AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

Ausgabe Juli 2016 | Seite 1

www.aok-verlag.info/ds-im-blick

INHALT

Verfahrensverzeichnis

Dr. Sebastian Ertel

Dem Datenschutzbeauftragten ist von der verantwortlichen Stelle eine Übersicht über die meldepflichtigen Verfahren automatisierter Verarbeitungen zur Verfügung zu stellen. Der Beauftragte für den Datenschutz macht diese auf Antrag jedermann in geeigneter Weise verfügbar. So zumindest lautet die gesetzliche Vorstellung (z. B. in § 4g Abs. 2 Bundesdatenschutzgesetz). In der Realität steht dem frisch ernannten Datenschutzbeauftragen bestenfalls die Dokumentation seines Vorgängers zur Verfügung. Schlimmstenfalls existiert noch gar kein Verfahrensverzeichnis.

Verfahrensverzeichnis?

Das Verfahrensverzeichnis, auch Verfahrensregister genannt, hat die Aufgabe, die Verfahren automatisierter (Daten-)Verarbeitungen innerhalb einer verantwortlichen Stelle zu dokumentieren und damit transparent für interne und externe auskunftsersuchende Personen zu machen.
Darüber hinaus ist das Verfahrensverzeichnis ein wichtiges Werkzeug für die Arbeit des Datenschutzbeauftragten. Insbesondere zur Vorbereitung interner Audits, zur Prüfung der Rechtmäßigkeit von Datenverarbeitungsprozessen sowie zur Kontrolle der getroffenen technischen und organisatorischen Maßnahmen zum Schutz der Daten ist das Verfahrensverzeichnis unerlässlich.

„Verfahren automatisierter Verarbeitungen“?

In das Verfahrensverzeichnis gehören alle Verfahren automatisierter Verarbeitungen. Eine genauere Definition findet sich im BDSG allerdings nicht. Allgemein wird von einem Verfahren gesprochen, wenn durch dieses mehrere (automatisierte) Verarbeitungsvorgänge stattfinden, die einem einheitlichen Zweck dienen. Unter diesem - zugegebenermaßen auch nur schwer fassbaren - Begriff ist zunächst jede Software (z. B. zur Zeiterfassung, Finanzbuchhaltung oder Personalverwaltung) einzuordnen, mit der personenbezogene Daten verarbeitet werden.
Häufig stellt sich die Frage, ob Word-Dateien oder insbesondere Excel-Tabellen ebenfalls als Verfahren automatisierter Verarbeitungen gelten. Jedenfalls wenn die einzelne Datei

so komplex ist, dass mit ihr konkrete programmgesteuerte Auswertungen und Selektionen möglich sind, sind diese in das Verfahrensverzeichnis aufzunehmen.
Ein normales Word-Dokument gehört also nicht in das Verfahrensverzeichnis, die Excel-Tabelle der HR-Abteilung, in der Überstunden, Krankheitszeiten, Urlaub und Einsatzpläne mit logischen Verknüpfungen verbunden sind, hingegen schon.

Zwei Versionen des Verfahrensverzeichnisses?

Auch wenn das Gesetz nicht explizit eine Differenzierung erkennen lässt, wird in der Praxis nach internem und öffentlichem Verzeichnis differenziert.
Tatsächlich betrifft die Differenzierung nur die Frage, welche Angaben des Verfahrensverzeichnisses für den internen Gebrauch bestimmt sind und auf welche Informationen eine auskunftsbegehrende Person einen rechtlichen Anspruch hat.
Es gibt somit nur ein gesetzliches Verfahrensverzeichnis. Da das Einsichtsrecht jedoch nicht alle Inhalte des Verzeichnisses erfasst, werden aus Praktikabilitätsgründen zwei Verzeichnisse (bzw. zwei separate Teile) vorgehalten, ein internes und ein öffentliches.

Was muss rein?

