Newsletter Datenschutz Ausgabe 02-2013

DaSuMed

Datenschutzinfos für medizinische und soziale Einrichtungen

Liebe Kolleginnen und Kollegen,

es tut sich weiterhin viel in Sachen Datenschutz. Lesen Sie die neuesten Entwicklungen …

Mit besten Grüßen, Mark Rüdlin

A. Gesetzesinfos

1. IT-Sicherheitsgesetz

Am 05.03.2013 hat das BMI einen Referentenentwurf für ein „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ eingebracht. Neben Verschärfungen einiger Straftatbestände (Computersabotage, Durchführung und Vorbereitung von Ausspähen bzw. Abfangen von Daten, Datenveränderung und Computerbetrug und Änderungen des Telemediengesetzes mit Mindestanforderungen eine Telemediendienstanbieters zur IT-Sicherheit wird das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seiner Rolle gestärkt. In einer Rechtsverordnung sollen die technisch-organisatorischen Maßnahmen, wie im Grundschutz-Katalog des BSI beschrieben, für Betreiber kritischer Infrastrukturen obligatorisch vorgeschrieben werden. Krankenhäuser und soziale Einrichtungen mit Patientendaten gehören zweifellos zu diesen Institutionen. Diese sollen zukünftig alle zwei Jahre ein Sicherheitsaudit durch anerkannte Auditoren durchführen lassen müssen. Und das BSI soll zentrale Meldestelle für Betreiber kritischer Infrastrukturen werden.

2. Direktabrechnung mit privat Versicherten

Seit Anfang des Jahres dürfen Krankenhäuser mit dem Krankenversicherungsunternehmen selbstzahlender Patienten direkt abrechnen, indem sie analog des der § 301 SGB V Datenübermittlung die Abrechnungsdaten elektronisch übertragen, § 17c Abs. 5 Satz 2 KHG. Aber auch hier gilt: Direktabrechnungen nur mit schriftlicher ausdrücklicher Einwilligung des Patienten.

B. Urteile

1. OLG Hamm: Arzt muss Auskunft über Samenspender erteilen

Das OLG Hamm hat in seinem Urteil vom 06.02.2013 (Az.: I-14 U 7/12) entschieden, dass ein durch heterologe Insemination gezeugtes Kind vom behandelnden Arzt Auskunft über seine genetische Abstammung verlangen kann. Damit wird das Interesse des Kindes, seine Abstammung zu erfahren, höher bewertet als das Interessen des Arztes und der Samenspender an einer Geheimhaltung der Spenderdaten.

2. Recht auf Auskunft durch Bundessozialgericht untemauert

Das Bundessozialgericht hat in einem Verfahren verdeutlicht, dass Behörden anfragenden Bürgern umfassend Auskunft geben müssen, welche Daten über sie gespeichert haben und in welcher Form und welchem Umfang diese an Dritte weiter gegeben wurde. Urteil vom 13.11.2012, Az.: B 1 KR 13/12R.

3. VG Schleswig: Facebook darf Registrierung mit echtem Namen verlangen

Facebook darf vorerst weiterhin von seinen Nutzern verlangen, dass sie bei ihrer Registrierung ihre wahren Daten (Vorname, Nachname, E-Mail-Adresse, Geschlecht und Geburtsdatum) angeben. Das Schleswig-Holsteinische Verwaltungsgericht hat mit Beschlüssen vom 14.02.2013 in zwei Verfahren des vorläufigen Rechtsschutzes den entsprechenden Anträgen von Facebook USA und der europäischen Niederlassung Facebook Irland stattgegeben. Das Unabhängige Landeszentrum für Datenschutz (ULD) Schleswig-Holstein habe seine Anordnung zu Unrecht auf das deutsche Datenschutzrecht gestützt, befand das Gericht. Nach Auffassung der Richter ist irisches Recht anwendbar (Az.: 8 B 60/12 und 8 B 61/12).

