher Ihre Einwilligungen sowie Behandlungsverträge und passen Sie diese den neuen, geltenden Erfordernissen an.

Aktualisieren Sie die Mitarbeiterverpflichtungen auf das Datengeheimnis

Die DS-GVO schreibt zwar nicht explizit die Verpflichtung auf das Datengeheimnis vor, jedoch verlangt Art. 32 DS-GVO, dass für die Verarbeitung Verantwortliche Schritte unternehmen, „um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet."

Diese Vorgaben erwecken den Anschein, dass eine Belehrung der Mitarbeiter künftig ausreichen würde. Doch dem ist keinesfalls so. Denn auch wenn der Begriff der Verpflichtung auf das Datengeheimnis in der DS-GVO nicht mehr existiert, so bleibt die Thematik des Datengeheimnisses weiterhin bestehen. Die Nachweisanforderungen ergeben sich aus Art. 5 DS-GVO, die den für die Datenverarbeitung Verantwortlichen dazu verpflichten, die Einhaltung des Datengeheimnisses auch explizit nachweisen zu können. Insofern ergibt sich auch durch die DS-GVO die Notwendigkeit einer schriftlichen Verpflichtung. Untermauert wird diese Tatsache zudem durch die Anforderungen des Art. 24 DS-GVO, der das Umsetzen geeigneter technischer und organisatorischer Maßnahmen fordert und ebenfalls zum Nachweis verpflichtet.

Das weiterhin geltende Erfordernis der schriftlichen Verpflichtung der Mitarbeiter auf das Datengeheimnis resultiert aus dieser Rechenschaftspflicht.

Zu beachten ist außerdem, dass der zu betrachtende Personenkreis größer geworden ist. Waren nach BDSG nur bei der datenverarbeitenden Stelle beschäftigte Personen zwingend zu verpflichten, so bezieht die DS-GVO auch Personen mit ein, die potenziell Zugang zu den personenbezogenen Daten haben, wie beispielsweise externe Wartungstechniker oder Reinigungspersonal.

Beachten Sie die künftig geltende 72-Stunden-Melderegel bei Datenschutzverletzungen – entwickeln Sie einen Prozess zur Meldung und kommunizieren Sie diesen.

Grundsätzlich müssen Sie gemäß DS-GVO alle Verletzungen des Schutzes der personenbezogenen Daten melden, es sei denn, „dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen."

Wir empfehlen, hierzu einen Meldeweg/Meldeprozess zu definieren, um bei Vorfällen die Meldung innerhalb der vorgegebenen Frist abgeben zu können. Wichtig: Sorgen Sie dafür, dass der Meldeprozess in Ihrem Unternehmen allen Mitarbeitern bekannt ist. Beachten Sie, dass die Meldung einer Datenschutzverletzung die folgenden Informationen beinhalten muss:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

Wir empfehlen Ihnen das Erstellen eines Formulars zur Meldung von Datenschutzvorfällen, das diese genannten Punkte enthält.

Apropos: Falls die geforderten Informationen nicht alle zum gleichen Zeitpunkt zur Verfügung gestellt werden können, so ist es wichtig, dass Sie diese „ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen".

Schulungskonzept für die Mitarbeiter entwickeln

Der Durchführung praxisorientierter Mitarbeiterschulungen kommt eine sehr große Bedeutung zu, denn es sind die Mitarbeiter, die tagtäglich mit personenbezogenen Daten umgehen und deren Handeln somit für die Qualität des Datenschutzes maßgeblich ist. Durch eine praxisnahe und lebendige Schulung der Mitarbeiter kann das Datenschutzniveau erheblich erhöht werden.

Empfehlenswert ist es, in den Schulungen auch den Bezug zum Bereich der Informationssicherheit herzustellen. Die verständliche Erläuterung von möglichen Angriffsszenarien wie beispielsweise Phishingmails, Trojanern oder auch das Social Engineering, also das Erschleichen des Vertrauens der angegriffenen Person durch den Angreifer, indem vorab umfangreiche Recherchen unternommen werden, erhöht hier die Aufmerksamkeit der Mitarbeiter.

Beachten Sie die Meldepflicht der Kontaktdaten des Datenschutzbeauftragten

Bis spätestens zum 25. Mai 2018 müssen die Kontaktdaten des Datenschutzbeauftragten schriftlich an die zuständige Aufsichtsbehörde übermittelt werden.

Während hierfür die klassischen Kommunikationswege (Fax, E-Mail, Post) zur Verfügung stehen, haben wir auf Anfrage bereits von einigen Aufsichtsbehörden erfahren, dass Lösungen für eine Onlinemeldung zur Verfügung gestellt werden sollen.

Bis spätestens zum 25. Mai 2018 müssen die Kontaktdaten des Datenschutzbeauftragten schriftlich an die zuständige Aufsichtsbehörde übermittelt werden.

Die Umsetzung der Datenschutz-Grundverordnung ist ein Großprojekt. Stellen Sie sich deshalb passgenau Ihr Projektteam zusammen. Denn Prozesse, die nicht gelebt werden, führen nur in eine frustrierende Endlosschleife. Gemeinsam sind Sie stark!

Die Datenschutz-Folgenabschätzung – Was ist zu bedenken?

Setzen Sie sich intensiv mit Ihren Prozessen auseinander und prüfen Sie, ob gegebenenfalls Datenschutz-Folgenabschätzungen nötig sind.

Immer dann, wenn ein Verfahren ein möglicherweise hohes Risiko für den Betroffenen bezüglich seiner Datenschutzrechte birgt, ist zu prüfen, ob eine Datenschutz-Folgenabschätzung durchzuführen ist.

Der Art. 35 DS-GVO ist hier zu befolgen und gibt einen Fahrplan vor, nach dem vorzugehen ist. Wichtig ist, den Rat des Datenschutzbeauftragten einzuholen. Bei einer Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung ist diese dann auch zwingend zu dokumentieren.

Übrigens: Die Aufsichtsbehörden haben angekündigt, sowohl eine Positivliste, also die Nennung von Verfahren, bei denen eine Datenschutz-Folgenabschätzung in jedem Fall durchzuführen ist, zu pflegen als auch eine Negativliste zu erstellen, die Verarbeitungsverfahren nennt, bei denen die Durchführung einer Datenschutz-Folgenabschätzung nicht notwendig ist.

Aktualisieren Sie Ihr Verzeichnis der Verarbeitungstätigkeiten (vormals Verfahrensverzeichnis)

Das Verzeichnis der Verarbeitungstätigkeiten, als Dokumentation und Übersicht aller Prozesse, bei denen personenbezogene Daten verarbeitet werden, ist dahingehend zu verändern, dass zusätzliche Angaben, wie etwa die jeweiligen Löschfristen und die eingesetzten technischen und organisatorischen Maßnahmen dokumentiert werden müssen. Die genauen Anforderungen nennt Art. 30 DS-GVO.

Aufbau einer Projektgruppe kurzfristig in Erwägung ziehen

Klar herausgestellt werden muss, dass das vollständige Umstellen auf die Erfordernisse der EU-DSGVO ein langfristiger Prozess ist, der gerade beim Vorliegen von Gesundheitsdaten, die einem erhöhten Schutzbedarf unterliegen, je nach Größe des Unternehmens einen Zeitraum von bis zu zwei Jahren umfassen kann, da die Implementierung eines umfangreichen Datenschutz-Management-Systems (DSMS) notwendig ist.