Das **„interne“ Verfahrensverzeichnis** umfasst alle in § 4e Satz 1 BDSG genannten Angaben. Hierbei handelt es sich um:

1. Name oder Firma der verantwortlichen Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift der verantwortlichen Stelle,
4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
7. Regelfristen für die Löschung der Daten,
8. eine geplante Datenübermittlung in Drittstaaten,
9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

Das **„öffentliche“ Verfahrensverzeichnis** umfasst nur den Katalog der § 4e Satz 1 Nr. 1 bis 8 BDSG. Die Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung (Nr. 9) sind daher kein Bestandteil dieses Verzeichnisses.

Meldepflichten

Besteht für ein Unternehmen keine Pflicht, einen Datenschutzbeauftragten zu bestellen, muss das Verfahren automatisierter (Daten)-Verarbeitungen nach § 4d BDSG vor der Inbetriebnahme bei der Aufsichtsbehörde angemeldet werden. Die hierbei zu meldenden Informationen sind identisch mit den Angaben des „internen“ Verfahrensverzeichnisses. Weitere Meldepflichten können sich aus Spezialgesetzen ergeben. Die Datenschutzverordnung der Nordelbischen Kirche sieht beispielsweise vor, dass das Verfahrensverzeichnis dem Datenschutzbeauftragten der Nordelbischen Ev.-Luth. Kirche auf Anforderung zu übermitteln ist.

Alles ganz einfach?

Wie immer steckt auch hier der Teufel im Detail. Bei zwei Punkten (Nr. 6 und 7) sollte besonders sorgfältig gearbeitet werden.

- **Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können**
  Oftmals wird verkannt, dass von einer Mitteilung der Daten, nicht von einer Übermittlung oder Weitergabe gesprochen wird. Die Mitteilung geht weiter als die Weitergabe oder Übermittlung. Daher sind unter diesem Punkt sehr ausführliche Angaben zu machen. Diese umfassen sämtliche Personengruppen, die Daten planmäßig erhalten. Hierzu gehören sowohl interne und externe Bereiche oder Abteilungen als auch Auftragsdatenverarbeiter.

- **Regelfristen für die Löschung der Daten**
  Häufig finden sich in Verfahrensverzeichnissen Formulierungen, wie: „Es existieren verschiedene Aufbewahrungspflichten und -fristen. Nach Ablauf dieser Fristen werden die entsprechenden Daten gelöscht, wenn deren Kenntnis nicht mehr erforderlich ist.“ Diese Formulierung wird von den Aufsichtsbehörden grundsätzlich akzeptiert. Der Datenschutzbeauftragte sollte auf

jeden Fall die genauen Fristen für das einzelne Datum und die dazugehörenden gesetzlichen Rechtsgrundlagen kennen, um bei entsprechenden Nachfragen Auskunft geben zu können. Diese Informationen sollten idealerweise in die interne Dokumentation (siehe unten) aufgenommen werden, damit auf sie schnell zurückgegriffen werden kann.

Zusätzliche Informationen

Die gesetzlichen Vorgaben definieren den Mindeststandard an Informationen, die im Verzeichnis vorzuhalten sind bzw. die vom Auskunftsanspruch erfasst werden. Dem Vorhalten zusätzlicher Informationen für den internen Gebrauch steht daher nichts entgegen. Im Gegenteil: Für den Datenschutzbeauftragten bietet es sich sogar an, in einem einheitlich aufgebauten Dokument die Informationen vorzuhalten, die er für seine Arbeit benötigt. Das können sein:

