AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

Ausgabe April/Mai 2020 | Seite 1

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

INHALT

SEITE 1
Datenschutz und Telearbeit

SEITE 5
Messenger-Dienste im Gesundheitswesen

SEITE 7
Kurznotiz

Datenschutz und Telearbeit

Viele Unternehmen und Behörden schaffen derzeit mit rasanter Geschwindigkeit Telearbeitsplätze für Beschäftigte, damit diese, nicht zuletzt wegen der Corona-Pandemie, aus dem Homeoffice heraus arbeiten können. Datenschutzrechtlich ist dies bei Beachtung einiger Punkte gut möglich.

Sven Venzke-Caprarese

Grundvoraussetzungen

Bevor eine verantwortliche Stelle Telearbeitsplätze schaffen kann, gibt es ein paar Dinge zu beachten:

Eine Grundvoraussetzung ist natürlich, dass die Tätigkeit an sich für die Telearbeit geeignet ist, also genauso gut auch von zu Hause (Homeoffice) oder von unterwegs (mobile Telearbeit) erbracht werden kann. Dies ist regelmäßig für Büro- und Verwaltungstätigkeiten denkbar..

Darüber hinaus spielt beim Thema Telearbeit aber auch die Sicherheit der Datenverarbeitung eine große Rolle. Es müssen also technische und organisatorische Maßnahmen getroffen werden, um die Telearbeit angemessen abzusichern.

Notebook oder zweite Vollausstattung

Man kann grundsätzlich zwischen zwei Konzepten der Telearbeit unterscheiden:

Stationäre Vollausstattung

Beschäftigte, denen die Teilnahme an der Telearbeit gestattet ist, erhalten bei dieser Variante neben der Ausstattung am regulären Arbeitsplatz darüber hinaus auch eine Vollausstattung am heimischen Arbeitsplatz (z. B. einen zweiten Desktop-PC oder einen zweiten Thin-Client).

Mobiler Client (Notebook)

Alternativ zur ersten Variante kann auch ein Notebook zur Verfügung gestellt werden, welches sowohl am regulären Arbeitsplatz, als auch zu Hause und ggf. sogar unterwegs benutzt werden darf. In der Praxis ist diese Lösung mittlerweile weitaus häufiger vorzufinden, als die stationäre Vollausstattung am heimischen Arbeitsplatz.

Sichere Verbindung mit Transportverschlüsselung

Egal, ob es um das klassische Homeoffice oder um die mobile Telearbeit geht - in beiden Fällen muss gewährleistet werden, dass die Verbindung zu den Daten, E-Mails und Fachverfahren angemessen sicher erfolgt. Eine Transportverschlüsselung ist insofern unumgänglich. Auch hier gibt es unterschiedliche Ansätze:

VPN-Verbindung

Viele Stellen setzen zur Verbindung des Homeoffice-Client mit dem internen Netzwerk auf sogenannte VPN-Verbindungen. VPN steht dabei für Virtual Private Network und dies wird in der Regel so eingesetzt, dass ein transportverschlüsselter Tunnel vom Client des Nutzers ins Netzwerk der verantwortlichen Stelle aufgebaut wird. Dabei ist grundsätzlich unerheblich, wie sicher der verwendete Weg durch das Internet ist. Denn die Daten werden – bildlich gesprochen – von Tunnelwänden geschützt durch das Internet transportiert. Ein Einblick von außen in das Innere des Tunnels ist ausgeschlossen. Grundsätzlich wäre es daher sogar unproblematisch, wenn für die erforderliche Internetverbindung ein öffentlicher Hotspot genutzt werden würde, dessen Sicherheit nicht gewährleistet werden kann.

Terminalserver

Gelegentlich werden in der Praxis auch sog. Terminalserver-Lösungen zur Realisierung der Telearbeit genutzt. Hier wird ebenfalls eine transportverschlüsselte Verbindung hergestellt. Diese erlaubt jedoch keinen direkten Zugriff auf das komplette interne Netz. Stattdessen wird eine Verbindung bis zu einem sog. Terminalserver aufgebaut. Dieser liefert dann grundsätzlich „nur“ noch Bilddaten an den Client, die dieser anzeigt. Auf diese Weise können die Daten dann zwar angezeigt, jedoch nicht auf dem Client selbst gespeichert werden.