4. Schadensersatzpflicht bei Löschung des betrieblichen E-Mail-Accounts

Gestattet ein Arbeitgeber die auch private Nutzung des betrieblichen E-Mail-Accounts, dann darf ein Arbeitgeber auch nach Beendigung des Beschäftigungsverhältnisses dieses Konto nicht ungefragt löschen. Wird dagegen verstoßen, kann eine Schadensersatzpflicht daraus resultieren, so das OLG Dresden in seinem Beschluss von 5. September 2012, Az.: 4 W 961/12

➔ Dieses Urteil sollte einmal mehr thematisieren, dass die private Nutzung von E-Mail und Internet in einem Unternehmen nicht einfach hingenommen und toleriert, sondern durch eine Betriebsvereinbarung geregelt werden sollte. Alternativ kommt nur ein völliges Verbot in Betracht.

5. Erste Verhandlung vor Europäischem Gerichtshof zum „Recht auf Vergessen"

Vor dem Europäischen Gerichtshof wurde Google Spain mit dem Ziel verklagt, die amtliche Bekanntmachung über die Zwangsversteigerung eines Hauses auf der Webseite einer spanischen Zeitung nicht mehr zu indizieren. Bejaht der Europäische Gerichtshof dies, dann wird das in der neuen EU-Datenschutz-Grundverordnung angestrebte „Recht auf Vergessen“ schon jetzt Wirklichkeit. EuGH, Rechtssache C-131/12.

C. Sonstiges

1. Datenschutz-Aufsicht Berlin: Verhalten bei Prüfung durch Aufsichtsbehörde

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat in seinen 220 Seiten starken Tätigkeitsbericht auf S. 42 unter Punkt 2.5 für das Jahr 2012 als einen Schwerpunkt beschrieben, wie sich Unternehmen auf Prüfungen durch die Aufsichtsbehörde vorbereiten können und welche Schwerpunkte bei

Prüfungen typischerweise gesetzt werden. Folgende Fehlerquellen werden dabei aufgeführt: Fehlendes oder mangelhaftes Verfahrensverzeichnis; Fehlende oder mangelhafte Verträge über die Auftragsdatenverarbeitung; Fehlende Unabhängigkeit oder Fachkunde der oder des Datenschutzbeauftragten; Fehlendes Lösch- und Sperrkonzept; Missachtung der Auskunftsrechte von Betroffenen; Fehlende oder mangelhafte Verpflichtung auf das Datengeheimnis der Mitarbeiter.

http://www.datenschutz-berlin.de/content/veroeffentlichungen/jahresberichte/bericht-12

2. EU Agentur ENISA warnt vor Cloud Computing in Gesundheitseinrichtungen

Die EU Agentur für Internetsicherheit hat in einem neuen Bericht vor den Gefahren beim Einsatz von Cloud Computing in sensiblen Bereichen, wie Finanz-, Gesundheits- und Versicherungswesen gewarnt.

http://www.enisa.europa.eu/media/neuer-enisa-bericht-uber-staatliche-cloud-computing-sicherheit-in-der-eu

3. Facebook für alle Bundesbürger?

Offenbar plant die Bundesregierung ein staatliches soziales Netzwerk für alle Bundesbürger. Im Gegensatz zu sonstigen sozialen Netzwerken – wie Facebook – werden bei diesem Netzwerk die Daten nicht nur durch die Nutzer eingepflegt, sondern durch den Staat. Die von ihm erhobenen Daten sollen dort abgelegt werden. Damit wird eine Vernetzungsqualität hergestellt, die ihresgleichen sucht.

http://www.heise.de/ct/inhalt/2013/08/142/

4. Bring Your Own Device (BYOD)

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ein IT-Grundschutz-Überblickspapier zum Thema veröffentlicht. Dabei wird ausgeleuchtet, wie die Grenzziehung zwischen beruflicher und privater Nutzung datenschutzkonform gestaltet werden kann.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_BYOD_pdf.pdf?__blob=publicationFile

