ISDSG Institut für Sicherheit und Datenschutz im Gesundheitswesen

ExperSite

Das Magazin für Sicherheit und Datenschutz im Gesundheitswesen

Ausgabe 02 2015

Fluch oder Segen?

Die Auftragsdatenverarbeitung

Tipps, Fakten & Termine
Vom eHealth-Gesetz bis zum Buchtipp

ADACOR
ADV aus Sicht eines Managed-Hosting-Dienstleisters

3. Goldene Regel
So erstellen Sie einen ADV-Vertrag

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.

Simon Hacks B. Sc.
Die Betreuung unserer Kunden vor Ort sowie die Unterstützung bei der Umsetzung von operativen Maßnahmen sind das Steckenpferd des Projektmanagers.
✉ hacks@isdsg.de

Alexander Vogel B. Sc.
Mit dem Schwerpunkt der medizinischen Informatik fühlt er sich im Gesundheitswesen ganz zu Hause. Dies zeigt sich in der Konzeptarbeit im Rahmen seiner Beratungstätigkeiten.
✉ vogel@isdsg.de

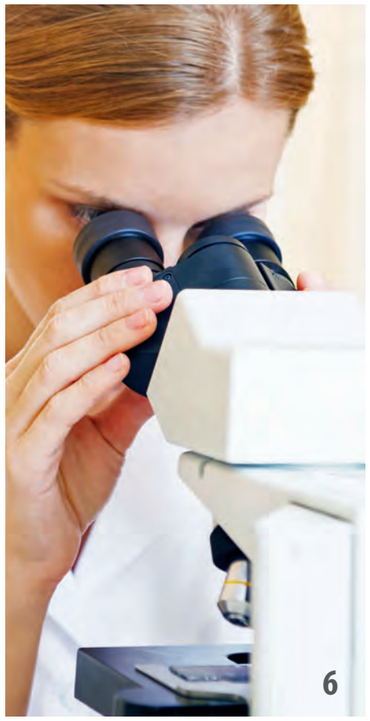
Prof. Dr. Thomas Jäschke
Der Medizin-Wirtschaftsinformatiker ist Experte im Gesundheitssektor und Datenschutzbeauftragter für namhafte Einrichtungen im Gesundheitswesen. Als Institutsleiter ist er der Kopf des ISDSG-Teams.
✉ jaeschke@isdsg.de

Nina Richard B. A.
Sie verantwortet die Bereiche Marketing und Public Relations. Von der strategischen Planung bis hin zur operativen Umsetzung von Kommunikationsmaßnahmen ist sie Ihre Ansprechpartnerin.
✉ richard@isdsg.de

Angelica Morina
Als Verantwortliche für alle Aufgaben in Vertrieb und Kundenmanagement sowie der Steuerung firmeninterner Abläufe ist sie Ihre erste Ansprechpartnerin bei allen aufkommenden Fragen.
✉ morina@isdsg.de

Magnus Welz
Der Projektleiter begleitet Sie direkt vor Ort und koordiniert die umzusetzenden Maßnahmen. Zudem gehört die strategische Ebene der Projektarbeit zu seinen Schwerpunkten.
✉ welz@isdsg.de

Inhalt



ADV oder Funktionsübertragung – wo ist die Grenze?

Die Expertenmeinung zur ADV in der Unternehmenspraxis.

Auch die Vertragsgestaltung hat ihre Tücken.

Das Team 2

Tipps, Fakten & Termine 4

Schwerpunkt

Auftragsdatenverarbeitung – Fluch oder Segen? 6
Über die Schweigepflicht, Unzulässigkeiten und Betroffenenrechte

Gastbeitrag

Herausforderung Datenschutz aus Sicht eines Managed-Hosting-Dienstleisters 10
Verträge mit aussagekräftigen Vereinbarungen zur Auftragsdatenverarbeitung sind ein Muss.

Voice

Interview mit Datenschutz-Auditor Dr. Bernd Schütze 12
Die Notwendigkeit eines Muster-ADV-Vertrags im Gesundheitswesen

Der Datenschutzbeauftragte

Aufgaben des Datenschutzbeauftragten im Rahmen der ADV 14
Es geht nicht ohne Datenschutzbeauftragten

Goldene Regeln

3. Goldene Regel: Gestalten Sie den ADV-Vertrag richtig! 15
Diese Eckpunkte gilt es zu beachten

EDITORIAL

Sehr geehrte Leserinnen und Leser,

die Arbeit in Gesundheitsberufen bringt häufig die Arbeit mit besonders schützenswerten Daten mit sich. Hierzu existiert die ärztliche Schweigepflicht, die zur Wahrung der Geheimnisse zwischen Ärzten und den Patienten gilt. Mithilfe von IT-Systemen wird die Patientenbetreuung effizienter gestaltet.

Häufig wird diese IT-Unterstützung von den Gesundheitseinrichtungen ausgelagert, wenn zum Beispiel extern Laborwerte ausgewertet werden oder die Abrechnung erledigt wird. Und schon befinden wir uns in der Auftragsdatenverarbeitung … oder doch einer Funktionsübertragung?

Die Abgrenzung ist hier gar nicht so leicht. Umso wichtiger ist die Einschätzung des Datenschutzbeauftragten in dieser Situation. Aber mal Hand auf´s Herz – sind Sie als Datenschutzbeauftragter in jede Dienstleistungsauslagerung involviert? Wenn nicht, dann wird es höchste Zeit.

In der aktuellen Ausgabe des Magazins ExperSite dreht sich alles rund um das Thema Auftragsdatenverarbeitung. Von der reinen Abgrenzung von Begrifflichkeiten bis hin zu Praxistipps und Expertenmeinungen ist in dieser Ausgabe einfach alles mit dabei.

Ihr

Prof. Dr. Thomas Jäschke
Institutsleiter ISDSG

Kommentar zum eHealth-Gesetz

Das im Mai 2015 verabschiedete eHealth-Gesetz soll nun die digitale Entwicklung im Gesundheitswesen vorantreiben und trifft dabei explizite Regelungen für Medikationspläne, Notfalldaten und Versichertenstammdaten. Und wie sieht es mit dem Datenschutz und der IT-Sicherheit aus?

Angekündigt wurde die Zusammenarbeit mit unterschiedlichsten Datenschutz- und IT-Sicherheitsstellen. Konkrete Maßnahmen werden allerdings nicht angesprochen – so werden beispielsweise Ärzte und Krankenhäuser in die Pflicht genommen, über geeignete Sicherheitsmaßnahmen zu entscheiden. Das Versprechen der Selbstbestimmung des Patienten wurde bisher nicht erfüllt.