VPN-less

Sehr selten kommen in der Praxis sog. VPN-less Lösungen zum Einsatz. Nach diesem Konzept ist gar kein Zugriff auf ein internes Netz mehr vorgesehen, da es dieses so gut wie gar nicht mehr gibt. Die jeweiligen Daten und Fachverfahren werden stattdessen nur noch über Cloud-Anwendungen als Software as a Service (SaaS) bereitgestellt. Die Verbindung erfolgt transportverschlüsselt via https über das Internet zum einzelnen Dienst. Diese Lösung kommt in der Praxis allerdings kaum vollumfänglich zum Einsatz. Häufig finden sich aber einzelne Anwendungen, die direkt über das Internet aufgerufen werden könnten.

Zwei-Faktor-Authentisierung

Egal, welche Lösung verwendet wird, in jedem Fall ist eine Zwei-Faktor-Authentisierung Pflicht.

Verantwortliche Stellen sollten sich daher nicht ausschließlich auf die klassische Authentisierung per Benutzername und Passwort verlassen. Zusätzlich muss ein weiterer Faktor zur Anwendung gebracht werden.

Auch hier gibt es mehrere Lösungen, u. a.:

Zertifikate

In der Praxis werden häufig auf den Geräten gespeicherte Zertifikate verwendet (am besten sog. Personenzertifikate). Nur das Gerät, auf dem sich das Zertifikat befindet, kann im Rahmen der Telearbeit zur Verbindungsaufnahme genutzt werden. Der Besitz des Geräts (Zertifikats) ist daher ein weiterer Faktor neben dem „Wissen“ des Passworts.

One-time Password

Ebenfalls häufig werden sog. One-time Passwords verwendet. Hierbei handelt es sich um ein zeitlich begrenztes, zusätzliches Passwort, welches für den konkreten Login-Vorgang temporär erzeugt wird. Im Grunde ist das Prinzip vergleichbar mit einem

TAN-Generator-Verfahren, welches aus dem Online-Banking bekannt ist.

Das One-time Password kann z. B. an den Besitz einer Telefonnummer geknüpft sein und per SMS übermittelt werden.

Häufig kommen aber auch Authenticator-Apps zur Anwendung. Diese sind in der Regel an den Besitz eines Smartphones geknüpft, auf dem eine App installiert und einmalig synchronisiert wurde.

Verschlüsselung des Clients ist Pflicht

Neben einer sicheren Transportverschlüsselung und einer Zwei-Faktor Authentisierung ist regelmäßig auch die Verschlüsselung der eingesetzten Clients Pflicht.

Sofern im Rahmen der Telearbeit Notebooks zum Einsatz kommen, wäre ansonsten die Gefahr zu groß, dass diese während des regelmäßigen Transports ins Homeoffice oder während der mobilen Arbeit verloren gehen oder gestohlen werden. Jeder Geräteverlust wäre ohne Verschlüsselung des Clients zudem eine meldepflichtige Datenpanne. Um die Daten angemessen sicher zu schützen und gar nicht erst in die Situation zu kommen, melden zu müssen, sollte eine echte Pre-Boot-Vollverschlüsselung der Festplatte verwendet werden. Zudem sollte das Aufheben der Verschlüsselung stets durch die manuelle Eingabe eines Passworts durch den Beschäftigten erfolgen. Andere Lösung, die z.B. unter Einsatz eines sogenannten TPM (Trusted Plattform Module) auch ein selbstständiges Entschlüsseln der verwendeten Notebooks ermöglichen, sollten grundsätzlich nicht genutzt werden, da dieses Verfahren Schwachstellen aufweist (sog. Direct Memory Access Attacken).

Gelegentlich wird in der Praxis von der Verschlüsselung der Clients Abstand genommen, sofern es sich um Thin-Clients handelt, die im Rahmen einer Terminalserver-Verbindung genutzt werden. Als Argument wird vorgebracht, dass sich auf den Clients gar keine Daten befinden können, da nur Bilddaten übertragen werden. Grundsätzlich ist aber auch hier eine Verschlüsselung der Clients empfehlenswert. Sollte darauf verzichtet werden, muss zumindest eine separate Risikoanalyse durchgeführt werden. Diese sollte auch betrachten, ob sich auf den Geräten Authentisierungsfaktoren (Zertifikate) befinden, die geschützt werden müssen. Zudem muss das Szenario betrachtet werden, dass unbefugte Personen kurzzeitig physischen Zugriff auf den Client bekommen und versuchen, unbemerkt Trojaner zu installieren. Schließlich muss die Frage gestellt werden, ob die Speicherung personenbezogener Daten auf dem Client ausgeschlossen werden kann oder ob es möglich ist, dass doch Daten durchgelassen wurden (z. B. im Rahmen von Druckaufträgen) oder Daten auf dem Client selbst durch den Nutzer erstellt wurden (z. B. offline mit Hilfe eines lokal installierten Textprogramms).