5. Umgang mit Passwörtern – Umfrage des BSI

Eine Umfrage des BSI ergab, dass der Umgang mit Passwörtern – insbesondere wenn Passwörter für verschiedene Internetdienste genutzt werden – nicht befriedigend ist. Die folgenden Empfehlungen spricht das BSI aus:

- Verwenden Sie nie dasselbe Passwort für mehrere Anwendungen und ändern Sie das Passwort regelmäßig.
- Wählen Sie ein Passwort, das mindestens acht Zeichen lang ist. Es sollte aus Groß- und Kleinbuchstaben in Kombination mit Zahlen und Sonderzeichen bestehen und auf den ersten Blick sinnlos zusammengesetzt sein. (Ausnahme: Bei Verschlüsselungsverfahren wie beispielsweise WPA und WPA2 für WLAN sollte das Passwort mindestens 20 Zeichen lang sein.)
- Tabu sind Namen von Familienmitgliedern, des Haustieres, des besten Freundes, des Lieblingsstars oder deren Geburtsdaten usw. Das Passwort sollte nicht in Wörterbüchern vorkommen. Auch Passwörter, die aus gängigen Varianten und Wiederholungs- oder Tastaturmustern bestehen (z. B. "asdfgh" oder "1234abcd"), sind nicht empfehlenswert. Einfache Ziffern oder Sonderzeichen wie "$" am Anfang oder Ende eines ansonsten simplen Passwortes bieten keinen ausreichenden Schutz.
- Bewahren Sie Ihre Passwörter sicher auf.
- Geben Sie Ihre Passwörter nicht an Dritte weiter.

- Ändern Sie immer bereits voreingestellte Passwörter.
- Nutzen Sie einen Bildschirmschoner mit Passwortabfrage nach einer voreingestellten Wartezeit, wenn der PC angeschaltet ist und nicht genutzt wird.

Die Verwendung eines Passwortverwaltungsprogramm – wie dem kostenfreien und als sicher eingestuften **KeePaas** – kann die Verwendung verschiedener Passwörter für verschiedene Anwendungen stärken.

6. Stiftung Datenschutz

Am 28. Januar hat die Stiftung Datenschutz ihre Arbeit aufgenommen. Aufgabe der Stiftung Datenschutz ist die vergleichende Prüfung von Produkten und Dienstleistungen auf Datenschutzfreundlichkeit, die Förderung der Bildung im Bereich des Datenschutzes und die Verbesserung des Selbstdatenschutzes durch Aufklärung sowie die Entwicklung eines Datenschutzaudits gehören.

Kritik gibt es in Bezug auf den Präsidenten der Stiftung Frederick Richter. Der SPD-Bundestagsabgeordnete Gerold Reichenbach monierte, mit Richter werde „ein eindeutiger Industrievertreter zum Präsidenten gemacht“. Der netzpolitische Sprecher der Grünen, Konstantin von Notz, beklagte die fehlende Erfahrung Richters mit dem Thema Datenschutz. Darüber hinaus äußerte der Grünenpolitiker Bedenken, die Satzung der Stiftung könnte mit der europarechtlich verankerten Unabhängigkeit der Datenschutzaufsicht unvereinbar sein.

7. Cyper Security Risk Report von HP veröffentlicht

Hewlett Packard (HP) hat den HP 2012 Cyber Security Risk Report veröffentlicht. In dem jährlich erscheinenden Bericht werden aktuelle Trends und Entwicklungen in der IT-Sicherheit beleuchtet. Die Zahl der Sicherheitslücken stieg im Vergleich zum Vorjahr 2011, lag aber unter dem Spitzenwert von 2006. Mobile Endgeräte tragen zu vielen Schwachstellen bei. Ein besonderes Problem waren dabei unberechtigte Zugriffe.

http://www.hpenterprisesecurity.com/collateral/whitepaper/HP2012CyberRiskReport_0213.pdf