Das Vorantreiben von telematischen Anwendungen im Gesundheitswesen ist grundsätzlich zu befürworten. Probleme wie die gesundheitliche Überwachung einer älter werdenden Gesellschaft oder auch der Ärztemangel in ländlichen Gebieten lassen sich durch die Unterstützung von Telemedizin gut handhaben. Jedoch besteht eHealth aus mehr als nur den drei im Gesetz beschriebenen Anwendungen (Medikationsplan, Notfalldaten, Versichertenstammdatendienst).

Um eHealth-Projekte deutschlandweit zu etablieren, müssen eine Vergütungsstruktur für telemedizinische Leistungen geschaffen und gleichzeitig die Aspekte von Datenschutz und IT-Sicherheit konkretisiert werden. Sonst wird es weiterhin zu Akzeptanzproblemen kommen.

ADV-Vertrag für das Gesundheitswesen

Eine Arbeitsgruppe aus Verbänden und Vereinen, bestehend aus Vertretern von BvD, bvitg, GMDS, GDD, entwickelte einen (Muster-)Vertrag zur Auftragsdatenverarbeitung. Dieser geht als Erster auf die Besonderheiten innerhalb des Gesundheitswesens ein und berücksichtigt zudem individuelle Anforderungen und optionale Ergänzungen.

Als Besonderheiten werden Regelungen zu nachfolgenden Themen gefunden:

- Umgang mit Zurückbehaltungsrecht (§ 273 BGB)
- Schadensersatz und Haftungsfragen
- Informationspflichten
- Wünsche bezüglich einer Zweckänderung durch den Auftragnehmer
- Fragen zu Sozialdaten
- Behandlung der sich aus § 203 StGB ergebenden Fragen sowie des Umgangs hinsichtlich des Beschlagnahmeschutzes
- Umgang mit Datenverarbeitung außerhalb EU/EWR

Mehr dazu auf Seite 15

ResearchKit

Die kürzlich veröffentlichte Open-Source-Softwareanwendung ResearchKit der Firma Apple erlaubt den iPhone-Nutzern, gesundheitsbezogene Daten an Forschungsinstitute weiterzuleiten. Durch die Installation der zugehörigen App können Menschen mit Krankheiten wie Parkinson, Diabetes oder Asthma ihren Krankheitsverlauf aufzeichnen und den Forschern zu Studienzwecken zur Verfügung stellen. Damit soll der Verwaltungsaufwand reduziert und der langwierige Prozess der Teilnehmerakquise verkürzt werden. Kritik gibt es beim Datenschutz, der zwar laut Apple durch die Anonymisierung der Daten gewährleistet sei, jedoch belegen andere Quellen, dass dies nicht im gesamten Übermittlungsprozess der Fall ist.

BUCH

Institutsleiter Prof. Dr. Thomas Jäschke arbeitet aktuell, zusammen mit seinem Team und weiteren Experten aus dem Bereich Datenschutz und IT-Sicherheit, an dem Buch **Datenschutz im Gesundheitswesen**, das voraussichtlich im Februar 2016 erscheinen wird.

Orientierung in grundlegenden Datenschutzfragen

Das Thema Datenschutz ist heutzutage wichtiger denn je. Noch nie war der Allgemeinheit so sehr bewusst, wie begehrt persönliche Daten sind. Die Datensammelwut wird von den Big Playern wie Google und Facebook aus den USA regiert, die bereits eine Fangemeinde in absoluter Abhängigkeit um sich herum geschaffen haben. Dem Gesundheitswesen in Deutschland wird, im Vergleich zu anderen Branchen, häufig nachgesagt, technologisch knapp zehn Jahre im Innovationsrückstand zu sein. Dennoch sind Entwicklungen wie Cloud-Computing, e- und mHealth-Anwendungen auf dem schnellen Vormarsch und versprechen neue Möglichkeiten in der medizinischen Betreuung der Patienten.

Der Ruf nach der Optimierung der Datenschutzorganisation in Bezug auf integrierten Datenschutz wird immer lauter. Dieses Praxishandbuch soll sowohl praktische Lehre als auch die Praktiker im Berufsalltag unterstützen und hier zu einer Orientierung in Bezug auf grundlegende Datenschutzaspekte führen.

Worin die Herausforderungen und Rahmenbedingungen bestehen, welche Strategien, Konzepte und Instrumente sich bewähren, zeigen Praktiker und ausgewiesene Experten auf.

T. Jäschke (Hrsg.), Datenschutz im Gesundheitswesen.
Grundlagen, Konzepte, Umsetzung
Preis: ca. 59,95 €
ISBN: 978-3-95466-221-0

VERANSTALTUNGSTIPPS

nrw.UniTS trifft Medizin
22.09.2015, Düsseldorf

Gesundheitsforen Leipzig – Fachsymposium Datenschutz im Gesundheitswesen
24.09.2015, Leipzig

Update BDSG – Datenschutz im Sozialwesen – Update 2015
06.10.2015, Wiesbaden

Update BDSG – Datenschutz in der Medizin – Update 2015
11.-12.11.2015, Leipzig

Gesundheitsforen Leipzig – 1. Arbeitstreffen der User Group „Datenschutz im Gesundheitswesen“
23. & 24. Februar 2016, Leipzig

Weitere Informationen erhalten Sie unter: www.isdsg.de.

Auftragsdatenverarbeitung – Fluch oder Segen?

Jeder sollte sie machen, jeder sollte wissen wie sie funktioniert und jeder sollte über sie reden – die Auftragsdatenverarbeitung (ADV) für Einrichtungen im Gesundheitswesen ist kein leichtes Unterfangen und sollte doch zu den Disziplinen gehören, mit denen sich die Verantwortlichen in den Unternehmen auseinandersetzen. Alles was Sie über die ADV wissen müssen.

Das Auslagern von einzelnen Dienstleistungen zur optimalen Versorgung der Patienten oder zur Entlastung der Krankenhausorganisation an externe Firmen ist heute für viele Einrichtungen im Gesundheitswesen gang und gäbe.

Seien es Labore, die die Analyse und Auswertung von Untersuchungsergebnissen, oder Firmen, die die Archivierung oder Vernichtung von Patientenakten übernehmen.

Sie alle haben etwas gemeinsam – das Arbeiten mit besonders schützenswerten Patientendaten, die der ärztlichen Schweigepflicht unterliegen.

Warum eigentlich die ADV?