- **Herstellerinformationen**
  Neben der Anschrift des Herstellers dienen die Kontaktdaten des zuständigen Key Account Managers einer schnellen Kontaktaufnahme.
- **Dienstleistungsumfang**
  Häufig wird neben der Anwendung auch ein First-Level-Support zur Verfügung gestellt. Relevant wäre hierbei die konkrete Umsetzung, z. B. telefonische Beratung oder Remote-Zugriff. Bei Letzterem sollten die genauen Voraussetzungen, unter denen sich der Dienstleiter aufschalten kann, festgehalten werden.
- **Auftragsdatenverarbeitung**
  Sofern die Dienstleistung zumindest teilweise als Auftragsdatenverarbeitung ausgestaltet ist, sollte dokumentiert werden, wer innerhalb der verantwortlichen Stelle für die Aufbewahrung der Verträge verantwortlich ist, wann die juristische Prüfung des Vertrages und die letzte Prüfung der getroffenen technisch-organisatorischen Maßnahmen erfolgten sowie das Ergebnis der Prüfung. Darüber hinaus sollte erfasst werden, ob der Dienstleister Subunternehmer eingeschaltet hat, um wen es sich handelt und welche Ergebnisse die Überprüfung dieser durch den Dienstleister hatten.
- **Administration**
  Nicht immer erfolgt die Administration eines Verfahrens durch Mitarbeiter der IT-Abteilung. Zunehmend fallen technische Administration (IT-Abteilung) und inhaltliche Administration (einsetzende Fachabteilung) auseinander. Für die Überprüfung des datenschutzkonformen Einsatzes (Berechtigungskonzept, freigeschaltete Datenfelder, Zugriffskontrollen) sollten die jeweils zuständigen Personen mit Kontaktdaten erfasst sein.

Einsichtnahme

Grundsätzlich hat jeder einen gesetzlichen Anspruch, das „öffentliche“ Verfahrensverzeichnis einzusehen – auch ohne ein berechtigtes Interesse nachweisen zu müssen. Nur in einigen spezialgesetzlichen Regelungen finden sich Ausnahmen von diesem Grundsatz. Nach § 3a Abs. 4 S. 2 der Anordnung über

Muster Verfahrensverzeichnis

- **Allgemeiner Teil (öffentlich)**
  1. Name/Firma, Kontaktdaten und Anschrift der verantwortlichen Stelle
  2. Name der gesetzlich oder nach der Verfassung des Unternehmens berufenen Leitung der verantwortlichen Stelle, des Leiters der IT-Abteilung und des Datenschutzbeauftragten

- **Verfahrensbeschreibung (öffentlich)**
  1. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung
  2. Beschreibung der betroffenen Personengruppen und der Daten oder Datenkategorien
  3. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können
  4. Regelfristen für die Löschung der Daten
  5. eine geplante Datenübermittlung in Drittstaaten

- **Zusätzliche Informationen**
  1. Beschreibung der getroffenen technisch-organisatorischen Maßnahmen
  2. Herstellerinformationen
  3. detaillierte Beschreibung des Dienstleistungsumfangs
  4. Auftragsdatenverarbeitung
  5. Administration des Verfahren

den kirchlichen Datenschutz (KDO) in Diözesen steht das Einsichtnahmerecht unter dem Vorbehalt, ein berechtigtes Interesse nachzuweisen. Gelingt dies nicht, ist das Einsichtnahmebegehren zu versagen.
Bei der Umsetzung der Einsichtnahme lässt der Gesetzgeber der verantwortlichen Stelle freie Hand. Von der Übersendung (per E-Mail oder Post) über die permanente Bereitstellung auf der Unternehmenswebseite bis zur Beschränkung der Einsichtnahme auf die Geschäftsräume der verantwortlichen Stelle ist alles möglich.
Bei einer permanenten Veröffentlichung im Internet ist zu bedenken, dass das Verfahrensverzeichnis tatsächlich von jedem abgerufen werden kann, ohne dass die verantwortliche Stelle von den abrufenden Personen Kenntnis nimmt. Zeichnet sich dieses durch seinen Detailgrad aus, müssen Änderungen in den Datenverarbeitungen unverzüglich umgesetzt werden, damit das Verzeichnis auf dem aktuellen Stand und die verantwortliche Stelle nicht angreifbar ist. Bei einer Übersendung des Verfahrensverzeichnisses, insbesondere per E-Mail, bleibt die Identität des Anfragenden wiederum meist ungeklärt. Ebenso der Grund für das Abrufen des Verfahrensverzeichnisses. Zwar bedarf es, wie bereits dargestellt, grundsätzlich keines berechtigten Interesses oder Grundes. Tatsächlich wird aber niemand ohne Grund das Verzeichnis anfordern. Überwiegend erfolgen entsprechende Anfragen, weil Daten des Anfragenden durch die verantwortliche Stelle erhoben, verarbeitet oder genutzt wurden (und der Betroffene hierbei einen Datenschutzverstoß vermutet, den er aufklären will). Gelegentlich nutzen die Vertriebsmitarbeiter von softwareproduzierenden Unternehmen den Rechtsanspruch, um sich über die eingesetzte Software zu informieren und die Chancen für ein Verkaufsgespräch auszuloten.
Etabliert hat sich die Vorgehensweise, dass der Anfragende von der verantwortlichen Stelle eingeladen wird, sich in deren Geschäftsräumen das Verfahrensverzeichnis anzusehen und Notizen zu fertigen.