Sollte bei Ihnen zum jetzigen Zeitpunkt die Differenz zwischen dem IST-Zustand und den Anforderungen der DS-GVO noch gravierend sein, so wird eine vollständige Umsetzung aller Erfordernisse in der verbleibenden, sehr kurzen Zeit nicht möglich sein.

Unsere Empfehlung ist, in diesem Fall kurzfristig eine Projektgruppe zu bilden, die sich umgehend mit den Anforderungen der DS-GVO auseinandersetzt und die wichtigsten Schritte zielgerichtet einleitet. Übergeordnet ist ein Faktor immens wichtig: Datenschutz ist, in Hinsicht auf die DS-GVO, als Managementaufgabe zu sehen und muss in die Unternehmensprozesse integriert sein. Der Datenschutz sollte somit auch fester Bestandteil der Unternehmensphilosophie sein. Achten Sie darauf, dass der Datenschutzbeauftragte immer dann, wenn Prozesse mit der Verarbeitung personenbezogener Daten in Verbindung stehen, frühzeitig mit in die Kommunikation einbezogen wird. Als gewinnbringend zeigt sich oftmals eine enge Zusammenarbeit mit dem Qualitätsmanagement, da hier viele Prozesse, in denen personenbezogene Daten verarbeitet werden, bereits dokumentiert sind. ■

> *Datenschutz ist, in Hinsicht auf die EU-DSGVO, als Managementaufgabe zu sehen und muss in die Unternehmensprozesse integriert sein.*

Fabian Rüter

Das Intranet – ein Gestaltungsbeispiel

Die interne Unternehmenskommunikation bedient sich einer Vielzahl von Instrumenten. In größeren Unternehmen und Einrichtungen hat sich hierfür die Verwendung des Intranets bewährt. Doch wie können Sie Ihren Bereich im Intranet sinnvoll und nützlich für Ihre Kollegen aufbereiten?

Machen Sie es übersichtlich

Ihre Kollegen können Inhalte nur finden, wenn sie übersichtlich dargestellt werden.

Machen Sie sich deshalb vorab darüber Gedanken, welche Informationen beispielsweise für den Alltag besonders wichtig und welche für viele Ihrer Kollegen „nur informativ" bestimmt sind (zum Beispiel Gesetzestexte).

Beispiel für eine mögliche inhaltliche Struktur

1. Startseite
a. Aktuelle Themen

2. Der Datenschutzbeauftragte
a. Ansiedlung im Organigramm
b. Vorstellung des DSB
c. Datenschutzberichte

3. Datenschutz in der Organisation
a. Datenschutzanfragen
b. Kontaktdaten und Anschriften

4. Interne Richtlinien und Vorlagen
a. Schulungsunterlagen
b. Fachartikel
c. Vorlagen/Muster
d. Datenschutzrichtlinien und Konzepte
e. Arbeits-/Verfahrensanweisungen

5. Gesetze/Rechtstexte/Verordnungen
(Der Aufbau versteht sich exemplarisch.)

In einer Vielzahl von Einrichtungen im Gesundheitswesen ist der Datenschutzbeauftragte operativ über das Qualitätsmanagement oder vergleichbare Stellen eingebunden. Darüber hinaus gilt aber, dass der Datenschutzbeauftragte als selbstständige Stabsstelle unterhalb der Unternehmensleitung angesiedelt sein muss und demnach auch entsprechend losgelöst in das Intranet einzutragen ist.

Beispielhafte Gestaltung von Inhalten – so könnte Ihre Startseite aussehen

Startseite

Der Einleitungstext kann gerne auch in einer Seitenspalte dargestellt und der Abschnitt „Aktuelles" in den Mittelpunkt gerückt werden. Die Ansprache bzw. der Einstieg soll nach dem unternehmensinternen Standard erfolgen. Wir haben Ihnen zwei Beispiele, einmal im eher formellen und einmal im kollegialen Ton, zusammengestellt:

Beispiel 1 (formell)
Sehr geehrte Mitarbeiterinnen und Mitarbeiter, in unserer Funktion als betrieblicher Datenschutzbeauftragter (DSB) der *[Platzhalter Einrichtung]* möchten wir Ihnen in diesem Bereich einige Informationen zum Thema „Datenschutz" und den damit verbundenen Aufgaben darstellen.}

Beispiel 2 (kollegial)
Herzlich willkommen, im Themenbereich „Datenschutz" bei der *[Platzhalter Einrichtung]*. Wir nehmen in Ihrem Unternehmen die Aufgaben des betrieblichen Datenschutzbeauftragten (DSB) wahr und möchten Ihnen in diesem Bereich einige Informationen zu den damit verbundenen Aufgaben zur Verfügung stellen.}

Wir sind gleichermaßen Ansprechpartner für Mitarbeiter, *[Medizinische Einrichtung | Patienten] [Dienstleister| Kunden]* und auch Externe bei allen Fragen rund um den „Datenschutz". Sollten Sie nicht sicher sein, ob Ihr Anliegen bei uns richtig aufgehoben ist, gilt grundsätzlich „lieber einmal mehr nachfragen als zu wenig".

Sie haben eine konkrete Frage oder ein Anliegen für den Datenschutzbeauftragten?

[Anfrage aufgeben] (Verweis auf das interne Meldesystem (falls vorhanden))

Aktuelle Themen
In diesem Bereich sollen aktuelle unternehmensinterne Meldungen (zum Beispiel Ankündigung von Datenschutzbegehungen, neue Arbeitsanweisungen usw.) und allgemeine Branchennews rund um das Thema Datenschutz und IT-Sicherheit veröffentlicht werden. Wir stellen diese Inhalte in unregelmäßigen Abständen per E-Mail zur Verfügung. Bitte teilen Sie die E-Mail-Adressen aller Mitarbeiter mit, die diese Informationen erhalten sollen.

Die datenschutzkonforme Einwilligung im Entlassmanagement

Das Entlassmanagement bringt nicht nur durch die DS-GVO neue Herausforderungen mit sich. Rechtsanwältin Sandra Große erklärt, wie Sie Einwilligungen datenschutzkonform gestalten.

Seit Inkrafttreten der Rahmenvereinbarung zum Entlassmanagement am 01.10.2017 zwischen dem GKV-Spitzenverband, der Kassenärztlichen Bundesvereinigung (KBV) sowie der Deutschen Krankenhausgesellschaft werden nunmehr die gesetzlichen Regelungen des bereits Mitte 2015 in Kraft getretenen GKV-Versorgungsstärkungsgesetzes auch beim Entlassmanagement umgesetzt. Jedoch scheinen sowohl die gesetzliche Regelung des § 39 Abs. 1a SGB V, die durch den Gemeinsamen Bundesausschuss angepassten Richtlinien und der Rahmenvertrag in der Praxis mehr Fragen als Antworten aufzuwerfen.

Zusammenarbeit von Krankenhäusern und Leistungserbringern ist ausdrücklich erwünscht

Neben all den offenen Fragen, die sich für Kooperationspartner des Krankenhauses oder innerhalb des Verordnungsrechts und Verordnungspflicht, Genehmigungspflicht, Hilfsmittelausschreibung ergeben, darf der eigentliche Zweck dieser Regelungen nicht vergessen werden. Es geht um die Unterstützung einer sektorenübergreifenden Versorgung der Versicherten beim Übergang in die Versorgung nach Krankenhausbehandlung. Eine entsprechende Anschlussversorgung kann zum Beispiel eine medizinische oder pflegerische Versorgung umfassen. Hierzu können Terminvereinbarungen mit Ärzten, Physiotherapeuten, Pflegediensten oder Hilfsmittelversorgern die Beantragung von Leistungen bei der Kranken- bzw. Pflegekasse gehören.