8. Verlust des firmeneigenen Geräts wird zu spät gemeldet

Eine Umfrage des Virenschutzprogramm-Herstellers Kaspersky ergab, dass nur jeder fünfte Mitarbeiter in kleinen und mittleren Unternehmen seinem Arbeitgeber den Verlust eines firmeneigenen Gerätes meldet, wenn dieser bemerkt wurde. In zwölf Prozent aller Fälle vergeht sogar mehr als ein Tag, bis eine Verlustanzeige erfolgt. Dies stellt ein erhebliches Risiko dar. Cyberkriminelle haben zwischenzeitlich die Möglichkeit vertrauliche Daten auszuspionieren.

http://www.kaspersky.com/de/news?id=207566663

9. Bericht von der BCLT Datenschutz Konferenz in Palo Alto

Am 21. März 2013 fand in Palo Alto die zweite Datenschutz-Konferenz des “Berkeley Center for Law and Technology” BCLT) der Universität Berkeley statt. Ein Schwerpunktthema war „The EU-US Privacy Collision”. Weitere Themen „Privacy and The Price of Free”, „The Management of Privacy Processes: the CPO And Beyond” und „Technology and Privacy Design” rundeten die Veranstaltung ab.

10. Joomla! 1.5

Wer seine Webseite mit dem Content Management System Joomla! in der Version 1.5 oder älter betreibt, sollte diese sehr zeitnah auf die aktuellen Versionen 2.5 oder 3 updaten. Bei den vorgenannten Joomla-Versionen bestehen ernsthafte Sicherheitslücken. Hacker dringen aufgrund von Sicherheitslücken in die betroffenen Joomla-Systeme ein und verursachen zum Teil erhebliche Schäden.

11. WhatsApp mit Datenschutzverstoß

Die kanadischen und niederländischen Aufsichtsbehörden haben einen Datenschutzverstoß des Mobile Messenger Service WhatsApp gerügt. Der Vorwurf lautet, dass auf das gesamte Adressbuch eines Nutzers zugegriffen wird, ohne dabei zwischen Nutzern und Nicht-Nutzern zu unterscheiden. Damit werden auf den Servern von WhatsApp auch Informationen über Dritte gespeichert, die dieser Nutzung gar nicht zugestimmt haben.

D. Selbsttests

1. Internetnutzer können Netzneutralität überprüfen

Internetnutzer könne bis Ende Juni die Möglichkeit ihren Breitbandanschluss auf versprochene und tatsächliche Geschwindigkeit zu testen.

http://www.initiative-netzqualitaet.de/startseite/

2. Teil eines Botnetzes?

Der eco - Verband der deutschen Internetwirtschaft e.V. bietet auf seiner Webseite in Zusammenarbeit mit verschiedenen Herstellern von Antivirensoftware Lösungen an, um Botnet-Infektionen erkennen und ggf. entfernen zu können.

https://www.botfrei.de/

Datenschutzkenntnisse gut? Testen Sie sich selbst!

Fragestellung: Ein unter Betreuung stehender Patient soll medizinisch behandelt werden. Reicht es aus die Behandlung mit dem Betreuer durchzusprechen und dessen Einwilligung einzuholen?

Antwort A: Ja, wozu ist der Betreuer denn sonst bestellt?

Antwort B: Nein, der Betreute ist auch stets zu fragen.

Antwort C: Es ist egal, ob der Betreute oder der Betreuer einbezogen wird.

Lösung:

Die zweite Lösung (B) ist die Richtige! Das neue, seit dem 01.03.2013 geltende Patientenrechtegesetz schreibt in §§ 630 e Abs. 5, 630 d Abs. 1 BGB zwingend vor, dass dem einwilligungsunfähigen Patienten entsprechend seinem Verständnis die Situation zu erläutern ist, soweit dieser aufgrund seines Entwicklungsstandes und seiner Verständnismöglichkeiten in der Lage ist, die Erläuterung aufzunehmen, und soweit dies seinem Wohl nicht zuwiderläuft. Analog gilt dies auch in anderen Zusammenhängen, z. B. in einer Behinderten- oder Altenpflegeeinrichtung.

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