Welche Sanktionen drohen?

Hält die verantwortliche Stelle kein Verfahrensverzeichnis vor, kann die Aufsichtsbehörde kein Bußgeld verhängen. Allerdings besteht die Möglichkeit, dass die Aufsichtsbehörde die Erstellung eines Verfahrensverzeichnisses anordnen kann. Wird dieser verwaltungsrechtlichen Anordnung nicht Folge geleistet, besteht die Möglichkeit der zwangsweisen Durchsetzung, beispielsweise durch Verhängung eines Zwangsgeldes.
Das Verfahrensverzeichnis ist aber auch das datenschutzrechtliche Aushängeschild eines Unternehmens. Ist dieses veraltet oder nicht existent, spricht der erste Anschein dafür, dass der Datenschutz nicht den erforderlichen Stellenwert hat. Unter Umständen kann hieraus eine umfangreiche Überprüfung sämtlicher Datenverarbeitungsprozesse durch die Aufsichtsbehörde resultieren.

Empfehlen Sie uns weiter!

Mit dem Newsletter „Datenschutz im Blick“ greifen unsere Autoren Themen auf, die Sie über rechtliche und technische Fragen zu Datenschutz und Datensicherheit im Gesundheitswesen informieren. Dieser Service ist und bleibt für Sie kostenlos! Unsere Redaktion freut sich über jeden neuen Leser, denn damit zeigen Sie, dass dieses Angebot auf Interesse stößt. Deshalb eine Bitte: **Empfehlen Sie uns weiter!**

Feedback, Anregungen oder auch **Fragen** können Sie gerne per E-Mail an **fachinfo@aok-verlag.de** übersenden.

Google Analytics und das EuGH-Urteil zu Safe Harbor

Sven Venzke-Caprarese

Ist der Einsatz des Trackingtools noch zulässig?

In unserer Aprilausgabe haben wir Deutschlands Top 10 Klinikwebsites datenschutzrechtlich bewertet und konkrete Tipps zur datenschutzkonformen Gestaltung von Internetauftritten gegeben. Ein Punkt betraf dabei den Einsatz des Trackingtools Google Analytics. Lange Zeit galt, dass sich Websitebetreiber auf den datenschutzkonformen Einsatz von Google Analytics verlassen konnten, sofern sie bestimmte Rahmenbedingungen einhielten. Es existierte sogar eine Orientierungshilfe des Hamburgischen Datenschutzbeauftragen zum beanstandungsfreien Betrieb des Trackingtools. Genau diese Orientierungshilfe wurde von der Aufsichtsbehörde nun aber im Juni dieses Jahres mit Hinweis auf das EuGH-Urteil zu Safe Harbor zurückgezogen. Google Analytics befinde sich derzeit in der Prüfung. Grund genug, sich ebenfalls Gedanken über den Einsatz des Trackingtools zu machen.

