Newsletter Datenschutz Ausgabe 5 | Oktober 2012

DaSuMed

Datenschutzinfos für medizinische und soziale Einrichtungen

Liebe Kolleginnen und Kollegen,

es ist wieder soweit. Vier Seiten datenschutzrechtliche Neuerungen haben sich in den letzten Wochen bei mir angesammelt, die ich an Sie weiter leiten möchte. Viel Spaß bei der Lektüre.

Mit besten Grüßen, Mark Rüdlin

A. Gesetzesinfos

1. Datentransparenzverordnung

Die Datentransparenzverordnung (auf Basis der §§ 303a ff. SGB V) ist in Kraft getreten. Dazu Bundesgesundheitsminister Daniel Bahr: *„Mit der Verordnung legen wir den Grundstein für die Nutzung ausgewählter Leistungs- und Abrechnungsdaten der Krankenkassen insbesondere für Analysen des Versorgungsgeschehens im Rahmen der Versorgungsforschung und für Steuerungsaufgaben in der gesetzlichen Krankenversicherung. Unter Gewährleistung eines hohen Datenschutzniveaus wird die Aufbereitung dieser Daten entscheidend zur Weiterentwicklung des Versorgungssystems beitragen. Der nun beginnende Aufbau der hierzu erforderlichen Infrastruktur beim DIMDI ist ein erster Schritt, dem weitere folgen sollen.“*

2. Krebsregistergesetz

Am 22.08.2012 wurde der Entwurf zum Gesetz zur Weiterentwicklung der Krebsfrüherkennung und zur Qualitätssicherung durch klinische Krebsregister verabschiedet, das eine Reihe von datenschutzrechtlichen Anforderungen aufstellt. Die Ausgestaltung datenschutzrechtlicher Gesichtspunkte wurde im Rahmen einer 3-Jahres-Frist auf den Gemeinsamen Bundesausschuss übertragen.

B. Urteile

1. Presserechtlicher Auskunftsanspruch auch gegenüber GmbH der öffentlichen Hand

Das VG Berlin hat mit Urteil v. 22.05.2012 (Az.: 27 K 6.09) entschieden, dass der presserechtliche Auskunftsanspruch nach § 4 Abs.1 PresseG Berlin auch gegenüber einer GmbH der öffentlichen Hand besteht. In dem Urteil heißt es: „Der Kläger hat nach § 4 Abs.1 PresseG [Berlin] (…) Anspruch darauf, dass die Beklagte ihm Auskunft über die Personen, die das in Rede stehende Fest sponserten, und über die Beträge, mit denen diese Personen dieses Fest jeweils förderten, gibt, wobei die Beklagte besagte Personen rechtlich zutreffend zu

bezeichnen hat. Nach der genannten Vorschrift sind die Behörden verpflichtet, den Vertretern der Presse, die sich als solche ausweisen, zur Erfüllung ihrer öffentlichen Aufgaben Auskünfte zu erteilen. Diese Voraussetzungen liegen hier vor. (…)".

Dieser erweiterte Behördenbegriff umfasst daher auch juristische Personen des Privatrechts – wie eine GmbH – derer sich die öffentliche Hand (Kommunen, Gemeinden, Kreise) zur Erfüllung ihrer öffentlichen Aufgaben bedienen.

2. Elektronische Ressourcen im Arbeitsverhältnis unterliegen nicht der Vertraulichkeit

Das Landesarbeitsgericht Hamm hat in seiner Entscheidung vom 10.07.2012 (Az.: 14 Sa 1711/10) im Ergebnis an der neueren Rechtsprechung (vgl. dazu: LArbG Berlin-Brandenburg, v. 16.02.2011, Az.: 4 Sa 2132/10 | Landesarbeitsgericht Niedersachsen, v. 31.05.2010, Az.: 12 Sa 875/09) angeschlossen, wonach die gelegentliche private Nutzung elektronischer Ressourcen gestattet werden kann, ohne dass der Arbeitnehmer von eine Vertraulichkeit – hier von Chatprotokollen – hoffen darf, sondern mit einer Überwachung durch den Arbeitgeber rechnen muss.