Erst durch die ADV wird es möglich, Aufgaben aus der Organisation auszulagern, bei denen personenbezogene Daten betroffen sind. Der einzige Weg, dies ohne ADV durchzuführen, besteht darin, von den Betroffenen eine Einverständniserklärung einzuholen.

Allerdings muss auch eine Möglichkeit geschaffen werden, die Daten zu verarbeiten, wenn keine Einverständniserklärung vorliegt, da sonst beispielsweise Laboruntersuchungen durch Subunternehmer nicht umsetzbar wären. Dies kann durch die Vereinbarung einer ADV geschehen, da der Auftragnehmer, an den die Datenverarbeitung ausgelagert wird, rechtlich wie eine interne Stelle angesehen wird. Das hat den entscheidenden Vorteil, dass die Außendarstellung des Auftraggebers gegenüber den Betroffenen nicht angepasst werden muss.

ADV oder Funktionsübertragung?

Damit der Auftragnehmer jedoch als interne Stelle gelten kann, hat der Gesetzgeber enge Rahmenbedingungen gesetzt, die auf jeden Fall einzuhalten sind. Werden die gesetzlichen Rahmenbedingungen nicht eingehalten, kann eine Funktionsübertragung angenommen werden. Eine Funktionsübertragung ist insbesondere dann anzunehmen, wenn der Auftragnehmer dem Betroffenen gegenüber als organisatorisch selbstständig auftritt (z. B. Gestaltung des Briefpapiers) oder der Auftragnehmer selbstständig Entscheidungen bei der Verarbeitung der personenbezogenen Daten treffen kann, die nicht durch Arbeitsanweisungen des Auftraggebers abgedeckt werden. Dies ist beispielsweise der Fall, wenn die übertragenen Daten vom Auftragnehmer zu eigenen wirtschaftlichen Zwecken, wie einer Marktanalyse, genutzt werden.

> *Rechtlich betrachtet stellt eine Funktionsübertragung eine unerlaubte Datenübermittlung an Dritte dar.*

Eine klassische Funktionsübertragung stellt das Factoring von Rechnungen dar. Hierbei wird nicht nur die Rechnungslegung ausgelagert, was sich noch als Auftragsdatenverarbeitung abbilden ließe, sondern auch das Risiko an den Factoringnehmer durch den Verkauf der Forderung. Gegenüber dem Endkunden tritt nun nicht mehr der ursprüngliche Vertragspartner als Gläubiger auf, sondern der Factoringnehmer. Dies äußert sich zum einen in der Kommunikation des Factoringnehmers (er wird in der Regel unter eigenem Firmennamen agieren) und zum anderen durch die eigenständige Entscheidungsmöglichkeit, ein Mahnverfahren einzuleiten.

Rechtlich betrachtet stellt eine Funktionsübertragung eine unerlaubte Datenübermittlung an Dritte dar, >

die ordnungs- und strafrechtlich geahndet werden kann.

Problematik Schweigepflicht

Im Gesundheitswesen werden die datenschutzrechtlichen Vorschriften durch die berufliche Schweigepflicht der Ärzte ergänzt. Man spricht in diesem Zusammenhang von der „Zwei-Schranken-Theorie“, die besagt, dass für Patientendaten sowohl die Anforderungen des Datenschutzes als auch die Anforderungen der Schweigepflicht erfüllt sein müssen. Dies hat auch direkte Auswirkungen auf das Konstrukt der Auftragsdatenverarbeitung.

In Industrieunternehmen stellt es mittels des Konzeptes der Auftragsdatenverarbeitung keine Herausforderung dar, die Kundendatenbank auf externen Servern eines Anbieters auszulagern. Bei der Übertragung dieses Szenarios auf ein Krankenhaus werden aus klassischen Kunden Patienten, deren Daten dem Arzt während seiner Tätigkeit anvertraut wurden und somit der ärztlichen Schweigepflicht unterliegen.

Auch ADV rechtlich unzulässig?

Ein Vertrag zur Auftragsdatenverarbeitung kann aber die datenschutzrechtliche Schranke „heben“, die der ärztlichen Schweigepflicht bleibt jedoch „geschlossen“. Hierdurch ist die Verarbeitung durch einen Auftragnehmer nicht zulässig. Dies liegt darin begründet, dass dem Arzt offenbarte Daten nur durch ihn und seine Erfüllungsgehilfen zur Kenntnis genommen werden dürfen. Dem Kreis der Erfüllungsgehilfen werden insbesondere keine Personen hinzugerechnet, die ihre Tätigkeit in einer anderen Gesellschaft

> *Dem Arzt offenbarte Daten dürfen nur durch ihn und seine Erfüllungsgehilfen zur Kenntnis genommen werden.*

ausüben. Dabei ist es unerheblich, ob die Gesellschaften sich in einer Holding- oder Konzernstruktur befinden.

Dies führt unter anderem dazu, dass zum Beispiel die Auslagerung der IT, aber auch anderer Abteilungen, die für ihre Tätigkeit Zugriff auf patientenbezogene Daten haben, in eine Servicegesellschaft aus Sicht der ärztlichen Schweigepflicht (und nicht des Datenschutzes) eigentlich nicht zulässig ist. Die zuständigen Aufsichtsbehörden sind sich dieser Problematik allerdings bewusst und bei Prüfungen dieses

> *Sensible Daten müssen auf Inhaltsebene verschlüsselt werden.*

Sachverhalts in der Regel wohlwollend eingestellt. Diese Problematik setzt sich beim Thema Fernwartung in gleicher Weise fort.

ADV geht doch – Maßnahmen

Es bestehen zwei Möglichkeiten, externe Dienstleister unter Wahrung der ärztlichen Schweigepflicht einzubinden. Die eine besteht darin, dass die Betroffenen den Arzt von seiner Schweigepflicht entbinden. Diese Entbindung darf jedoch nicht generell erfolgen, sondern immer nur anlassbezogen. Außerdem muss in Fällen, in denen ein Patient nicht abgelehnt werden kann und dieser nicht bereit ist, eine Schweigepflichtsentbindung durchzuführen, dafür Sorge getragen werden, dass die Versorgung auch ohne die Entbindung sichergestellt ist.

Kryptografische Maßnahmen

Die zweite Möglichkeit besteht darin, eine unerlaubte Offenbarung gegenüber dem Dienstleister durch geeignete kryptografische Maßnahmen zu verhindern. Das Ausmaß der Verschlüsselung ist dabei abhängig von den Möglichkeiten der Einsichtnahme des Dienstleisters. Hat der Dienstleister prinzipiell Zugriff auf die Datenbank einer Anwendung, in der Daten gespeichert sind, die der ärztlichen Schweigepflicht unterliegen, dann müssen die sensiblen Daten auf Inhaltsebene verschlüsselt werden.