Aus der Praxis kaum noch wegzudenken

Auch wenn das Thema Webtracking von vielen Datenschutzbeauftragten nicht gerne gesehen ist, so ist es aus der Praxis kaum noch wegzudenken. Dies gilt auch für das Gesundheitswesen, wie wir in unserer Aprilausgabe gezeigt haben: Acht von zehn untersuchten Krankenhauswebsites nutzen Trackingtools, sechs davon setzen auf Google Analytics.

Webtracking und Auftragsdatenverarbeitung

Eine rechtliche Grundlage für Webtracking findet sich in § 15 Abs. 3 TMG. Demnach dürfen Websitebetreiber zur bedarfsgerechten Gestaltung ihres Internetauftritts Nutzungsprofile unter Verwendung von Pseudonymen erstellen, sofern die Websitebesucher hierüber informiert werden und nicht widersprechen. Führt der Websitebetreiber das Webtracking nach diesen Vorgaben selbst durch, also auf eigenen Webservern, ergeben sich im Grundsatz keine weiteren Probleme. Sofern das Webtracking allerdings von Dritten erbracht wird, stellt sich relativ schnell die Frage, ob hierin eine Auftragsdatenverarbeitung zu sehen ist. Aufsichtsbehörden bejahen diese Frage insbesondere deshalb, weil im Vorfeld des Webtrackings regelmäßig auch IP-Adressen verarbeitet werden.
Google selbst hat sich dieser Haltung angepasst und bietet seit Jahren den Abschluss eines schriftlichen Vertrags zur Auftragsdatenverarbeitung an, der dem deutschen Bundesdatenschutzgesetz entspricht und mit den Aufsichtsbehörden abgestimmt wurde. Dieser Vertrag regelt in Ziffer 4.7, wie Google mit den Daten im Vorfeld des Webtrackings umgeht:
„Kundendaten werden von Google erfasst und gespeichert. Die Speicherung erfolgt nach der IP-Maskierung. Die von Ihnen aktivierte IP-Maskierung erfolgt stets und erfolgt in der Regel auf Servern innerhalb von Mitgliedstaaten der Europäischen Union oder in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum. Google ist an die US Safe Harbor-Grundsätze zum Schutz der Privatsphäre gebunden. Für weitere Informationen über die Safe Harbor-Vereinbarung und Googles Registrierung besuchen Sie bitte die Website des US-Handelsministeriums.“
Noch konkreter wurde an entscheidender Stelle ein Formulierungsvorschlag, den Google für die Datenschutzerklärung zumindest bis ins Jahr 2012 bereitstellte:
„Im Falle der Aktivierung der IP-Anonymisierung auf dieser Webseite, wird Ihre IP-Adresse von Google jedoch innerhalb von Mitgliedstaaten der Europäischen Union oder in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum zuvor gekürzt. Nur in Ausnahmefällen wird die volle IP-Adresse an einen Server von Google in den USA übertragen und dort gekürzt.“

EuGH Entscheidung zu Safe Harbor und Google Analytics

Die USA gilt nach europäischem Datenschutzrecht als unsicheres Drittland. Werden personenbezogene Daten in ein solches Drittland übermittelt bzw. Auftragsdatenverarbeiter in diesem Land eingesetzt, muss vorab u. a. ein angemesse-

nes Datenschutzniveau hergestellt werden. Google berief sich im Hinblick auf Google Analytics insoweit auf eine Safe Harbor Selbstzertifizierung. Seit dem EuGH-Urteil vom 6. Oktober 2015 ist jedoch klar, dass eine Safe Harbor-Zertifizierung nicht geeignet ist, automatisch ein angemessenes Datenschutzniveau zu gewährleisten.
An dieser Stelle ist Googles Trackingtool datenschutzrechtlich angreifbar. Denn wenn Daten über die Verweildauer und die Interaktion mit den Seiten eines deutschen Websitebetreibers nebst ungekürzten IP-Adressen durch einen Auftragsdatenverarbeiter in den USA verarbeitet werden, kann sich die Frage nach der Angemessenheit des Datenschutzniveaus durchaus stellen.
Es ist nicht ausgeschlossen, dass bei einer genauen Betrachtung des Sachverhalts am Ende das Ergebnis steht, dass die bisherige Datenverarbeitung durch Google im Rahmen von Google Analytics seit dem EuGH-Urteil vom 6. Oktober 2015 unzulässig ist und die Rahmenbedingungen der Datenverarbeitung angepasst werden müssen. Vorangehen müsste einem solchen Ergebnis allerdings die Prüfung, ob tatsächlich personenbezogene Daten betroffen sind. Dies wird von den Aufsichtsbehörden (zu Recht) wohl zumindest für das Datum der IP-Adresse bejaht werden, auch wenn diese Frage unter Juristen nach wie vor umstritten ist. Eine eindeutige Klärung dieser Rechtsfrage wird in Kürze durch den EuGH erwartet, der in der Rechtssache C-582/14 genau hierüber zu entscheiden hat.