Zu betonen ist dabei, dass der Gesetzgeber eine Zusammenarbeit von Krankenhäusern und anderen Leistungserbringern ausdrücklich erwünscht hat.

Von Wahlrecht und Einwilligungen

Das Krankenhaus hat eine gesetzliche Verpflichtung, dem Patienten ein Entlassmanagement vorzuhalten, damit für ihn eine lückenlose Anschlussbehandlung organisiert werden kann. Dies setzt aber zwingend voraus, dass der Patient zum einen sein Wahlrecht ausübt und zum anderen eine wirksame Einwilligung zur Datenweitergabe an externe Leistungserbringer und auch seine Krankenkasse, sowohl die privaten als auch die gesetzliche, erteilt hat.

Sicherstellen von Informationsaustausch

Der Patient hat das Recht, sich seinen nachstationären ambulanten Leistungserbringer auszuwählen. Auch wenn das Krankenhaus sinnvollerweise mit Kooperationspartnern zusammenarbeitet, darf dem

Patienten das Wahlrecht nicht genommen werden. Wünscht ein Patient nicht durch einen Kooperationspartner des Krankenhauses versorgt zu werden, besteht für ihn die Möglichkeit, unter den im System der gesetzlichen Sozialleistungsträger für den maßgeblichen Versorgungsbereich zugelassenen oder präqualifizierten Leistungserbringern auszuwählen und diese im Rahmen des Entlassmanagements zu beauftragen. Das Krankenhaus ist dann verpflichtet, mit diesem ausgewählten Leistungserbringer Kontakt aufzunehmen, um die Überleitung anzubahnen und den Informationsaustausch sicherzustellen. Hierbei geht der Patient allerdings das Risiko ein, dass mangels enger Kooperation mit dem von ihm ausgewählten Leistungserbringer

Der Patient hat das Recht, sich seinen nachstationären ambulanten Leistungserbringer auszuwählen.

weder sichergestellt ist, dass die sachlichen bzw. personellen Ressourcen von diesem Leistungserbringer tatsächlich vorgehalten werden und zeitnah zur Verfügung stehen, noch dass der Leistungserbringer in der Lage ist, unverzüglich auf Mitteilung des konkreten Versorgungsbedarfs seitens des Krankenhauses zu reagieren, den Patienten zu kontaktieren, den ambulanten Versorgungsbedarf näher zu spezifizieren, erforderliche Anträge zu erstellen und so zu einer unverzüglichen Versorgung mit allen für die ambulante Versorgung benötigten Produkten und Dienstleistungen beizutragen. Über diese Unterschiede muss das Krankenhaus den Patienten im Rahmen der Informations- und Beratungspflicht und der Anlage 1a des Rahmenvertrages aufklären.

Hat der Patient seinen weiteren Leistungserbringer für die ambulante Versorgung ausgewählt, ist das Krankenhaus aufgrund der Einwilligung in das Entlassmanagement zur Datenweitergabe an den jeweiligen Leistungserbringer und die Krankenkasse des Patienten berechtigt. Hierzu ist der Vordruck der Anlage 1b zum Rahmenvertrag Entlassmanagement zwingend zu nutzen. Erfolgt dies nicht, liegt ein Verstoß gegen den Rahmenvertrag vor.

Nur aufgrund der Einwilligung des Patienten darf das Krankenhaus überhaupt an externe Leistungserbringer die Daten weiterleiten.

Nur aufgrund dieser Einwilligung des Patienten darf das Krankenhaus überhaupt an externe Leistungserbringer die Daten weiterleiten.
Diese Einwilligung muss ausdrücklich auf den konkreten Einzelfall bezogen und eindeutig sein, damit der Patient über die Verarbeitung der Gesundheitsdaten informiert ist.

Im Mai kommt die DS-GVO

Nach der ab dem 25. Mai 2018 unmittelbar anzuwendenden Datenschutzgrundverordnung muss der Patient seine Einwilligung gem. Art. 7 DS-GVO freiwillig erteilen. Inwieweit eine Freiwilligkeit vorliegt und wie dieser unbestimmte Rechtsbegriff auszulegen ist, wird beispielsweise in den Erwägungsgründen 42 und 43 zur DS-GVO geregelt. Danach kann nur dann von einer freiwilligen Einwilligung ausgegangen werden, wenn die betroffene Person eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden. Denn dann ist davon auszugehen, dass dem Patienten der einzuwilligende Sachverhalt ausreichend transparent ist. Die Einwilligung gilt hingegen nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist. Demnach ist die Einwilligung von sonstigen Erklärungen zu trennen, zumindest aber deutlich hervorzuheben.

Darüber hinaus soll der Grundsatz der Transparenz gem. Art. 5 Abs. 1a) DS-GVO gewährleisten, dass der Patient im engeren Sinne seine Betroffenenrechte und im weiteren Sinne generell sein Recht auf informationelle Selbstbestimmung wahrnehmen kann. Dem kann nur dann Genüge getan werden, wenn die verantwortliche Stelle – das Krankenhaus – über die Datenverarbeitung im ausreichenden Maße informiert. Die Datenschutzgrundverordnung regelt die Informationspflichten in den Art. 13 und 14 in zwei sehr umfangreichen und über das bisher Erforderliche hinausgehenden Katalogen. Ergänzend dazu finden sich in einer Vielzahl der Erwägungsgründe der Datenschutzgrundverordnung Anmerkungen und Hinweise, welche den Grundsatz der fairen und transparenten Verarbeitung stets hervorheben. Dieser Katalog sollte von den Krankenhäusern in ihren Datenschutzerklärungen aufgenommen werden, um die Einwilligung nach Anlage 1b des Rahmenvertrages datenschutzkonform zu gestalten. ■

Sandra Große

Sandra Große, Rechtsanwältin, arbeitet für die im Gesundheitsmarkt spezialisierte Kanzlei HARTMANN Rechtsanwälte und berät Unternehmen und Versicherte in allen das deutsche Gesundheitswesen betreffenden Fragestellungen mit Schwerpunkt Datenschutz und Datensicherheit.

Jürgen Hirsch (geb. 1964) ist Gründer und arbeitet als Geschäftsführer des Softwareunternehmens Qyte GmbH, das Werkzeuge für die Datenanalyse (RayQ) herstellt. Als Analyst ist er spezialisiert auf komplexe Analysen zur Betrugsaufdeckung und die Entwicklung von Modellen zur Betrugsvermeidung. Durch den praktischen Einsatz dieser Werkzeuge in der Revisionspraxis kennt er die zahlreichen Spannungsfelder zwischen Nutzen und Risiken dieser Verfahren. Jürgen Hirsch ist Dozent an privaten Hochschulen und Referent für die Themen Datenanalyse und Betrugsabwehr bei verschiedenen Schulungs- und Seminaranbietern.
hirsch@qyte.com
www.qyte.com

Sascha Wiskandt ist seit über zehn Jahren Seniorberater bei der CAS AG und verantwortet die Teamleitung des Themenbereiches Krankenversicherung. Als Projektleiter, BI-Architekt und Scrum Master berät er insbesondere Kunden aus dem Umfeld der Krankenversicherungen bei der Konzeption und dem Design von Integrations- und DataWarehouse-Architekturen.