Besteht kein Zugriff auf die Datenbank, kann die unerlaubte Offenbarung möglicherweise auch schon durch eine Verschlüsselung des Dateisystems verhindert werden.

Betroffenenrechte bei ADV

Die Datenschutzgesetzgebung sieht verschiedene Rechte für Betroffene vor, damit diese ihren Anspruch auf informationelle Selbstbestimmung geltend machen können. Dies sind zum einen die Rechte auf Auskunft, Löschung* bzw. Sperrung und Berichtigung und zum anderen Schadenersatz.

Da die Auftragsdatenverarbeitung dazu führt, dass der Auftragnehmer wie eine interne Stelle behandelt wird, müssen die Betroffenen ihre Rechte beim Auftraggeber geltend machen, auch wenn rein technisch gesehen, die Verarbeitung beim Auftragnehmer stattfindet.

Fazit

Die Auftragsdatenverarbeitung stellt ein einfaches Mittel dar, eine Verarbeitung personenbezogener Daten durch Auftragnehmer zu realisieren. Allerdings gilt es, im Gesundheitswesen auch immer die ärztliche Schweigepflicht zu berücksich-

> *Im Gesundheitswesen gilt es auch immer die ärztliche Schweigepflicht zu berücksichtigen.*

tigen. Dies hat zur Folge, dass sensible Daten durch Verschlüsselung vor unerlaubter Offenbarung geschützt werden müssen, wenn diese an externe Dienstleister abgegeben werden. Dabei wird nicht zwischen dritten Unternehmen oder Tochter- bzw. Schwestergesellschaften in einer Konzernstruktur unterschieden. ■

Simon Hacks

*Beachtung der Archivierungs- und Dokumentationspflichten von Ärzten

Die Schweigepflichtsentbindung oder kryptografische Maßnahmen sind zwei Möglichkeiten zur ADV.

Fundstellen zur Auftragsdatenverarbeitung

Bund

- § 11 Bundesdatenschutzgesetz
- § 80 Zehntes Buch Sozialgesetzbuch

Länder

Baden-Württemberg
- § 7 Gesetz zum Schutz personenbezogener Daten
- § 48 Landeskrankenhausgesetz Baden-Württemberg

Bayern
- Art. 6 Bayerisches Datenschutzgesetz
- Art. 27 Abs. 4 Satz 5f Bayerisches Krankenhausgesetz

Berlin
- § 3 Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung
- § 24 Abs. 7 Landeskrankenhausgesetz

Brandenburg
- § 11 Gesetz zum Schutz personenbezogener Daten im Land Brandenburg

Bremen
- § 9 Bremisches Datenschutzgesetz
- § 10 Bremisches Krankenhausdatenschutzgesetz

Hamburg
- § 3 Hamburgisches Datenschutzgesetz
- § 9 Hamburgisches Krankenhausgesetz

Hessen
- § 4 Hessisches Datenschutzgesetz

Mecklenburg-Vorpommern
- § 4 Gesetz zum Schutz des Bürgers bei der Verarbeitung seiner Daten
- § 39 Krankenhausgesetz für das Land Mecklenburg-Vorpommern

Niedersachsen
- § 6 Niedersächsisches Datenschutzgesetz

Nordrhein-Westfalen
- § 11 Datenschutzgesetz Nordrhein-Westfalen
- § 7 Gesetz zum Schutz personenbezogener Daten im Gesundheitswesen

Rheinland-Pfalz
- § 4 Landesdatenschutzgesetz
- § 36 Abs. 9 Landeskrankenhausgesetz

Saarland
- § 5 Saarländisches Gesetz zum Schutz personenbezogener Daten
- § 13 Abs. 7 Saarländisches Krankenhausgesetz

Sachsen
- § 7 Sächsisches Datenschutzgesetz
- § 33 Abs. 10 Sächsisches Krankenhausgesetz

Sachsen-Anhalt
- § 8 Gesetz zum Schutz personenbezogener Daten der Bürger

Schleswig-Holstein
- § 17 Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen

Thüringen
- § 8 Thüringer Datenschutzgesetz
- § 27b Thüringer Krankenhausgesetz

Kirchen
- § 8 Anordnung über den kirchlichen Datenschutz
- § 7 Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern und Rehabilitationskliniken
- § 11 Datenschutzgesetz der Evangelischen Kirche in Deutschland

Herausforderung Datenschutz aus Sicht eines Managed-Hosting-Dienstleisters

Für komplexe Internetseiten und Webapplikationen, die individuelle Unternehmensprozesse und -services abbilden, wie beispielsweise Kundenportale, sind Standard-Hosting-Angebote nicht sinnvoll. Ausfallsicherheit, Performance und Flexibilität kann nur eine Infrastruktur bieten, die exakt auf diese Anforderungen zugeschnitten ist. Das betrifft insbesondere auch die datenschutzsensiblen Bereiche.

Die ADACOR Hosting GmbH entwickelt in enger Abstimmung mit ihren Kunden Hosting-Konzepte. Das Unternehmen garantiert unter anderem führenden Institutionen aus dem Gesundheitswesen oder Unternehmen aus der Energiebranche das Funktionieren der gesamten Infrastruktur. Datenschutz und Datensicherheit sind deshalb längst zum integralen Bestandteil der Dienstleistungen geworden.

Immer mehr Unternehmen und Konzerne lagern die Infrastruktur für ein umfassendes Hosting, also den Betrieb von Softwareanwendungen auf zentralen Servern in externen Serverräumen (z. B. in einem Rechenzentrum), aus oder beziehen diese direkt als Service. Der Trend geht dahin, einen Hosting-Spezialisten zu beauftragen, der alternativ zum klassischen Server-Betrieb im Unternehmen Lösungen und Services mit großer Flexibilität und Skalierbarkeit anbietet.

> *Der Trend geht dahin, einen Hosting-Spezialisten zu beauftragen.*

Damit verbunden ist allerdings auch die Auslagerung von betrieblichen, personen- bzw. kundenbezogenen Daten von dem geschützten Unternehmensraum in öffentlich zugängliche Netze und Systeme. Bei der Wahl des passenden Hosting-Anbieters empfiehlt es sich darauf zu achten, dass dieser selbst Wert auf Datenschutz und -sicherheit legt.