Welche Lösungen gibt es?

Für Websitebetreiber, die Google Analytics nutzen, wäre eine Zusicherung durch Google, dass die IP-Adressen immer innerhalb der Europäischen Union anonymisiert werden, die einfachste Lösung.
Alternativ könnten Websitebetreiber versuchen, die Datenverarbeitung durch Google mittels einer Einwilligung der Betroffenen zu legitimieren. In diesem Rahmen könnten die im Internet immer häufiger anzutreffenden „Cookie-Banner“ einen weiteren Einsatzbereich erhalten. Die Diskussion, unter welchen Voraussetzungen mit Hilfe dieser „Cookie-Banner“ eine rechtswirksame Einwilligung eingeholt werden kann, muss allerdings erst noch geführt werden: Reicht eine konkludente Einwilligung (Nutzen der Website trotz Wahrnehmung des Banners) oder ist eine ausdrückliche Einwilligung erforderlich? Wie werden die Anforderungen des § 13 Abs. 2 TMG (etwa zur Protokollierung der Einwilligung) umgesetzt?
Die naheliegendste Lösung ist vermutlich, dass Google künftig neben dem bisherigen Vertrag zur Auftragsdatenverarbeitung zusätzlich noch den Abschluss von EU-Standardvertragsklauseln anbieten wird. Nehmen die jeweiligen Websitebetreiber diese Möglichkeit auch wahr und schließen die Verträge ab, dürften sie dann (zumindest vorerst) von einem angemessenen Datenschutzniveau ausgehen.

Fazit

Die Nutzung von Google Analytics begegnet seit der Entscheidung des EuGHs zu Safe Harbor einer ganzen Reihe von Grundsatzfragen. Aufsichtsbehörden scheinen diese zu sehen, sich jedoch noch nicht klar in Bezug auf Google Analytics positioniert zu haben. Die Nutzung von Google Analytics bedeutet für Websitebetreiber in der momentanen Lage daher ein gewisses rechtliches Risiko. Will man sich diesem Risiko nicht aussetzen und dennoch Webtrackingtools nutzen, ist auf Alternativen umzusteigen (etwa Piwik). Websitebetreiber, die bereit sind, das Risiko zu tragen, sollten die weitere Vorgehensweise der Aufsichtsbehörden genau beobachten. Bisher agieren die Aufsichtsbehörden in Bezug auf Google Analytics noch eher zurückhaltend.

Ein Passwort für alle Anwendungen?