Schließlich wird gelegentlich argumentiert, dass Desktop-Rechner, die sich in Homeoffice-Umgebungen befinden, nicht verschlüsselt werden müssten. Grundsätzlich sollten aber auch diese Geräte durch eine Pre-Boot-Vollverschlüsselung gesichert werden, da die Geräte im heimischen Umfeld grundsätzlich erhöhten Risiken ausgesetzt sind (z. B. Wohnungseinbrüchen) und in der Regel im Privatbereich nicht die adäquaten Sicherheitsvorkehrungen getroffen wurden bzw. angenommen werden dürfen (z. B. Alarmanlagen).

Nicht vergessen: Regelung zu Papierunterlagen

Im Rahmen der Telearbeit kommen Maßnahmen zum Schutz von Papierunterlagen oftmals zu kurz.

Die verantwortliche Stelle sollte z. B. den Transport von Papierunterlagen auf ein Mindestmaß beschränken bzw. sogar – wenn mit der Aufgabe vereinbar – komplett untersagen. Denn wo Clients mit Hilfe einer Vollverschlüsselung für den Fall des Verlusts gut geschützt werden können, bestehen hier keine ähnlich wirksamen Möglichkeiten für Papierunterlagen.

Sollten doch einmal Papierunterlagen transportiert oder am Heimarbeitsplatz erstellt (ausgedruckt) werden, kommt dem Thema Vernichtung eine wichtige Rolle zu. Die Beschäftigten sollten entweder mit angemessenen Shreddern für das Homeoffice ausgestattet werden (Sicherheitsstufe 4 nach DIN

66399 sollte regelmäßig ausreichen) oder angewiesen werden, die Unterlagen nur am regulären Arbeitsplatz mit den dort zur Verfügung gestellten Mitteln zu vernichten.

Definierte Ansprechpartner

Besonders wichtig ist es, den Beschäftigen Ansprechpartner zu nennen, an die sie sich im Falle von besonderen Vorkommnissen (Verlust des Notebooks, Verdacht auf Schadsoftware etc.) wenden können bzw. müssen.

Schulung und Sensibilisierung

Beschäftigte sollten zudem regelmäßig auf die besonderen Gefahren der Telearbeit sensibilisiert werden. Hierzu können Schulungen oder sonstige Sensibilisierungsmaßnahmen geplant werden. Es sollte in der Praxis mindestens ein Merkblatt ausgehändigt werden, über das Mitarbeiter sensibilisiert werden und das auch bestimmte Handlungsanweisungen enthalten kann (siehe nächster Punkt).

Konkrete Handlungsanweisungen

Neben den besten technischen Sicherheitsmaßnahmen werden im Rahmen der Telearbeit auch immer organisatorische Maßnahmen erforderlich sein. Hierzu gehört mindestens auch ein Merkblatt, in dem den Beschäftigten konkrete Handlungsanweisungen gegeben werden. Hierzu können z. B. folgende Punkte gehören:

- Hinweis auf die Plicht zur Vertraulichkeit. Je nach Situation insbesondere ein Hinweis, dass weder Familienangehörige, noch Mitbewohner noch Mitreisende Zugriff auf den Client nehmen dürfen.
- Der Umgang, die Aufbewahrung und Vernichtung von Papierunterlagen sollte geregelt werden.
- Auch Telefonsituationen sollten angesprochen werden. Darf das private Festnetztelefon genutzt werden? Oder wird ein dienstliches Telefon gestellt? Unbefugte Mithörer müssen ausgeschlossen und Gesprächssituationen ggf. geplant werden (nicht in der Bahn telefonieren, nicht im Café aber auch nicht auf der Terrasse oder dem Balkon, wenn Nachbarn mithören könnten).
- Der Ort der Telearbeit könnte spezifiziert werden. Ist nur die Arbeit im Homeoffice erlaubt? Oder auch mobile Arbeit an definierten anderen Orten? Darf auch von unterwegs gearbeitet werden? Falls ja, was ist hier zu beachten? Gibt es Orte, an denen keinesfalls gearbeitet werden darf (z. B. im öffentlichen Bus oder der Straßenbahn)?
- Werden Sichtschutzfolien und Notebook-Schlösser zur Verfügung gestellt?
- Darf am Heimarbeitsplatz gedruckt werden?
- Was darf an privater Ausstattung verwendet werden? Mehr als Tastatur, Maus und Monitor?
- Was muss beim Transport des Notebooks beachtet werden (z. B. nicht unnötig transportieren, bestenfalls direkte Wege). Darf das Notebook auch kurzfristig im Auto aufbewahrt werden (z. B. während eines Einkaufs oder Fitness-Studio-Aufenthalts nach der Arbeit). Was ist zu beachten?
- Was ist bei der Verwendung von Hotspots oder Hotelnetzwerken zu beachten? Oder kommt es hier eigentlich auf nichts an, da die Verbindung ohnehin abgesichert ist.

