Newsletter Datenschutz Ausgabe 4 | August 2012

DaSuMed

Datenschutzinfos für medizinische und soziale Einrichtungen

Liebe Kolleginnen und Kollegen,

viele von Ihnen sind aus den Sommerferien zurück und Sie dürfen sich an Ihrem Arbeitsplatz wieder auf den aktuellen Stand bringen. Anhängend finden Sie die neuesten Datenschutzthemen für Ihren Arbeitsbereich.

Mit besten Grüßen, Mark Rüdlin

A. Gesetzesinfos

1. Die Elektronische Gesundheitskarte (eGK) ist verfassungskonform

Das informationelle Selbstbestimmungsrecht wird durch den gesetzlichen Zwang zur Verwendung der eGK nicht verletzt, so die 9. Kammer des Sozialgerichts Düsseldorf (Az. S 9 KR 111/09 v. 28.06.2012). Denn die Pflichtangaben sind identisch mit den Angaben auf der bisherigen Krankenversicherungskarte.

2. Aufbewahrungsfristen verkürzen sich ab 2013

In der Kabinettsitzung der Bundesregierung vom 23.05.2012 hat diese beschlossen, dass ab 2013 die Mindestaufbewahrungsdauer für viele Steuerunterlagen von heute zehn Jahren auf acht reduziert werden sollen. Im Jahre 2015 soll in einem zweiten Schritt eine Verkürzung auf sieben Jahre erfolgen. Diese Änderung findet auch ihren Niederschlag in einer Vereinheitlichung der Vorschriften der Abgabenordnung und des Umsatzsteuergesetzes.

3. Patientenrechtegesetz

Das Patientenrechtegesetz hat den Weg in das Gesetzgebungsverfahren genommen. Kritik kommt von der Datenschutzkonferenz (dem Zusammenschluss der Aufsichtsbehörden des Bundes und der Länder). Sie bemängeln eine zu weit gehende Offenbarungsobliegenheit der Patienten gegenüber den Behandelnden, dass Patienten auch zukünftig nach Behandlungsfehlern fragen müssen und sie nicht erst auf Nachfrage Auskunft bekommen, mangelnde Vorgaben zur Absicherung des Auskunftsrechts und der Archivierung, zu großen Beschränkungen der Einsicht in die Behandlungsdokumentation, fehlende Vorgaben zur Auftragsdatenverarbeitung und wie mit dem vollen oder teilweisen Ausfall des Behandlers bei Auskunftswünschen umzugehen ist.

4. Vorsteuerabzug für per E-Mail-Anhang übermittelte Rechnungen

Einem BMF-Schreiben vom 02.07.2012 ist zu entnehmen, dass § 14 Abs. 1 + 3 UStG durch Artikel 5 Nr. des Steuervereinfachungsgesetzes 2011 bezüglich der Regelung für elektronische Rechnungen mit Wirkung zum 01.07.2012 novelliert wurde. Seit diesem Datum dürfen auch Rechnungen, die beispielsweise im PDF- oder JPEG-Format per E-Mail an den Rechnungsempfänger übermittelt wurden, zum Vorsteuerabzug berücksichtigt werden. Dabei muss die Echtheit der Herkunft, die Unversehrtheit des Inhalts und die Lesbarkeit gewährleistet sein.

B. Urteile

1. Beweisverwertungsverbot nicht legitimierter Videoaufzeichnungen

Wir einem Kündigungsschutzverfahren durch den Arbeitgeber mit belastenden Videoaufzeichnungen der Klägerin begegnet, dann kommt es entscheidend darauf an, ob die Videoaufnahmen datenschutzkonform entstanden. Verstoßen die Aufzeichnungen gegen Datenschutzbestimmungen, sind sie als Beweismittel verboten, so das Bundesarbeitsgericht (Az.: 2 AZR 153/11 v. 21.06.2012).

2. Private Chatprotokolle dürfen zur Begründung einer Kündigung verwendet werden.

Das Landesarbeitsgericht Hamm (LAG) hat in seiner Entscheidung vom 10.07.2012 (Az.: 14 Sa 1711/10) entschieden, dass die Auswertung der Inhalte privater Chatprotokolle rechtmäßig und zur Begründung einer Kündigung tauglich ist. Damit folgt das LAG zwei neueren Urteilen (Landesarbeitsgericht Niedersachsen vom 31.05.2010, Az.: 12 Sa 875/09 + LAG Berlin-Brandenburg vom 16.02.2011 (Az.: 4 Sa 2132/10) zur privaten Nutzung von E-Mails.

C. Sonstiges

1. E-Mail-Versandtechnik

Der Ulmer Akademie für Datenschutz und IT-Sicherheit wurde vor kurzem Verursacher einer Datenschutz-Panne. Mehrere hundert Empfänger waren im E-Mail-Adressfeld offen sichtbar. Dies ist ein Verstoß gegen Datenschutzvorschriften, da auch die E-Mail-Adresse zu den personenbezogenen Daten zu rechnen ist. Soll einfach an viele eine E-Mail versandt werden, dann sollten die Adressen nicht im Feld „An:“ oder „Cc:“ eingetragen, sondern im „Bcc:“ genannten Blind-Copy-Feld. Problematisch dabei ist jedoch, dass solche Mails von den verschieden Empfängern zum Teil als Spam aussortiert werden und diese gar nicht erreichen. Das gilt insbesondere für Empfänger größerer Einrichtungen. Lösung: kleine Mailhilfsprogramme übernehmen die individuelle Versendung von Mails an listenmäßig erfasste Empfänger.