Pflichtaufgabe Auftragsdatenverarbeitungsvereinbarungen

Mit der Auslagerung von Daten auf die Services eines externen Dienstleisters ist oft auch die Übergabe von personenbezogenen Daten verbunden. Wie diese Daten genau zu handhaben sind, regelt eine Vereinbarung zur Auftragsdatenverarbeitung (ADV), deren genauen Inhalte im Bundesdatenschutzgesetz (BDSG) verankert sind. Der Abschluss einer solchen ADV-Vereinbarung ist kein selbstverständliches Unterfangen, wie der kritische Blick auf die Hosting-Branche zeigt. Denn auch wenn sich ein Hosting-Dienstleister komplett um die Infrastruktur kümmert, so ist rechtlich für die Pflege und Kontrolle der datenschutzrelevanten Daten und Prozesse allein der Auftraggeber verantwortlich. Bei Kunden, die ihre Softwareanwendungen selbst entwickeln

> *Verträge mit aussagekräftigen Vereinbarungen zur Auftragsdatenverarbeitung sind ein Muss.*

und betreiben, haben Hosting-Anbieter zudem in der Regel keinen Überblick über die Datenschutzrelevanz der Anwendung. Schon in der Konzeptionsphase für individuelle Hosting-Infrastrukturen muss deshalb fundierte Beratung durch den Hosting- Dienstleister und eine intensive Zusammenarbeit zwischen Auftraggeber und Hoster stattfinden, um rechtlich einwandfrei zu bleiben. Verträge mit aussagekräftigen Vereinbarungen zur Auftragsdatenverarbeitung sind hier ein Muss. Anbieter müssen ihre Kunden auf das rechtliche Spannungsfeld aufmerksam machen und gemeinsam mit ihnen Rahmenbedingungen für den Umgang mit personenbezogenen Daten ausarbeiten. Die so entstehenden Auftragsdatenverarbeitungsvereinbarungen legen dann alle technischen und organisatorischen Maßnahmen wie zum Beispiel Zugriffshierarchien, Back-up-Muster oder Dokumentationsformalien und deren korrekte Handhabung fest.

Praktikables Leitsystem

Das ist ein aufwendiger Prozess – rücken doch einzelne Server oder Projekte in den Fokus, für die es gesonderte ADV-Verträge zu schließen gilt. Außerdem müssen die vereinbarten Prozesse dauerhaft kontrolliert und nachgehalten sowie kontinuierlich an dynamische Projektverläufe angepasst werden.

Ein jährliches Review ist deshalb Mindeststandard. Bereits in der Konzeptionsphase geht einer ADV eine umfassende Analyse der Applikation und der Daten voraus, um im Abgleich mit den gesetzlichen Vorgaben Datencluster, die durch Standardsets abgesichert werden können, und sensible Bereiche, für die besondere Maßnahmen eingeführt werden müssen, zu identifizieren.

Audits und Zertifizierungen

Eine bundesweit geltende behördliche Zertifizierung gibt es zwar nicht, aber die Landesbehörden bieten verschiedene Audit-Möglichkeiten an.

In der Praxis ist es sinnvoll, dass Auftraggeber einen Audit-Katalog erstellen, anhand dessen ein Auditor einer unabhängigen Stelle den Managed-Hosting-Dienstleister prüfen kann. Allgemeine Richtlinien lassen sich auf diese Weise mit individuellen Unternehmensanforderungen kombinieren. Denn diese können sehr unterschiedlich sein: Bundesbehörden, Ärzte, Banken oder Versicherungen unterliegen unterschiedlichen gesetzlichen und regulatorischen Anforderungen. Kirchliche Einrichtungen zum Beispiel von Caritas und Diakonie beanspruchen zusätzlich spezielle kirchenrechtliche Regelungen für sich.

Das Erstellen von Audit-Katalogen zum Datenschutz kann für Unternehmen übrigens weitaus mehr als lästige Pflichterfüllung sein. Denn mit der Analyse der datenschutzrelevanten Bereiche – denkbar sind hier zum Beispiel technische und organisatorische Voraussetzungen für Löschfristen oder Zugriffshierarchien – geht häufig auch eine Optimierung der Geschäftsprozesse einher. Nicht selten

> *Mit der Analyse der datenschutzrelevanten Bereiche geht häufig auch eine Optimierung der Geschäftsprozesse einher.*

werden Schwachstellen im Unternehmen im Rahmen der Analysen früh entdeckt und rechtzeitig beseitigt.

Fazit

Das Fazit von Andreas Bachmann, Geschäftsführer und CIO der ADACOR, hinsichtlich des Umgangs mit der rechtlichen Kontroverse von Datenschutz und Datensicherheit fällt schließlich positiv aus: „Viele unserer Kunden müssen das Thema schon deshalb ernst nehmen, weil sie selbst strengen gesetzlichen Vorgaben unterliegen. Aber auch Kunden, die rechtliche Vorgaben flexibler handhaben können, gehen zunehmend sensibler mit dem Themenfeld Datenschutz und -sicherheit um. In der Regel nutzen sie unsere entsprechenden Beratungsangebote umfassend. Denn das Ergebnis sind stimmige und nachhaltige Datenschutzkonzepte, die Gesetzesvorgaben und Datenschutzrichtlinien detailliert berücksichtigen.“ ■

Kiki Radicke

Die Arbeitsweise der ADACOR zum Thema Datenschutz

Die in enger Abstimmung mit den Kundenunternehmen erarbeiteten Anforderungen finden schließlich Eingang in die Betriebshandbücher. Alle verantwortlichen Personen erhalten auf diese Weise ein praktikables Leitsystem zum Datenschutz. Zugriffsrechte, Weisungsbefugnisse oder Prozesse werden so zweifelsfrei definiert. Darauf aufbauend können Kunden selbstverständlich die Umsetzung und Einhaltung der vereinbarten Maßnahmen und der Datenschutzstandards bei der ADACOR auditieren. Hierfür bieten sich verschiedene Wege an: ADACOR gewährt entweder Einsicht in die von unabhängigen Wirtschaftsprüfern erstellten PS-951/ISAE-3402-Prüfberichte ihres dienstleistungsbezogenen internen Kontrollsystems oder Kundenunternehmen beauftragen Auditoren, ihre eigene Revision oder ihren Datenschutzbeauftragten, um die ADACOR im Rahmen eines Vor-Ort-Audits zu prüfen. So können die ADACOR-Kunden nachweisen, dass sie ihrer Sorgfaltspflicht im Umgang mit personenbezogenen Daten und der Auslagerung von deren Verarbeitung nachgekommen sind.