Sicherheitskonzept

Last but not least ist es für Stellen, die ihren Beschäftigten dauerhaft die Möglichkeit der Telearbeit anbieten, empfehlenswert, ein Sicherheitskonzept zu erstellen, in dem u. a. auch die in diesem Beitrag behandelten Themen detailliert dargestellt und ggf. mit festen Prozessen hinterlegt werden.

Messenger-Dienste im Gesundheitswesen

Im privaten Leben kaum noch wegzudenken, erlangen Messenger-Dienste im beruflichen Kontext und auch im Gesundheitswesen zunehmend an Bedeutung. Mal eben ein Konsil in einem komplizierten Fall eingeholt, die Änderung der Medikation eines Patienten kurz abgestimmt oder eine Dienstplanänderung mitgeteilt – was gibt es Einfacheres, als das Smartphone zu zücken und schnell eine Nachricht zu versenden? Aber Vorsicht: Nicht jeder Messenger ist geeignet.

Dr. Sebastian Ertel

Whitepaper der DSK

Am 7.11.2019 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder ein Whitepaper zu den „Technischen Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich“ (https://bit.ly/2vGUyMy) veröffentlicht. In diesem werden 29 Anforderungen formuliert, die ein Messenger-Dienst erfüllen muss oder soll, damit er in einer Gesundheitseinrichtung eingesetzt werden darf.

Wer wie Wahl hat ...

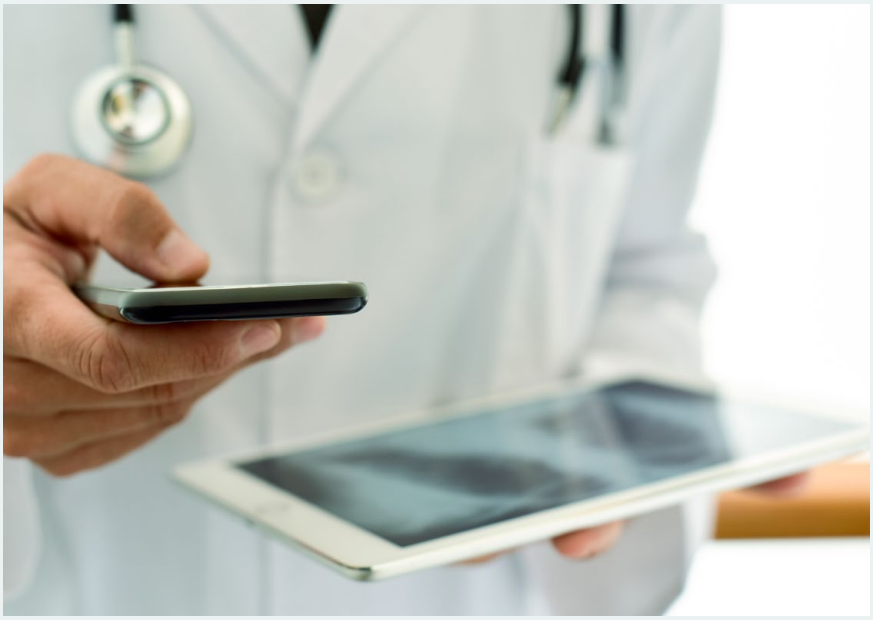
Leider ist es nicht so, dass der Markt im Bereich Messenger übersichtlich ist und nur eine Handvoll Apps bietet. Vielmehr wird eine schier unübersichtliche Auswahl an Messenger-Diensten angeboten, die mal mehr und mal weniger bekannt sind. Und mit jedem neuen Messenger steigt die Unsicherheit. Wir haben uns mit dem Klassiker WhatsApp und den Alternativen Siilo und stashcat intensiv auseinandergesetzt.