2. Bring-Your-Own-Device (BYOD)

Smartphones und Tablet-PCs haben sich durchgesetzt in sind im Alltag vieler Nutzer angekommen. Viele möchten die Nutzung nicht auf den privaten Bereich beschränken und es kommt zunehmend zu einer Vermischung privater und geschäftlicher Kommunikation. Dabei werden auch Daten der Einrichtungen verwendet und gesendet.

Als Stelle, die personenbezogene Daten verarbeitet (Patienten-, Klienten- und Mitarbeiterdaten) bleibt das Krankenhaus oder der Träger einer sozialen Einrichtung datenschutzrechtlich verantwortlich. Es fehlt jedoch vielfach die Möglichkeit, mit eigenen technischen und organisatorischen Maßnahmen Einfluss auf die privaten Smartphones und Tablets zu nehmen. Daher lautet die klare Empfehlung**: Treffen Sie Regelungen und Absprachen in Bezug auf die berufliche Nutzung privater Smartphones und Tablets.** Themen wie

Haftungsfragen, Gewährleistung des Fernmeldegeheimnisses, Schutz und Sicherung der Patienten- und Mitarbeiterdaten durch ordnungsgemäße Datenverarbeitung und Trennung stehend dabei im Vordergrund. Eine praktische Umsetzung auf den gängigen Smartphone-Plattformen wie iOS (Apples iPhone und iPad), Android von Google, RIM mit seinem BlackBerry oder Windows Phone von Microsoft lässt sich im ersten Schritt durch die Einrichtung mehrerer E-Mail-Konten (privat und geschäftlich) realisieren und die geschäftlichen Accounts können mit dem Exchange-Server (Microsoft) oder Lotus-Domino (Lotus-Notes) verbunden werden. Dabei muss darauf geachtet werden, dass private und geschäftliche Konten nicht durcheinander kommen. Beispielsweise besteht sehr leicht die Gefahr, versehentlich mit dem privaten Account geschäftliche Mails zu versenden. Nicht nur dass dann Firmendaten unkontrolliert quasi ins falsche Netz laufen, entstehen auch eine Reihe von Folgeproblemen, wie beispielsweise die Verletzung der rechtssicheren Firmenarchivierung oder die Übermittlung von geschäftlichen Daten über privat installierte Apps. Daher sollten mit den Beschäftigten vereinbart werden, wer wann in welcher Form auf der Seite des Krankenhauses oder des Trägers sozialer Einrichtungen (Fern-)Zugriff auf die Smartphone-Daten nehmen darf. Das gilt insbesondere für BlackBerrys, die spezielle Software für ihre Geräte verfügbar halten. Denn sonst stellen sich sehr schnell rechtliche Probleme in den Weg, sollte mit verdeckten Datenverarbeitungsmaßnahmen gearbeitet werden. Regelungen zur vollständigen Gerätelöschung im Verlustfall, zur routinemäßigen Löschung nicht mehr benötigter Daten und die obligatorische Verwendung einer PIN vor jeder Nutzung des Geräts (nicht nur zum Einschalten) vervollständigen den Regelungskatalog. Regelung der Haftungsverteilung und Mitteilungspflichten bei Verlust, Vorgaben zur festen Einstellung von Systemparametern, Nutzung des privaten Gerätes durch Dritte und die Durchführung von Reparatur und Wartungsarbeiten sind weitere regelungsbedürftige Punkte.

3. Handlungsempfehlungen des Bundeskriminalamtes für Fälle von Cybercrime

Das Bundeskriminalamt (BKA) hat "Handlungsempfehlungen für die Wirtschaft in Fällen von Cybercrime" herausgegeben. Sie finden die Broschüre unter dem folgenden Link:

http://www.bka.de/nn_238144/SharedDocs/Downloads/DE/ThemenABisZ/InternetKriminalitaet/handlungsempfehlungenWirtschaft,templateId=raw,property=publicationFile.pdf/handlungsempfehlungenWirtschaft.pdf

Datenschutzkenntnisse gut? Testen Sie sich selbst!

Fragestellung: Die Polizei fragt in einer Suchthilfeklinik an, ob M. gestern Abend betrunken ins Haus kam. Welche Auskunft ist gesetzeskonform?

Antwort A: Nein ich gebe aus datenschutzrechtlichen Gründen gar keine Auskunft.

Antwort B: Ja, er war gestern in der Einrichtung. Ob er was getrunken hatte, sollten Sie ihn selbst fragen.

Antwort B: Ja, er kam hier stockbetrunken an.

Lösung: Die Landesmeldegesetze verpflichten stationäre Einrichtungen gegenüber Polizei und Feuerwehr zu Meldeauskünften (Name, Vorname, Geb.Datum, Meldeadresse, Auf- und Entlassdatum) im Falle der Gefahrenabwehr. Die Anwesenheit muss also preisgegeben werden. Darüber hinausgehende Infos (hier: Alkoholisierung) verstoßen gegen die strafbewehrte Schweigepflicht, § 203 StGB.

Impressum: Mark Rüdlin – Rechtsanwalt und Datenschutzbeauftragter
Struenseestr. 37 | 22767 Hamburg | Tel. 040 697972 -80 | Fax -90 | mailto: ra@markruedlin.de