Dr. Bernd Schütze ist Mitglied in verschiedenen Gesellschaften und Berufsverbänden, in denen er auch aktiv in verschiedenen Arbeitsgruppen mitarbeitet. Weiterhin ist er als Datenschutzbeauftragter und -auditor tätig. Derzeit arbeitet Dr. Schütze bei der Deutschen Telekom Healthcare and Security Solutions GmbH (DTHS) im Bereich Datensicherheit und Datenschutz im Gesundheitswesen.

Im Interview mit …

Dr. Bernd Schütze

Warum war es für die Arbeitsgruppe ADV so wichtig, einen Mustervertrag explizit für das Gesundheitswesen zu entwickeln? Kann das Thema ADV nicht branchenübergreifend einheitlich betrachtet werden?
Es stimmt, es gibt von den verschiedensten Institutionen und Organisationen schon Vorlagen für den Abschluss eines ADV-Vertrages. Jedoch geht keine dieser Vorlagen auf die Besonderheiten im Gesundheitswesen ein, was nicht verwundert, da die Vorlagen aus der Industrie (z. B. BITKOM, DateV), von Verbänden (z. B. GDD) oder auch von den Aufsichtsbehörden (z. B. LDI NRW, Hessischer Datenschutzbeauftragter) kommen und tatsächlich branchenübergreifend gelten sollen.

Aber es existieren, bedingt durch die vielfältige Gesetzgebung wie SGB oder spezifische Landesgesetze, nun einmal im Gesundheitswesen spezielle Anforderungen wie beispielsweise beim Umgang mit Sozialdaten oder dem Umgang mit Datenverarbeitung außerhalb EU/EWR (man muss bedenken, dass einige Landesgesetze die Verarbeitung an anderen Orten sehr stark einschränken).

Und natürlich gibt es auch Anforderungen, die zwar sehr speziell sind, aber nicht nur für das Gesundheitswesen gelten. Hier denke ich beispielsweise an den Umgang mit der gesetzlichen Schweigeverpflichtung gemäß § 203 StGB, die nicht nur für Ärzte und Pflegepersonal gilt, sondern auch für Anwälte, Berufspsychologen usw. Es kann nicht erwartet werden, dass diese Themen in einer „allgemeingültigen" Vorlage behandelt werden. Da wir hier Handlungsbedarf sowohl seitens in Arztpraxis und Krankenhäusern beschäftigten Datenschützern als auch vonseiten der Hersteller sahen, erstellten wir die Vorlage.

Welche „typischen" Fehler passieren Ihrer Meinung nach beim Outsourcing bezüglich ADV?
Zunächst einmal ist es rechtlich im Gesundheitswesen nicht gestattet alles, was man sich vorstellen kann, extern zu beauftragen. In der Regel ist es bei allen Fragen, die mit Patientendaten im weitesten Sinne zu tun haben, nicht statthaft, eine Funktionsübertragung durchzuführen. Das heißt, einerseits muss die Verarbeitung für die Datenverarbeitung beim Auftraggeber bleiben, andererseits muss die Datenverarbeitung nach den (genauen) Vorgaben des Auftraggebers erfolgen. Die Freiheiten zur Auftragserfüllung beim Auftragnehmer müssen deutlich eingeschränkt sein. Im Prinzip ist nur eine Auftragsdatenverarbeitung statthaft, wenn es um die externe Verarbeitung von Patientendaten geht.

Verlagert beispielsweise ein Konzernverbund mit x Krankenhäusern die vollständige EDV-Betreuung in ein Tochterunternehmen „EDV-Dienstleister GmbH" und beauftragt die Tochter mit „erledige irgendwie den 1st- und 2nd-Level-Support bezüglich des Krankenhausinformationssystems", so kann dies rechtlich unzulässig sein. Auch in diesem Fall muss festgelegt sein, was wann, wo, von wem, unter welchem Umständen und wie zu erledigen ist: Der Auftraggeber muss genau definieren, was der Auftragnehmer zu erbringen hat. Ansonsten ist es eine Funktionsübertragung. Und natürlich muss bei einer Auftragsdatenverarbeitung ein ADV-Vertrag abgeschlossen werden.

Ist das Thema ADV in der Praxis überhaupt gängig oder wird es vielerorts vernachlässigt?
Theoretisch muss ein ADV-Vertrag für jede Wartung oder Fernwartung abgeschlossen werden, da der Gesetzgeber dies explizit als Auftragsdatenverarbeitung definiert. Dies betrifft nicht nur die klassische IT wie KIS oder PACS, sondern auch Medizingeräte wie MRT oder CT, aber ebenso nichtmedizinische Anlagen, die per Wartung oder Fernwartung betreut werden. Klassisches Beispiel hierfür ist eine Telefonanlage, die vermutlich jeder Gesundheitsdienstleistungsanbieter einsetzt, aber von einer Fremdfirma betreuen lässt.

Eine kleine Arztpraxis (ein Arzt, zwei Arzthelferinnen) kommt so schnell auf eine relativ hohe Anzahl von ADV-Verträgen: Telefonanlage, Heizungsanlage, Computer-Hardware, Arztpraxissystem, Ultraschallgerät, EKG-Gerät, Point-of-Care-Testing-Geräte usw.

Dies ist organisatorisch kaum zu bewältigen. Ähnlich sieht es im Krankenhausumfeld aus, das zwar eine entsprechende Verwaltung hat, aber natürlich auch ein Vielfaches an Herstellern und Lieferanten, mit denen entsprechende Verträge geschlossen werden müssen.

Da hier seitens der Aufsichtsbehörden kaum Prüfungen stattfinden und dementsprechend nur sehr selten Bußgelder verhängt werden, ist das Interesse, sich mit dieser Thematik zu beschäftigen begrenzt. Das heißt, man versucht zu identifizieren, wo im Sinne des Schutzes des Patientengeheimnisses auch aus Sicht des Gesundheitsdienstleisters ein ADV-Vertrag zwingend notwendig ist (z. B. KIS-Wartung), verzichtet jedoch aus Gründen der Handhabbarkeit an anderer Stelle auf entsprechende Verträge.

Welche Folgen kann eine unvollständige bzw. fehlende ADV für die Vertragspartner haben?
Verantwortlich für die Datenverarbeitung ist der Auftraggeber. Den Auftragnehmer trifft hier ggfs. eine Mitschuld (z. B. entsprechend § 242 BGB), aber der Auftragnehmer wird bei Entgegennahme der Daten ohne ADV-Vertrag vermutlich selbst zur verantwortlichen Stelle. Das heißt, der Auftragnehmer ist für alle Rechtsverstöße verantwortlich, die unter seiner Aufsicht passieren, wie beispielsweise eine unlegitimierte Weitergabe der Daten an Sub-Auftragnehmer.