Im Rahmen der zunehmenden regulatorischen Anforderungen bei Versicherern in Bezug auf die Datenherkunft hat er sich auf die Themen Data-Governance und Data-Lineage spezialisiert.
sascha.wiskandt@c-a-s.de
www.c-a-s.de

Daten- oder Täterschutz?!

Die Aufdeckung von Missbräuchen, insbesondere im Bereich des Arzneimittelbetrugs, wird ohne gezielte Verfahren wie zum Beispiel durch Datenanalysen zunehmend schwieriger. Das Thema Datenanalyse führt im Zusammenhang mit dem Thema Datenschutz aber auch zu großer Unsicherheit, inwieweit nach der Einführung der EU-Datenschutzrichtlinie (GDPR) im Mai 2018 die Daten der Versicherten noch analysiert und ausgewertet werden dürfen.

Gut versteckt in der Masse

Für Täter ist es leicht, in der Masse unterzutauchen, reicht doch ein angepasstes Verhalten, um unsichtbar zu agieren. So einfach ist das Kernproblem in der Praxis der Datenanalyse zu beschreiben: Indikatoren und Spuren krimineller Handlungen sind in gewaltigen Daten- und Informationsmengen versteckt. Die schiere Masse der Daten ist dabei ein wesentlicher Faktor für ein brauchbares Versteck. Im Gesundheitswesen erzeugen schon relativ kleine Gruppen von Versicherten und Leistungserbringern beträchtliche Datenmengen, welche die Auffälligkeiten einer einzelnen Abrechnung oder Verordnung komplett überlagern.

Die große Masse der Daten ist der Grund, dass gängige Analyselösungen auf die Vorhaltung von aufbereiteten Daten abzielen. Die Detailinformationen beispielsweise eines Einzelrezeptes gehen dabei schnell in aufsummierten Aufstellungen, zum Beispiel über Wirkstoffe oder Apotheken, unter. Diese sind dann nur noch mittelbar zu identifizieren und die primäre Spur ist somit verwischt. Untersuchungen auf einer aggregierten Datenbasis sind grundsätzlich zwar möglich, jedoch sind die Informationen bereits auf einen generellen Standard eingeschränkt.

Bei einem sehr konkreten Verdachtsfall zu einer kriminellen Handlung kann die Analyse der aggregierten Datenbasis möglicherweise Einzelfälle erkennen lassen. Dieses ist aber leider entsprechend selten und eher zufällig.

Die erfolgreiche Identifizierung von Abrechnungsbetrug ist wesentlich davon abhängig, dass Rohdaten ohne vorherige Aggregation mit spezialisierten Verfahren für Data-Mining untersucht werden. Ziel dieser Verfahren ist es, Auffälligkeiten und Muster in den Daten zu finden, die es erlauben, Rückschlüsse auf eventuell kriminelle Handlungen zu ziehen und diese zu identifizieren.

Vor dem Hintergrund dieser intensiven Datenanalysen steht dann für Krankenversicherer die Frage im Raum, ob ohne entsprechende Vorfilterung alle Versicherten und Leistungserbringer unter Generalverdacht gestellt werden und ob die gesetzliche Ermächtigung zum Beispiel nach § 197a SGB V für die umfassende Auswertung ausreicht. Tauchen auch interne Sachbearbeiter in Auswertungen auf, weil besondere Leistungskorrelationen immer durch eine bestimmte Person bearbeitet und freigegeben werden, ist es im Vorfeld der neuen EU-Datenschutzgrundverordnung sehr schwer zu entscheiden, welche Analysen zulässig sind und welche unterbleiben müssen.

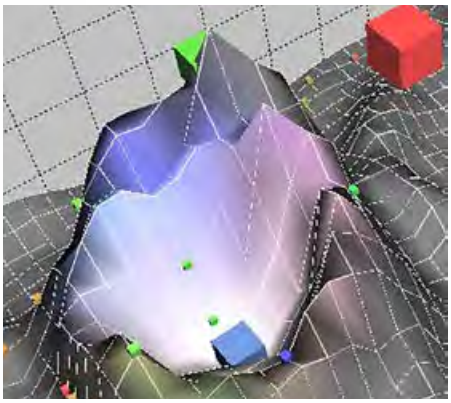
Diese Situation ist für potenzielle Täter die beste Ausgangslage, um Betrugsvarianten zu erproben.

Neuronale Netze benötigen keine Namen oder Versichertennummern, um Täter zu identifizieren

Die Analyse pseudonymisierter Daten mittels neuronaler Netze erlaubt in der Masse der Daten diejenigen Vorgänge zu erkennen, die sich von den anderen Vorgängen unterscheiden. Auch ohne juristisches Detailwissen ist es so möglich, Datenanalysen durchzuführen, die den bestehenden Limitationen und Bedenken als pragmatische, zulässige Lösung gegenübersteht.

Die Daten werden dabei selbst zum Hintergrund, vor dem sich auffällige Zusammenhänge besser erkennen lassen und die einzelne Person als Patient oder der konkrete Leistungserbringer treten hinter pseudonymen Ziffern oder Zeichenketten zurück. Für die aufscheinenden auffälligen Datensätze besteht dann ein Anfangsverdacht auf dolose Handlungen.

Dieser Ansatz der künstlichen Intelligenz erlaubt die Interpretation von versteckten Mustern in den vorhandenen Daten ohne vorbelegten Anfangsverdacht oder die Erhebung einer Hypothese. Datenanalysen sind so ohne Generalverdacht möglich.



Datenanalyse neuronales Netz

Die kriminelle Kreativität bei der Anpassung von Betrugsmustern und die vielfältigen technischen Möglichkeiten machen eine gezielte Identifizierung von Tätern, um Abrechnungsbetrug wirkungsvoll zu bekämpfen, zu einer kontinuierlichen Herausforderung. Neben der Minimierung von wirtschaftlichen Schäden durch einen Rückertrag sind insbesondere Präventionsmaßnahmen stetig weiterzuentwickeln.

Die neue EU-Datenschutzgrundverordnung führt zu breiter Verunsicherung, sodass sich niemand in der Lage sieht, abzuschätzen, welche Datenanalysen zulässig sind und welche nicht. Ein zögerliches Abwarten kann jedoch Krankenversicherungen und Versicherten möglicherweise großen Schaden zufügen und ungewollt betrügerischen Handlungen passiv Vorschub leisten.

Die Techniken der Analyse von Massendaten erlauben es, Warnsignale für Abrechnungsbetrug zu entdecken, angemessen auf diese zu reagieren und geeignete Präventionsmaßnahmen abzuleiten, um so Mehrausgaben im Gesundheitswesen zu reduzieren. ■

Sascha Wiskandt und Jürgen Hirsch

Informationssicherheit vom Management bis ins Wohnzimmer

Eine gemeinsame Kommunikationsebene von Informationssicherheits-, Datenschutzbeauftragten und Geschäftsführern lässt sich finden.

Während des letzten Treffens der Initiative stellten sich Vertreter aus Datenschutz, Informationssicherheit sowie der Geschäftsführung aus Kliniken und Gesundheitseinrichtungen aus ganz Deutschland dem Thema „Management Attention" und diskutierten über Herausforderungen und Lösungsansätze für das Gesundheitswesen.