Mindestens acht Zeichen lang, einen großen und einen kleinen Buchstaben, ein Sonderzeichen und eine Zahl – das sind die gängigen Vorgaben für ein Passwort. Oftmals muss dieses dann noch regelmäßig, z. B. alle 90 Tage, geändert werden und darf nicht mit den letzten zehn Passwörtern identisch sein. Alle Vorgaben sind technisch erzwungen. Das Aufschreiben des Passwortes ist natürlich verboten. Werden mehrere solcher Passwörter gefordert, stoßen Menschen sehr schnell an ihre Grenzen. Auch Eselsbrücken zum Merken der Passwörter und selbst Passwortkarten helfen mit zunehmender Anzahl von Passwörtern nicht weiter. Könnte ein Passwort für alle Anwendungen an dieser Stelle eine Lösung sein? Unter gewissen Rahmenbedingungen kann diese Frage durchaus bejaht werden. Passwort-Safesoftware basiert im Grunde auf diesem Prinzip: Alle Passwörter werden durch ein Masterpasswort geschützt. Auch Single Sign-on Lösungen erfordern lediglich ein Passwort auf Betriebssystemebene und reichen dieses an dahinterliegende Anwendungen durch. Bei diesen Lösungen muss das Passwort dann allerdings ganz besonders geschützt werden. Zudem erhöhen sich die Gefahren, falls ein Mitarbeiter seinen Rechner verlässt und vergisst, diesen zu sperren. Hier sind daher weitere technische (automatische Sperre nach kurzer Zeit) und organisatorische Maßnahmen (Sensibilisierung der Mitarbeiter über Schulungen und Awareness-Kampagnen) erforderlich. Gefährlich wird es allerdings, wenn sich Mitarbeiter abseits von den dargestellten Lösungen selbst entscheiden, nur noch ein Passwort für alle Anwendungen zu benutzen und dieses Prinzip sowohl auf den privaten als auf den beruflichen Bereich ausdehnen. Wird hier ein privat genutzter Dienst gehackt, könnten Angreifer versuchen, mit dem erbeuteten Passwort auch berufliche Anwendungen zu kompromittieren. Konkret wird in diesem Zusammenhang derzeit über einen vier Jahre alten LinkedIN Hack berichtet, bei dem 117 Millionen Passwörter erbeutet worden sein sollen, die nun zum Verkauf angeboten werden. Zeitgleich wird in den Medien über zahlreiche unbefugte Zugriffe auf berufliche TeamViewer Anwendungen berichtet. Abseits von Single Sign-on Lösungen sollte daher jede Anwendung mit einem unterschiedlichen Passwort geschützt werden.

Nachtrag zur Messenger-Dienst-Thematik

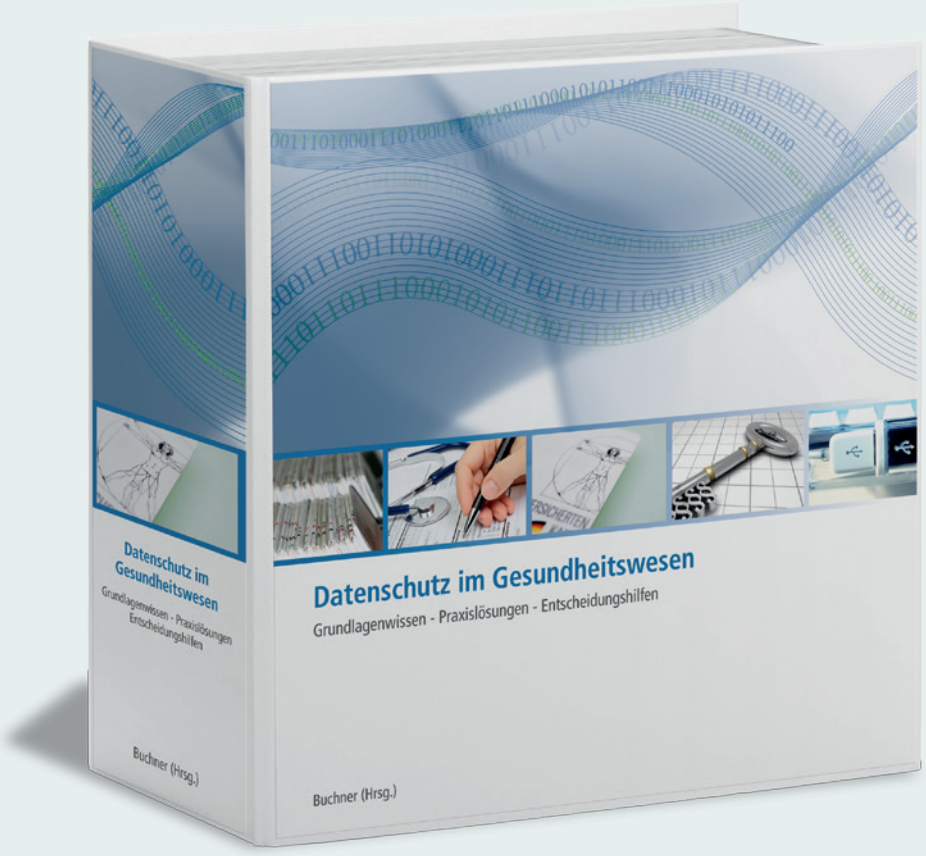
In unserem Juni 2016-Newsletter berichteten wir über den Einsatz von Messenger-Diensten im Gesundheitswesen und konkret den Einsatz von WhatsApp. Im Ergebnis konnte festgestellt werden, dass eine datenschutzkonforme Nutzung unter Beachtung der ärztlichen Schweigepflicht unter bestimmten Voraussetzungen möglich ist. Marit Hansen, schleswig-holsteinische Datenschutzbeauftragte des Unabhängigen Landeszentrums für Datenschutz, hat sich im Rahmen der Frage der rechtlichen Bewertung von Arzneimittel-Vorbestellung per WhatsApp zu der Thematik in einem Interview auf DAZ.Online geäußert.