3. Datenschutzverstöße sind abmahnfähig!

Das OLG Karlsruhe (Az. 6 U 38/11 v. 09.05.2012) hat entschieden, dass auch Datenschutzverstöße abgemahnt werden können. Diesem Urteil kommt eine große Bedeutung zu, da bis dato allgemein davon ausgegangen worden war, dass Datenschutzverstöße gerade nicht abgemahnt werden können. Aufhänger dafür war die fehlende Einordnung von Datenschutzvorschriften als Marktverhaltensregeln. Das OLG Karlsruhe nimmt eine Marktverhaltensregel an, wenn der Marktteilnehmer personenbezogene Daten erhebt, um eigene Angebote betreiben und bewerben zu können.

Dieses Urteil hat Konsequenzen. Zukünftig muss davon ausgegangen werden, dass Datenschutzverstöße wettbewerbsrechtlich geahndet werden können. Fehlerhafte Datenverarbeitung können dann genauso abgemahnt werden, wie unrichtige Datenschutzerklärungen.

4. Kein Entgelt für Branchenverzeichnis im Internet

Der BGH hat mit seinem Urteil vom 26.07.2012 (Az.: VII ZR 262/11) Abzockern endlich eine Grenze aufgezeigt. Wird eine Leistung in einer Vielzahl von Fällen unentgeltlich angeboten – wie beispielsweise ein Grundeintrag in ein Online-Branchenverzeichnis – und wird eine Entgeltklausel so in das Antragsformular eingefügt, dass es nach dem Gesamtbild nicht augenscheinlich ist, dann wird diese Entgeltklausel nicht Bestandteil eines Vertrages.

5. Verdeckte Arbeitnehmer-Videoüberwachung in Ausnahmefällen erlaubt

Das Bundesarbeitsgericht hat entschieden (Urteil v. 21.06.2012, Az.: 2 AZR 153/11), dass die heimliche Videoüberwachung von Arbeitnehmern erlaubt ist, um bei einem konkreten Verdacht auf strafbare Handlungen oder vergleichbaren schweren Verfehlungen, die zu Lasten des Arbeitgebers gehen, und keine weniger drastischen Mittel verfügbar sind, die Videoüberwachung im Ergebnis ultima ratio darstellt und diese dann erlaubt ist.

6. Kopftuch im Bewerbungsverfahren

Das Arbeitsgericht Berlin hat am 28.03.2012 (Az: 55 Ca 2426/12) entschieden, dass im Falle des Ausschlusses einer Bewerberin vor dem Abschluss des Bewerbungsverfahrens, weil diese auf Nachfrage des potentiellen Arbeitgebers angibt, das Kopftuch auch während der Arbeitszeit nicht ablegen zu wollen, wegen ihrer

muslimischen Religionszugehörigkeit diskriminiert wird. Denn es liegt ein Verstoß gegen das Allgemeine Gleichbehandlungsgesetz vor.

C. Sonstiges

1. Button-Lösung im Online-Verkauf

Seit dem 01.08.2012 ist § 312 g BGB zu beachten. Soll etwas über die eigene Webseite verkauft werden, dann muss der Bestellvorgang mit eindeutigen Hinweisen versehen werden. Einige Krankenhäuser und Träger sozialer Einrichtungen bieten zum Teil versteckt auf Unterseiten einzelne Produkte, wie z. B. ein Buch oder einen Film zum Kauf an. Nicht selten wird dabei übersehen, dass auch ein solcher Kaufvorgang so gestaltet werden muss, dass keine Zweifel daran aufkommen, dass Besucher etwas bestellen und wie viel dies kostet. Verstöße können abgemahnt werden, was bekanntermaßen teuer ist. Weitere Infos dazu finden sich beispielsweise im „Whitepaper zur Einführung der sogenannten Button-Lösung“ vom Bundesverband Digitale Wirtschaft (BVDW) - http://www.bvdw.org/medien/bvdw-handlungsempfehlungen-fuer-online-haendler-zur-einfuehrung-der-button-loesung?media=4043.

2. Übergangsregelungen für die Nutzung von alten Daten für Werbezwecke

Seit dem 01.09.2012 müssen Einwilligungen betroffener Personen eingeholt werden, wenn diese für Werbezwecke genutzt werden sollen. Eine solche Einwilligung muss in Verträgen oder allgemeinen Geschäftsbedingungen optisch deutlich hervorgehoben werden. Aber es gibt Ausnahmen:

- Hat die werbetreibende Einrichtung die Daten selbst erhoben oder aus einen öffentlichen Verzeichnis erlangt und möchte es die Daten für eigene Zwecke verwenden, ist das legitim. Ebenso für berufsbezogene Werbung, die an die berufliche Anschrift geht und für Spendenwerbung.
- Auch Daten, die von Adresshändlern bezogen wurden, dürfen zu Werbezwecken verwendet werden, wenn die Datenherkunft protokolliert ist und darüber Auskunft erteilt werden kann.