Was kann den Auftraggeber nun erwarten?
Wenn rechtlich gesehen keine ADV durchgeführt wird (also eine „unvollständige" ADV z. B. mit fehlendem ADV-Vertrag), so fehlt der Datenweitergabe die rechtliche Legitimation. Damit werden mehrere Tatbestände entsprechend § 43 Abs. 2 BDSG erfüllt, das heißt, ich begehe eine bußgeldwehrte Ordnungswidrigkeit. Erfülle ich die Tatbestände des § 44 Abs. 1 BDSG, so wird eine Straftat begangen, die mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft werden kann.

Da der Datenschutzbeauftragte in der Regel die verantwortliche Stelle auf die Notwendigkeit des Abschlusses eines ADV-Vertrages bei der Vergabe einer Auftragsdatenverarbeitung hinwies, kann das Fehlen eines ADV-Vertrages ggfs. auf Vorsatz der verantwortlichen Stelle hindeuten, was den Straftatbestand erfüllt. Es kann also ein Bußgeld bis zu 300.000 Euro oder höher drohen, bzw. eine zweijährige Haftstrafe. ■

Interview: Nina Richard

Aufgaben des Datenschutzbeauftragten im Rahmen der ADV

Der Datenschutzbeauftragte (DSB) sollte das zentrale Bindeglied zwischen dem Auftragnehmer und dem Auftraggeber sein. In der Praxis wird er aber häufig übergangen.

Das Auslagern von Dienstleistungen und somit das von Daten gehört in der Unternehmenspraxis oft zu einer optimalen und wirtschaftlichen Ressourcennutzung. Leider passiert es aber häufig, dass dies zu einer Art der Datenverarbeitung führt, bei der personenbezogene Daten genutzt und verarbeitet werden und das, ohne den Datenschutzbeauftragten mit einzubeziehen. Einen besonders bitteren Beigeschmack bekommt das Thema dann, wenn dabei kein Vertrag zur Auftragsdatenverarbeitung abgeschlossen wird. Verhindert wird dieses Szenario am besten durch das direkte Einbinden des Datenschutzbeauftragten in den gesamten Outsourcing-Prozess, damit dieser so seine Aufgaben erfüllen kann.

Aufgaben des DSB

Zu den Aufgaben des DSB gehört es, bereits zu Beginn des Prozesses aufkommende Datenschutzfragen zu klären, beispielsweise ob überhaupt personenbezogene Daten verarbeitet werden und ob eine Auftragsdatenverarbeitung vorliegt und so auch eine Funktionsübertragung ausgeschlossen werden kann. Vor dem Beginn des Outsourcens unterstützt der Datenschutzbeauftragte mit seinem Know-how die jeweiligen Fachabteilungen bei der Klärung der Frage, ob der Dienstleister aus Datenschutzsicht geeignet ist. Außerdem sollte er bei der Erstellung eines Vertrages zur Auftragsdatenverarbeitung einbezogen werden.

Stetige Pflicht

Da der Auftraggeber bei einer Auftragsdatenverarbeitung die Pflicht hat, die technischen und organisatorischen Maßnahmen bei dem Auftragnehmer zu kontrollieren, sollte der Datenschutzbeauftragte diese im Namen des Auftraggebers durch Begehungen vor Ort und Begutachtung der Prozesse vor Abschluss des Vertrages überprüfen. Auch nach dem Abschluss und der Umsetzung des Outsourcings kann der Datenschutzbeauftragte noch als beratendes Organ tätig sein. So ist er beispielsweise bei einer möglichen Anpassung des Vertrages einzubinden oder stellt durch regelmäßige Kontrollen, die bei Prozessänderungen notwendig werden, die Einhaltung der technischen und organisatorischen Maßnahmen sicher.

Fachkundige Hilfe

Der Datenschutzbeauftragte übernimmt bei dem Prozess des Outsourcings eine fachkundige Vermittlerfunktion. So nimmt er den beteiligten Fachabteilungen Aufgaben wie die datenschutzkonforme Erstellung eines Vertrages zur Auftragsdatenverarbeitung ab oder überprüft die potenziellen Auftragnehmer hinsichtlich ihres datenschutzkonformen Umgangs mit personenbezogenen Daten.

Fazit

Viele Fachabteilungen und Unternehmen wissen nicht über die unterstützende Funktion des Datenschutzbeauftragten bei einer geplanten Auslagerung von Dienstleistungen Bescheid, wodurch es bei der Durchführung zu Problemen mit dem Datenschutz kommen kann. Grundsätzlich sollte der Datenschutzbeauftragte lieber einmal zuviel als einmal zu wenig in den Outsourcing-Prozess einbezogen werden. ■

Alexander Vogel

ADV-Verträge sollten nicht ohne den Datenschutzbeauftragten abgeschlossen werden.

Der Weg zum datenschutzkonformen ADV-Vertrag. So geht´s richtig.

3. Goldene Regel: Gestalten Sie den ADV-Vertrag richtig!

Bei der Gestaltung eines datenschutzkonformen ADV-Vertrages gibt es einige Punkte zu berücksichtigen. Für Sie haben wir das Wichtigste auf einen Blick zusammengestellt.

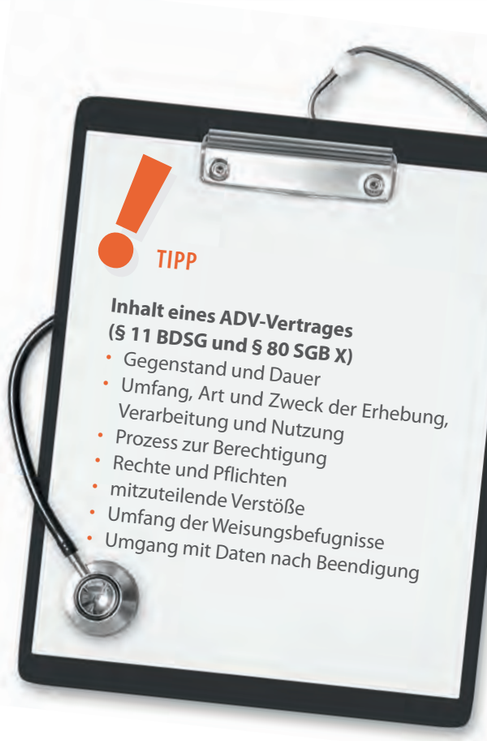
Vor Beginn der Auftragsdatenverarbeitung durch einen externen Dienstleister sollten sich Verantwortliche die Frage stellen: Wie gestalte ich den Vertrag zur Auftragsdatenverarbeitung datenschutzkonform?