Wie finden Verantwortliche für Informationssicherheit und Datenschutz eine gemeinsame Kommunikationsebene mit dem Management ihrer Einrichtung?

Die Rolle des Informationssicherheitsbeauftragten ist bisher nicht gesetzlich geregelt. Genau das führt dazu, dass Zuständigkeiten und Verantwortlichkeiten nicht eindeutig sind. Häufig sind es IT-Verantwortliche, die sich „nebenbei" um die Informationssicherheit kümmern sollen. Dies erschwert die Kommunikation sowie die eigene Stellung gegenüber dem Management. Hier muss häufig erst noch das Bewusstsein für die Notwendigkeit von Budget und Ressourcen geschaffen werden, damit ein ausreichendes Managementsystem für Informationssicherheit implementiert werden kann. In vorbildlichen Fällen sind aber ausreichende Management Attention und Budgets vorhanden, wie sich auch in den Diskussionen herausstellte.

Cybercrime-Potenziale sind noch lange nicht ausgeschöpft

Den Auftakt der Veranstaltung machte Landeshauptkommissar Peter Vahrenhorst vom Landeskriminalamt Nordrhein-Westfalen, der in seinem praxisnahen Vortrag auf die aktuellen Herausforderungen der Cyberkriminalität einging. Mit einem Schaden von 55 Millionen Euro pro Jahr ist Cyberkriminalität eine erhebliche Bedrohung für die deutsche Wirtschaft. „Und bei dieser Zahl handelt es sich nur um die gemeldeten Schäden – die Dunkelziffer ist um einiges höher."

> *Darüber hinaus findet die Bedrohung nicht nur im klinischen Alltag statt, sondern betrifft jeden von uns: bis ins eigene Wohnzimmer.*

Darüber hinaus findet die Bedrohung nicht nur im klinischen Alltag statt, sondern betrifft jeden von uns: bis ins eigene Wohnzimmer. Geräteentwicklungen, die unter Begrifflichkeiten wie Internet of Things, smart oder autonomes Fahren entwickelt werden, bieten Kriminellen neue Möglichkeiten und Wege, uns anzugreifen.

Von der Möglichkeit, private Gespräche abzuhören, der Sprachsteuerung in modernen Fernsehgeräten bis zur Ausnutzung von IT-Schwachstellen in Medizingeräten gibt es viele Wege, in erheblichem Ausmaß im Klinikalltag Patientendaten abzugreifen und sogar die Gesundheit bzw. das Leben der Opfer zu gefährden.

Niemand ist sicher

Kliniken, Behörden oder auch Privatpersonen haben eines gemeinsam. Niemand ist vor Hackerangriffen sicher. Aktuelle Phänomene, wie Erpressungssoftware (Ransomware) oder Schadsoftware, die direkt auf dem mobilen Endgerät installiert werden (Mobile Malware), sind nur zwei von einer Vielzahl von Schadsoftware. Darüber hinaus wird Cyberkriminalität aber auch zunehmend zu einem immer professioneller werdenden Servicemodell. Hierbei zu nennen sind Denial of Service, Crime as a Service oder Advanced Persistent Threads, die sich zunehmender Beliebtheit erfreuen.

Vahrenhorst machte deutlich, dass das in NRW gegründete Kompetenzzentrum Cybercrime Hilfestellung bietet. Die Experten des Kompetenzzentrums Cybercrime beraten Behörden und Unternehmen bei der Ermittlung gegen Cyberkriminelle. Zur Meldung von Vorfällen wurde der Single Point of Contact (SPoC) eingerichtet, der rund um die Uhr an sieben Tagen der Woche erreichbar ist.

„Ein Managementsystem für Informationssicherheit ist kein IT-System"

Nach dem Vortrag des Kriminalhauptkommissars tauchte Informationssicherheitsberater Jan Domnik von der DATATREE AG in die Organisationsstruktur von Einrichtungen ein und widmete sich den Präventionsmaßnahmen, die Einrichtungen im Gesundheitswesen durchführen können. „Auch wenn Ihnen motivierte Vertriebler technische Lösungen verkaufen wollen, die angeblich all Ihre Sicherheitsprobleme lösen – die Thematik ist in der Realität leider etwas komplexer. Denn Informationssicherheit bindet personelle, zeitliche und auch monetäre Ressourcen." Der einzige Weg für Einrichtungen, sinnvolle Informationssicherheit zu betreiben, ist der Aufbau eines Managementsystems für Informationssicherheit. Ein Managementsystem

> *Es macht keinen Sinn, wenn Sie sich zu Tode dokumentieren, ohne echte Informationssicherheit leben zu können.*

bezeichnet keine Software. Vielmehr wird hiermit die Bündelung von Ressourcen und Einzelsystemen gemeint, die die Organisation der Informationssicherheit ermöglicht.

Domnik stellte verschiedene Ansätze aus der Praxis dar und verdeutlichte, dass sich

Schutz durch Gemeinschaft, und Know-how-Aufbau und Erfahrungsaustausch: Die Allianz für mehr Informationssicherheit wächst stetig. Partizipieren Sie an der Initiative.

Verantwortliche an bewährten Standards wie beispielsweise der ISO 27001 orientieren sollten.„Wichtig bei der Einführung eines Managementsystems für Informationssicherheit ist und bleibt der Pragmatismus, mit dem solche Ansätze in Unternehmen gebracht werden. Es macht keinen Sinn, wenn Sie sich zu Tode dokumentieren, ohne echte Informationssicherheit leben zu können."

Aus diesem Grund kann es sinnvoll sein, nur die wichtigen Teilaspekte aus den bewährten Standards zu nutzen.

Management Attention – Informationssicherheit ist Führungsaufgabe

Während sich die Geschäftsführung der Unternehmung mit unternehmerischen Gesamtstrategien beschäftigt, sind Verantwortliche der Informationssicherheit häufig eher operative Experten. Dies führt dazu, dass sich beide Parteien kommunikativ auf zwei unterschiedlichen Ebenen befinden und einander nicht das ausreichende Gehör schenken (können). Doch wie gelingt es dem Verantwortlichen für Informationssicherheit, sich und seine Anliegen so zu präsentieren, dass er Gehör findet?

Professor Dr. Thomas Jäschke hatte hierzu einige Umsetzungsideen, die gemeinsam im Expertenkreis diskutiert wurden.

Präsentieren Sie sich

Hierzu gehört, dass Verantwortliche sich und ihre Arbeit , Risikoanalysen, Handlungsempfehlungen und Arbeitsergebnisse regelmäßig vor der Geschäftsführung managementgerecht präsentieren. „Nehmen Sie hierzu die strategische Ebene ein", so der Informationssicherheitsbeauftragte:

- **„Machen Sie Probleme deutlich"**
  Probleme können nicht aufgezeigt werden, wenn Sie auf der Ebene des IT-Experten diskutieren. Machen Sie deshalb Probleme deutlich, indem Sie diese beispielsweise verbildlichen oder Beispiele aus der aktuellen Tagespresse sammeln, um Parallelen zu der eigenen Einrichtung herzustellen.
- **„Gemeinsam sind Sie stark"**
  Existiert das Bewusstsein für ein Problem nicht nur bei einer Einzelperson, sondern bei einer Vielzahl von Betroffenen, erhält die Darstellung eines Problems eine stärkere Gewichtung.