Insgesamt sieht sie die Nutzung des Messenger-Dienstes sehr kritisch und spricht sich gegen den Einsatz aus, insbesondere weil die Metadaten der Kommunikation (wer hat wann mit wem kommuniziert) nicht von der Verschlüsselung umfasst sind und auch diese Informationen durchaus für Unternehmen interessant seien. So bestehe u. a. die Gefahr, dass sich bereits aus den Kommunikationsbeziehungen der WhatsApp-Nutzer Diagnosedaten ableiten lassen könnten. Das komplette Interview kann unter https://www.deutsche-apotheker-zeitung.de/news/artikel/2016/06/10/whatsapp-wurde-nicht-fur-apotheken-geschaffen abgerufen werden.

gesundheit | versorgung | kommunikation – für diese Begriffe steht die gevko. Mit S3C, unserer IT-Schnittstelle für Versorgungsverträge, vernetzen wir die gesetzlichen Krankenkassen mit den Leistungserbringern, um eine effiziente Abbildung und Abwicklung, u. a. von Selektivverträgen zu ermöglichen. Auf diese Weise sorgen wir dafür, dass die Vertragsinhalte im Praxisalltag ankommen und sowohl Patienten als auch Ärzte von den Vorteilen der Einzelverträge in vollem Umfang profitieren.

gesundheit | versorgung | kommunikation heißt auch unser Newsletter, mit dem wir regelmäßig über Neuigkeiten rund um die Themen S3C-Schnittstelle und IT-gestütztes Versorgungsmanagement informieren. Wir stellen Ihnen aktuelle Projekte und Projektvorhaben der gevko, Neuerungen aus unserer Produktschmiede und deren Anwendungsmöglichkeiten und -vorteile in der Praxis sowie Veranstaltungen und aktuelle Trends und Themen im Gesundheitswesen, in der Softwareindustrie und in der Politik vor.

Interessiert? Dann abonnieren Sie kostenlos unseren Newsletter
gesundheit | versorgung | kommunikation unter http://www.gevko.de/de/newsletter/.



Datenschutz im Gesundheitswesen

Grundlagenwissen – Praxislösungen – Entscheidungshilfen

2 Ordner mit Register im Format DIN A5,
ca. 1.300 Seiten Inhalt
ISBN: 978-3-553-43000-5
Preis 179.- inkl. MwSt.

Uneingeschränkter Online-Zugriff auf alle Arbeitshilfen inkl. 3-4 kostenpflichtige Nachtragslieferungen pro Jahr zum Preis von jeweils 74,90 Euro inkl. MwSt. und versandkostenfreier Zusendung im Inland.