Der Vertrag zur Auftragsdatenverarbeitung regelt das Vertragsverhältnis zwischen dem Auftraggeber und dem Auftragnehmer sowie die Rechte und Pflichten beider Vertragsparteien. Weiterhin sind die genauen Dienstleistungen, die der Auftragnehmer zu leisten hat, und der Erfüllungsort zu definieren. Wichtig ist die Benennung der verarbeiteten Daten im Vertrag.

Ein weiterer Punkt, der häufig nicht oder nur unzureichend definiert wird, ist die Einbindung von Unterauftragnehmern. Unterauftragnehmer helfen dem eigentlichen Auftragnehmer bei der Erfüllung der Dienstleistung. Setzt der Auftragnehmer Unterauftragnehmer ein und ist dieses unvermeidbar, sind vor der Vertragsunterzeichnung alle Unterauftragnehmer sowie die zu erbringenden Dienstleistungen vollständig in der Auftragsdatenverarbeitungsvereinbarung zu erfassen. ■

Alexander Vogel

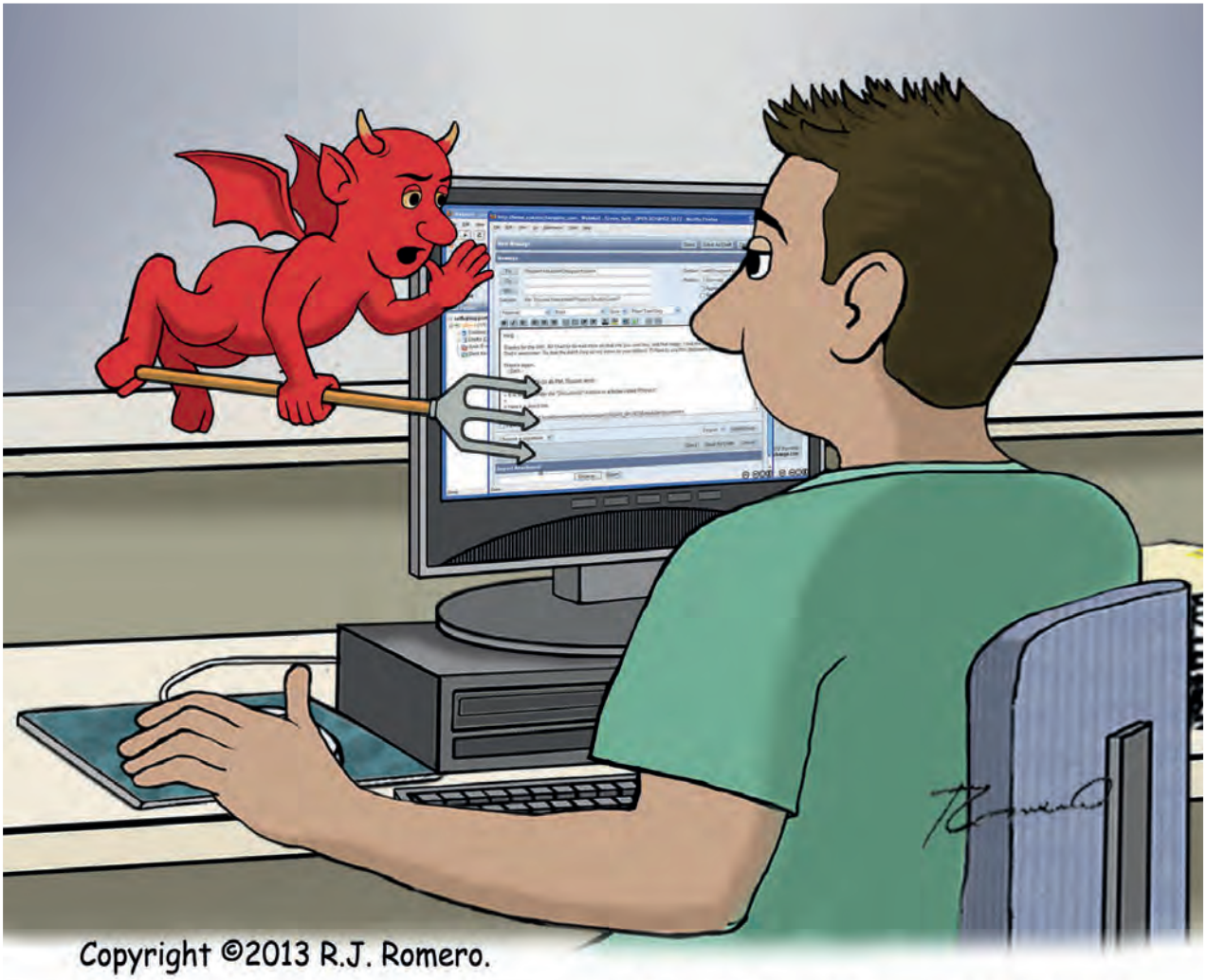
Weitere Informationen erhalten Sie unter: https://www.isdsg.de/muster-adv



Impressum

ExperSite Ausgabe 02 2015 | 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 und Umsetzung:** c74 gestaltung & design, C. Robrahn, Dortmund, www.c74.org | **Druck:** Druckerzeugnisse Gerbrunn | **Auflage:** 5.000 | **Fotos:** Titel: shutterstock, Pressmaster; S. 2: Falko Wübbecke, Dortmund; S. 3: Falko Wübbecke, Dortmund; shutterstock, luckyraccoon ; Fotolia, Andrey Popov, Halfpoint; S. 4: shutterstock, aycatcher; S. 5: T. Jäschke; S. 6.: Fotolia, kasto; S. 8: shutterstock, luckyraccoon; S. 10: iStock, xenotar; S. 12: B. Schütze; Fotolia, Andrey Popov ; S. 14: Fotolia, contrastwerkstatt; S. 15: Fotolia, Halfpoint; shutterstock, John Smith Design ; U4: hipaacartoons, R. J. Romero.

Einblicke & Ausblicke



"Go ahead - email that patient information with no encryption. What could go wrong?"

Wir bedanken uns für die inhaltlichen Beiträge bei:

Dr. Bernd Schütze, Deutsche Telekom Healthcare and Security Solutions GmbH (DTHS)

Kiki Radicke, ADACOR

Die nächste Ausgabe erscheint im März 2016

Im Schwerpunkt: Mitarbeiterdatenschutz