Über die Initiative für Informationssicherheit im Gesundheitswesen

Die jüngsten Vorfälle haben gezeigt, dass niemand von uns sicher vor Hackerangriffen ist. Die Auslegung innerhalb der Medien war dabei nicht immer ganz korrekt. Dies führt zu Zweifeln an Deutschlands Krankenhäusern und der Sicherheit der hoch sensiblen Gesundheitsdaten. Diesem Bild soll mit der Initiative für IT-Sicherheit im Gesundheitswesen öffentlichkeitswirksam entgegengewirkt werden. Das ISDSG – Institut für Sicherheit und Datenschutz im Gesundheitswesen möchte deshalb einen Zusammenschluss von IT- Verantwortlichen, Geschäftsführern und Datenschutzbeauftragten herbeiführen, um Transparenz und Aufklärungsarbeit im Bereich der IT-Sicherheit zu schaffen. Es sollen so praxisnahe Handlungsempfehlungen für die Krankenhauslandschaft entwickelt werden.

Mitglieder der Initiative sind:

- Asklepios Kliniken GmbH & Co. KGaA
- Diakonisches Werk Bethanien e.V.
- Institut für Sicherheit und Datenschutz im Gesundheitswesen
- KIT Services GmbH - Knappschaft Bahn See
- Klinikum Chemnitz gGmbH
- Kliniken Essen-Mitte – Evang. Huyssens-Stiftung/Knappschaft GmbH
- Krankenhaus-Kommunikations-Centrum
- radprax Gesellschaft für Medizinische Versorgungszentren mbH
- Serapion
- St. Marien-Krankenhaus Siegen gem. GmbH ■

Nina Richard

Die Informationssicherheit hat in den letzten Jahren erheblich an Bedeutung gewonnen. Insbesondere im Krankenhausbereich ist das Thema aufgrund der hohen Komplexität nicht mehr durch eine einzelne Person, sondern nur über ein stimmiges Konzept und im Team für die gesamte Organisation abbildbar. Das Team Informationssicherheit berät Management und Mitarbeiter in Fragen der Informationssicherheit. Dabei reicht das Spektrum von Analysen zur Sicherheit und Datenschutzkonformität einzelner Softwarelösungen bis hin zur konkreten Abwehr von Gefahren im Klinikalltag.

Das Themagehört in viele Hände

Der Betrieb von IT-Systemen ist für alle Unternehmen mit Risiken verbunden, die permanent vorhanden sind und als inhärente Risiken bezeichnet werden können. Diese Risiken müssen durch ein engmaschiges und funktionsfähiges internes Kontrollsystem auf ein Minimum begrenzt werden. Es muss gefragt werden, wie ein Gesundheitsunternehmen diesen Aufgaben gerecht werden kann?

Sicher ist, dass der Aufbau einer Informationssicherheitsorganisation alle Akteure im Unternehmen berücksichtigen muss und nicht nur auf die Spezialisten der IT-Abteilung zurückgreifen darf. So wird vermieden, dass Aspekte ausschließlich durch die Expertenbrille betrachtet werden und so der unternehmerische Gesamtkontext unberücksichtigt bleibt. Am Beispiel des Koordinationsteams Informationssicherheit am St. Marien-Krankenhaus Siegen gem. GmbH wird nun aufgezeigt, wie eine solche Aufgabe interprofessionell angegangen werden kann. Den Grundstein zur Schaffung einer berufsübergreifenden Sicherheitsorganisation bildete die Risikoanalyse eines unabhängigen Beratungsunternehmens. Hierbei wurden eine Einschätzung der aktuellen Bedrohungssituation, ausgehend von einem zunächst mittleren Schutzbedarf im Sinne der Definition des Bundesamtes für Sicherheit in der Informationstechnologie (BSI), vorgenommen und ein Maßnahmenplan mit Priorisierung der empfohlenen

Koordinationsteam Informationssicherheit

Vorstellung des interprofessionellen Ansatzes im St. Marien-Krankenhaus Siegen

Maßnahmen entwickelt. Darauf aufbauend wurde als sinnvolle Vorgehensweise zur Umsetzung dieser Maßnahmen die zielgruppengerechte Aufbereitung des geplanten Sicherheitskonzepts beschlossen.

Zur Initiierung, Umsetzung, Überwachung und Evaluation der notwendigen Schritte entstand dann der Gedanke der Implementierung eines Koordinationsteams Informationssicherheit zur berufsübergreifenden Zusammenarbeit mit dem Ziel der Erstellung eines Informationssicherheitskonzepts. Das im Unternehmen bereits bestehende Koordinationsteam IT-Sicherheit erhielt eine neue Geschäftsordnung mit erweiterten Aufgaben, wurde umbenannt und personell ergänzt. Informationssicherheit besteht dabei primär darin, die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen sicherzustellen. Aufgabe dieses Teams ist die Gewährleistung eines informationstechnischen Sicherheitsniveaus, das auch aus rechtlicher Sicht zwingend notwendig ist; die Bestellung eines IT-Sicherheitsbeauftragten dient ebenfalls diesen Zielen. Darüber hinausgehende selbstgestellte Anforderungen an die Informationssicherheit kommen gegebenenfalls hinzu und müssen ebenfalls erfüllt werden. Bei sämtlichen Maßnahmen zur Informationssicherheit ist zu berücksichtigen, wie hoch im Einzelfall die Wahrscheinlichkeit eines Schadens ist, mit welcher Schadenshöhe zu rechnen ist und welche Schutzmaßnahmen konkret hieraus resultieren und sinnvoll erscheinen.

Zusammensetzung des Teams:

Das Koordinationsteam Informationssicherheit im St. Marien-Krankenhaus Siegen setzt sich aus folgenden Personen zusammen:

a) dem von der Geschäftsführung ernannten IT-Sicherheitsbeauftragten
b) dem Leiter der Zentralen Dienste IT und Informationsmanagement
c) dem von der Geschäftsführung ernannten Datenschutzbeauftragten
d) dem Leiter Referat Organisationsentwicklung und Qualitätsmanagement
e) dem Leiter Referat Risikomanagement
f) dem Leiter Referat Kommunikation und Marketing
g) dem Leiter der Betriebstechnik
h) einem von der Geschäftsführung ernannten Vertreter aus dem Bereich der Medizin
i) einem von der Geschäftsführung ernannten Vertreter aus dem Bereich der Pflege

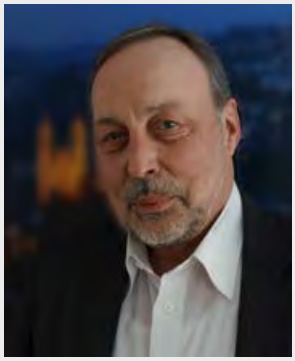
An den Sitzungen des Koordinationsteams Informationssicherheit kann die Geschäftsführung jederzeit teilnehmen. Das Koordinationsteam Informationssicherheit wird durch den IT-Sicherheitsbeauftragten geleitet. Dieser kann zu den Sitzungen weitere Personen zur Teilnahme zulassen und die Zulassung jederzeit widerrufen. Er berichtet der Geschäftsführung regelmäßig. Die Beschlüsse des Koordinationsteams Informationssicherheit stellen Empfehlungen dar. Die Inkraftsetzung erfolgt durch die Geschäftsführung.