Siilo ist ein Messenger-Dienst der niederländischen Siilo Holding B.V. Er ist speziell für das Gesundheitswesen entwickelt und wird von der Arbeitsgruppe der Deutschen Gesellschaft für Kardiologie – Herz- und Kreislaufforschung e. V. genutzt und empfohlen.

stashcat, von der hannoverschen stashcat GmbH, ist unter dem Namen NIMes (steht für Niedersachsen-Messenger) bei der Polizei in Niedersachsen im Einsatz.

Was verlangt das Whitepaper?

Es würde diesen Newsletter sprengen, wenn wir auf alle 29 Punkte eingehen würden. Daher werden an dieser Stelle einige spezielle Punkte dargestellt. Das Fazit berücksichtigt dann wiederum alle 29 Punkte.



Kommunikationspartner

Nach Punkt I.4. des Whitepapers sollte eine Kommunikation über die Messenger-Applikation nur auf der Grundlage einer verlässlichen Identifizierung und Authentifizierung der Kommunikationspartner möglich sein.

WhatsApp bietet zu diesem Punkt keine Lösung.

Siilo bietet ein zweistufiges Verfahren. Auf der ersten Stufe muss die Zugehörigkeit zu einem Beruf aus dem Gesundheitswesen nachgewiesen werden (beispielsweise durch ein Abschlusszeugnis oder die Approbationsurkunde). Wurde diese Hürde genommen, muss mit einem Ausweisdokument die Identität nachgewiesen werden. Nur wenn dies ebenfalls erfolgreich war, erhält der Nutzer Zugriff auf alle registrierten Angehörigen der Gesundheitsberufe.

stashcat ist als geschlossener Einrichtungs-Messenger zu verstehen, d. h. die Einrichtung bestimmt, wer den Messenger nutzen darf. Über das Verzeichniszugriffsprotokoll LDAP kann die einrichtungsbezogene Nutzung über den Verzeichnisdienst Active Directory reglementiert werden. Das bedeutet, dass Mitarbeitende, die die Einrichtung verlassen und im Active Directory gelöscht bzw. deaktiviert werden, automatisch von der weiteren Nutzung von stashcat ausgeschlossen sind.

Fotos

Gerade bei der Einholung eines Konsils erfolgt regelmäßig der Versand eines MRT- oder CT-Bildes. Auf diesem sind eine Vielzahl personenbezogener Daten (z. B. Name, Geburtsdatum) des Patienten abgebildet, die für das Konsil nicht offengelegt werden müssen.

Werden Fotos über WhatsApp erstellt, werden diese automatisch auch in der Foto-App des Smartphones gespeichert. Diese werden dann in der Regel sofort mit dem entsprechenden CloudDienst (z. B. der Apple-Cloud) synchronisiert und auf Servern, die ihren Standort außerhalb der EU/des EWR haben, gespeichert.

Fotos, die mit der Siilo-App erstellt werden, verbleiben im Speicher der App. Eine Synchronisation mit dem „allgemeinen“ Fotoalbum des Smartphones findet nicht statt. Darüber hinaus besteht die Möglichkeit, Passagen auf den Bildern unkenntlich zu machen (sog. Verwischen). Dadurch ist es möglich, nicht erforderliche Informationen aus dem Bild zu entfernen, bevor es an den Empfänger weitergeleitet wird. Die Verwisch-Funktion ist eine Eigenentwicklung. Sub-Dienstleister werden hier nicht eingesetzt.

Auch bei stashcat werden Fotos, die über die App erstellt werden, nicht mit dem Fotoalbum des Smartphones synchronisiert. Eine Verwisch-Funktion wie bei Siilo gibt es allerdings nicht.

Datenlöschung

Insbesondere auf Grund der Sensibilität der Daten kommt der Datenlöschung besonderes Augenmerk zu.

Alle drei getesteten Messenger verfügen über eine Ende-zu-Ende-Verschlüsselung. Bei Siilo wird die Open-Source-Verschlüsselung „NaCl“ genutzt. Die Verschlüsselung, die stashcat nutzt, ist nicht bekannt. Bei WhatsApp ist der Verschlüsselungscode nicht öffentlich verfügbar. Dadurch ist eine Überprüfung der Verschlüsselungsqualität nicht möglich. Wie WhatsApp mit den verschlüsselten Kommunikationsdaten verfährt, ist nicht bekannt. Eine Löschung der Nachrichten ist auf den Endgeräten nur manuell möglich. Wie die Löschung von den Servern erfolgt, ist nicht bekannt.