Organisation des Teams

Das Koordinationsteam Informationssicherheit trifft sich regelmäßig zweimonatlich. Darüber hinaus werden bei Bedarf und aktuellen Ereignissen (wie zum Beispiel während der massiven Angriffe mit Ransomware) auch außerplanmäßige Sitzungen einberufen. Die Einladungen erfolgen durch den IT-Sicherheitsbeauftragten. Dieser legt auch, orientiert an den Bausteinen des BSI, die Tagesordnungspunkte fest. Übergreifende Aspekte (Organisation, Datenschutz und Berechtigungsmanagement), Infrastruktur, IT-Systeme, Netze und Anwendungen bilden das Gerüst der zu behandelnden Themen.

Im Koordinationsteam Informationssicherheit beschlossene Maßnahmen werden nach eingehender Risikobetrachtung und -bewertung mit der Geschäftsführung erörtert. Die Umsetzung der dort getroffenen Entscheidungen wird im Koordinationsteam geplant und durchgeführt. Jedes Mitglied trägt nach seinen Möglichkeiten in dem Fachbereich hierzu bei. Gerade an diesem wichtigen Punkt zeigt sich der Vorteil eines interprofessionellen Teams. Das Koordinationsteam Informationssicherheit agiert nun seit circa zwei Jahren in der genannten Konstellation. In dieser Zeit konnte das Thema Informationssicherheit im St. Marien-Krankenhaus Siegen entscheidend vorangebracht werden. Die Sensibilisierung der Mitarbeitenden konnte so vorangebracht werden, dass das Team zentraler Anlaufpunkt für alle Fragestellungen rund um die Informationssicherheit geworden ist. ■

Rüdiger Karbach



Rüdiger Karbach
Zentrale Dienste IT- und Informationsmanagement
Die St. Marien-Krankenhaus Siegen gem. GmbH, die GSS Gesundheits-Service Siegen gem. GmbH und die MVZ Medizinisches Versorgungszentrum am St. Marien-Krankenhaus Siegen GmbH sind ein modern geführtes und organisiertes integriertes Gesundheitsunternehmen mit schlanken und transparenten Strukturen. Das Unternehmen beschäftigt in seinen Einrichtungen und Filialen in den Bundesländern Nordrhein-Westfalen und Rheinland-Pfalz über 1800 Menschen.

8. Goldene Regel: Flagge zeigen

Das Thema Datenschutz darf und sollte kein Tabuthema sein. Trauen Sie sich und kommunizieren Sie, dass Sie vorbildlich mit den Daten Ihrer Patienten umgehen.

Einrichtungen im Gesundheitswesen können, ebenso wie es bereits die Großen der strategischen Positionierung predigen, Alleinstellungsmerkmale definieren, mit denen sie die Einrichtung als Nummer 1 vermarkten können. Die definierten Nutzenversprechen für die Patienten bilden im Rahmen der ganzheitlichen Kommunikationsstrategie das Alleinstellungsmerkmal, das die Einrichtung von den Wettbewerbern abhebt. Aber inwieweit eignet sich hierzu das Thema Datenschutz?

Nutzen Sie Attribute

Es ist von elementarer Bedeutung, für die Positionierung die Eigenschaften zu wählen , die die Einrichtung von den Wettbewerbern abheben und in einem hohen Maße für die Wahl einer Einrichtung relevant sind. So können Attribute wie die Behandlungsqualität, oder der besondere Service ausschlaggebend sein. Auch Ihr Bereich – nämlich ein besonderes Ausmaß des Datenschutzes – kann hier in die Kategorie Service eingeordnet werden.

Praxistipp:

Seien Sie besser als die Wettbewerber und heben Sie sich durch ein besonders hohes Datenschutzlevel ab. Datenschutz ist nichts, das hinter verschlossenen Türen geschehen darf. Sorgen Sie deshalb für ausreichend Transparenz.

Kommunizieren Sie mit der richtigen Zielgruppe

Wichtig bei der Kommunikation der Datenschutzattribute ist die Struktur der Zielgruppe. Jede Kommunikationszielgruppe hat andere Bedürfnisse bezüglich der von Ihnen aufgearbeiteten Informationen. Stellen Sie sich deshalb die Fragen: Welche Informationen benötigt Ihre Zielgruppe, um sich für die Einrichtung zu entscheiden? Und welche Aufgabe erfüllt hier der Datenschutz?

Viele Studien zeigen auf, dass es in erster Linie die Behandlungsqualität, die Reputation der Einrichtung und ebenso die Empfehlungen von Familienangehörigen und Freunden sind, die die Entscheidung von Patienten für oder gegen eine Einrichtung beeinflussen.

Fest steht auch, dass Zusatzangebote wie der Datenschutz für den Patienten nur dann einen positiven Einfluss auf die Patientenentscheidung haben, wenn die Kernleistung, also die medizinische Behandlungsqualität, ausreichend ist.

Praxistipp:

Die Wahl, über welchen Kanal Sie mit Ihren Patienten kommunizieren, kann Einfluss auf die Glaubwürdigkeit Ihrer Informationen haben. Informationen, die auf der Website zur Verfügung gestellt werden, wird in der Regel weniger Vertrauen entgegengebracht.

Ist Ihre Arbeit mehr als nur Hygienefaktor?

Wenn sich ein überragendes, von Ihnen initiiertes Datenschutzniveau also nur als Begleiterscheinung darbietet, wenn der Basisnutzen der Einrichtung stimmt, lässt dies doch schlussfolgern, dass Ihre Arbeit kein Alleinstellungsmerkmal für Ihre Einrichtung bilden kann, oder?

In der Berichterstattung in der Öffentlichkeit erfährt das Thema Datenschutz unter einer Prämisse viel Bedeutung – nämlich dann, wenn es zu einer Datenschutzpanne kommt. Unter dieser Voraussetzung entwickelt sich ein großes Interesse , das gleichzeitig zu erheblichen Reputations- und Imageschäden für die Einrichtung führen kann. Doch warum ist das so? Dies zeigt wieder einmal, dass die Öffentlichkeit und somit auch die einzelnen Patienten davon ausgehen, dass ihre Daten bei den „Vertrauenspersonen des Gesundheitswesens“ in guten Händen sind. Der Datenschutz wird hierdurch, ähnlich wie die Behandlungsqualität einer Einrichtung, somit schnell zu einem Basisnutzen, der erfüllt sein muss, um überhaupt Akzeptanz zu finden. Die Nichtexistenz des Faktors Datenschutz führt zu einer erheblichen Unzufriedenheit.

Praxistipp:

Ihre Arbeit ist unglaublich wichtig. Machen Sie auch in Ihrem Kollegium und der Einrichtungsleitung deshalb deutlich, dass ein niedriges Datenschutzniveau einen erheblichen Schaden verursachen kann. Argumentieren Sie deshalb ruhig mit den negativen Folgen, denn eine mit viel Arbeit und langfristig aufgebaute Unternehmensreputation kann durch einen Fehler schnell zerstört werden. Hinzu kommen natürlich auch noch potenzielle Bußgelder oder Schadenersatzansprüche der Betroffenen, die mit einkalkuliert werden müssen.

Achtung Abmahngefahr

Beachten Sie auch, dass Wettbewerber bei Ihnen die Möglichkeit haben, Datenschutzverstöße abzumahnen. Das kann teuer werden und belastet das Image Ihrer Einrichtung. Umgekehrt steht die Abmahnung auch Ihnen offen. ■

Nina Richard

Datenschutz-Managementsystem

Mit Ihrem individuellen Modulbaukasten zum Datenschutz-Managementsystem, optimal vorbereitet auf die DS-GVO.