Bei Siilo fungieren die Server als eine Art Briefkasten. Der Absender verschickt seine Nachricht. Diese wird auf dem Siilo-Server zwischengespeichert. Sobald der Empfänger mit seinem Gerät online ist, erfolgt die Zustellung und damit verbunden, die sofortige Entfernung der Nachricht von den Servern. Die App ist so konfiguriert, dass Nachrichten von der Grundeinstellung her automatisch nach 30 Tagen von den Endgeräten gelöscht werden. Der Nutzer kann diesen Automatismus manuell außer Kraft setzen.

stashcat bietet neben der App auch eine Desktop-Version an. Beide Varianten können parallel genutzt werden. Damit dies möglich ist, verbleibt die Nachricht auf den stashcat-Servern. Eine Datenlöschung ist grundsätzlich nur manuell möglich.

Zugriffsschutz

Alle drei Messenger bieten die Möglichkeit, den Zugriff auf die App mittels PIN-Code sowie Touch- bzw. Face-ID zu schützen. Bei WhatsApp muss dies manuell eingestellt werden. Bei Siilo und stashcat erfolgt die entsprechende Konfiguration im Rahmen der Installation.

Art. 13 Informationen

Siilo und stashcat bieten umfangreiche Informationen zur Datenverarbeitung an. Die Anforderungen an Art. 13 DS-GVO sind erfüllt. Bei WhatsApp sind entsprechende Angaben nicht zu finden.

Auftragsverarbeitung

Über die Webseiten der Anbieter von Siilo und stashcat können Verträge zur Auftragsverarbeitung (in deutscher Sprache) heruntergeladen und abgeschlossen werden. Diese erfüllen die Anforderungen des Art. 28 DS-GVO.

Fazit

Auch wenn WhatsApp der wohl bekannteste Messenger-Dienst ist, es lohnt sich definitiv der Blick nach links und rechts. Gerade im Gesundheitsbereich, wo aufgrund der Sensibilität der Daten erhöhte Anforderungen bestehen, gibt es sehr anwendungsfreundliche Alternativen. Siilo und stashcat gehören dazu. Vor einer Einführung sollte allerdings im Detail geprüft werden, ob der anvisierte Messenger-Dienst für die konkrete Einrichtung tatsächlich passt.

Kurznotiz:

Entwurf für ein Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur.

Um die Digitalisierung im Gesundheitswesen voranzutreiben, hat das Bundesgesundheitsministerium einen Referentenentwurf für ein Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (PDSG) formuliert.

Das PDSG sieht Änderungen in zahlreichen Gesetzen, beispielsweise in den Sozialgesetzbüchern, dem Apothekengesetz und dem Transplantationsgesetz vor. Vor allem seitens der Datenschützer hagelte es Kritik:

- So sei die Rechtsauffassung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur datenschutzrechtlichen Verantwortlichkeit innerhalb der Telematik-Infrastruktur nicht beachtet worden. Die entsprechenden Regelungen seien unklar und stark aufgespalten. Betroffene könnten ihre Datenschutzrechte so kaum adäquat umsetzen.
- Das PDSG bietet die Möglichkeit, Daten für Forschungszwecke zu spenden. Kritisiert wird hierbei, dass die Anforderungen an eine informierte und freiwillige Einwilligung nicht erfüllt seien. Auch sei es nicht vorgesehen, die Datenverarbeitung durch einen Widerruf der Einwilligung zu beenden.

© AOK-Verlag GmbH | Lilienthalstraße 1-3 | 53424 Remagen | Tel 02642 931-333 | Fax 02642 931-215 | Mail fachinfo@aok-verlag.de | Web http://www.aok-verlag.info Herausgeber: AOK-Verlag GmbH, Remagen | Geschäftsführer: Frank Schmidt | Redaktion: Prof. Dr. Benedikt Buchner, Dr. Sebastian Ertel, Sven Venzke-Caprarese | Der Inhalt des vorliegenden Newsletters ist mit größter Sorgfalt zusammengestellt worden. Eine Haftung für die Angaben übernimmt der Verlag jedoch nicht. | Bildnachweise: gettyimages