Sie buchen nur, was Sie benötigen!

- Modular
- Sie buchen nur die wirklich benötigten Leistungen
- Erfüllen Sie alle gesetzlichen Vorgaben
- Datenschutz als Teil Ihrer Unternehmensphilosophie

Auf Basis der Anforderungen, die sich aus der DS-GVO ergeben, ist es zukünftig verpflichtend, ein Datenschutz-Managementsystem (DSMS) nachzuweisen. Organisatorisch kann dies zu einem komplizierten Großprojekt werden. Mit unserem DSMS schaffen Sie Strukturen, erfüllen gesetzliche Anforderungen und setzen das Thema Datenschutz praxisnah um.

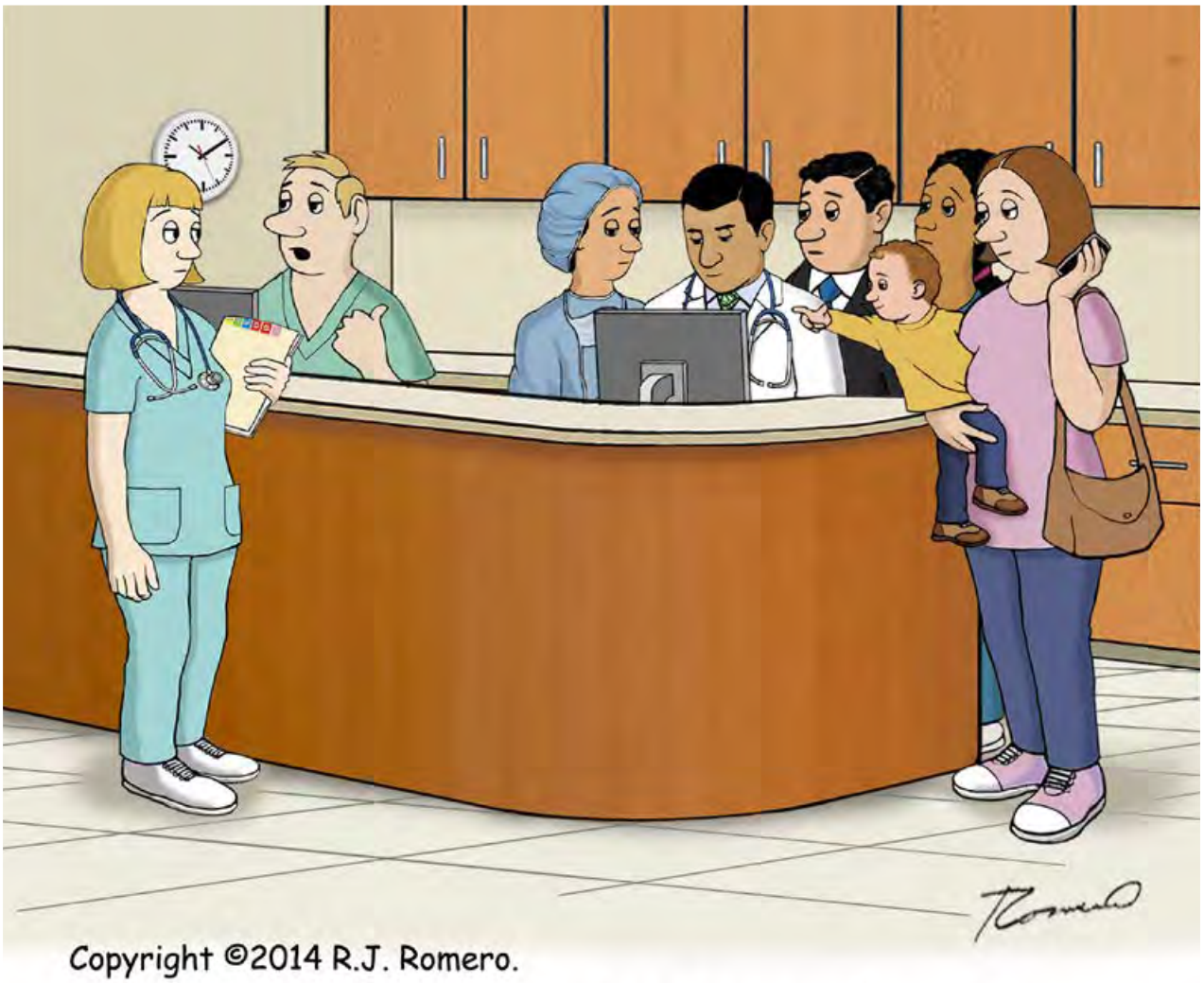
DATATREE
YOUR COMPLIANCE PROVIDER

Datatree AG • Heubesstraße 10 • 40597 Düsseldorf
T +49 211 93190-700 • F +49 211 93190-799 • office@datatree.eu • www.datatree.eu

Impressum

ExperSite Ausgabe 01 2018 | ISSN-Print 2364-5636 | ISSN-Internet 2364-5644 | **Herausgeber:** ISDSG – Ein Dienstleistungsbereich der DATATREE AG Datatree AG, Heubesstraße 10, 40597 Düsseldorf, T +49 211 93190-700, F +49 211 93190-799, office@datatree.eu, www.datatree.eu | **Sitz der Gesellschaft:** Düsseldorf | **Registergericht:** Amtsgericht Düsseldorf | **Registernummer:** HRB 66132 | **Umsatzsteuer-Identifikationsnummer:** DE 279402614 | **Vorstand:** Prof. Dr. Thomas Jäschke | **Vorsitzender des Aufsichtsrates:** Prof. Dr. Julius Reiter | **Inhaltlich Verantwortlicher gemäß § 1 Abs. 4 TMG, § 55 Abs. 1 RStV und § 55 Abs. 2 RStV:** Prof. Dr. Thomas Jäschke | **Redaktionsleitung:** Nina Richard | **Editorial Design u. Umsetzung:** c74 gestaltung & design, C. Robrahn, Dortmund, www.c74.org | **Druck:** Druckerzeugnisse Gerbrunn | **Auflage:** 5.000 | **Fotos:** Titel: shutterstock, Panchenko Vladimir; S. 3: unsplash.com, loic-djim, Falko Wübbecke, Dortmund; shutterstock Pressmaste/kb-photodesign; S. 4/5: F. Wübbecke, Dortmund, B. Sandrock; Stefan Brandau, Henning Mertes; S. 8/9 unsplash.com, loic-djim; S. 10/11: sutterstock, Leonardo da; S. 12: shutterstock, Africa Studio; S.13: unsplash.com, jesus kieque, S. 14: shutterstock, Alexander Raths; S. 15: Sandra Große; S. 16/17: unsplash.com, timon studler, Jürgen Hirsch, Sascha Wiskandt; S. 19: sutterstock, Carmen Murillo; S. 20: shutterstock, wavebreakmedia; S. 22: shutterstock, Rawpixel.com ; U4: hipaacartoons, R. J. Romero.

Einblicke & Ausblicke



"Looks like somebody walked away and left the computer screen logged into the EMR again."

Für die inhaltliche Mitgestaltung möchten wir uns herzlich bei nachfolgenden Gastautoren bedanken:

Rüdiger Karbach, St. Marien-Krankenhaus Siegen gem. GmbH
Sandra Große, Kanzlei HARTMANN Rechtsanwälte
Jürgen Hirsch, CAS AG
Sascha Wiskandt, CAS AG

Die nächste Ausgabe erscheint im September 2018