Auch in den vorgenannten Fällen können die Adressaten der Nutzung oder Übermittlung ihrer Daten widersprechen. Auf das Widerspruchsrecht ist ausdrücklich hinzuweisen.

Bis zum 31.08.2012 galt eine Übergangsregelung für Daten, die bis zum 01.09.2009 erhoben worden waren. Diese Übergangsregel ist ausgelaufen.

3. Medizintechnik ist anfällig für Computerviren

Auch medizinische Technologie kann Ziel von Virenattacken werden. Grund veraltete Betriebssysteme in Krankenhäuser, so die BBC (http://www.bbc.co.uk/news/technology-19979936). Wenn zum Beispiel ein Herzfrequenzmessgerät unter einer alten Windows-Version betrieben und von Schadsoftware manipuliert wird, könnten Patienten durch falsche Messungen zu Schaden kommen.

4. Notfallzugriffe im UKE

Die vom Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) bei Universitätsklinikum Hamburg-Eppendorf kritisierte sehr hohe Zahl von Notfallzugriffen – zur Umgehung eingerichteter Zugriffsrechte – hat sich weiter deutlich reduziert. Im März 2012 gab es noch 11.671 Zugriffe, zwischenzeitlich hat sich die Zahl halbiert.

Die Beachtung durch die Aufsichtsbehörde macht deutlich, dass der Datenschutz im IT-Management einer Einrichtung mit sensiblen personenbezogenen Daten, wie die von Patienten und Klienten, angemessen umzusetzen ist.

5. Achtzig Prozent aller Daten gehen innerhalb der Unternehmen verloren

Bei IT-Brunch in Ludwigsburg wiesen Sicherheitsexperten darauf hin, dass ein Hauptgefahrenpunkt für Datenverluste nicht von außen, sondern von innen ausgelöst werden. „80 Prozent aller Daten gehen innerhalb der Unternehmen verloren“, so Arne Vodegel von Protected-networks.com, einem Berliner Software-Unternehmen. In vielen Einrichtungen haben zu viele Mitarbeiter zuviele Zugriffsrechte auf Daten, die sie für ihre eigene Arbeit gar nicht benötigen. Dabei ist gar keine kriminelle Energie notwendig, um Datenschutzpannen zu verursachen. 65 % aller Mitarbeiter in deutschen Unternehmen können vollkommen legitim auf sensible Unternehmensdaten zugreifen. Mehr als die Hälfte aller Beschäftigten monieren, dass sie auf mehr Daten zugreifen können, als für Arbeit notwendig wäre.

6. Schutzrechte im Internet

Die Klagen von Bettina Wulff und Max Mosley haben verdeutlicht, dass Menschen auch im Internet, insbesondere auch in Suchmaschinen nicht schutzlos sind. Wird gemäß § 35 Abs. 5 BDSG ein Widerspruch gegen eine Datenverarbeitung erklärt oder sperrt sich die betroffene Person speziell gegen eine Veröffentlichung im Internet, dann muss eine Prüfung der schutzwürdigen Interessen erfolgen. Überwiegen diese aufgrund einer „besonderen persönlichen Situation“, dann müssen zur Beendigung der Beeinträchtigung der Schutzrechte diese Störungen unterbleiben und entsprechende Inhalte vom Netz genommen werden, sofern dies technisch und organisatorisch möglich ist.

7. Smartphone-Besitzer vernachlässigen Sicherheit

Eine Umfrage im Auftrag des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) hat ergeben, dass jeder fünfte Smartphone-Besitzer vollständig auf Sicherheitsfunktionen verzichtet. Jeder Zweite hat keine Virenschutz aktiviert und nur jeder sechste Nutzer verwendet ein Programm zur Ortung des Smartphones bei Verlust oder Diebstahl. Nur jeder neunte Besitzer hat eine App installiert, die die Löschung von Daten per Fernzugriff im Falle des Abhandenkommens ermöglichen.

Der elementarste Schutz eines Smartphones – das in Wirklichkeit ein Hochleistungsrechner mit Telefonfunktion ist – wird durch die Verwendung eines Zugriffsschutzes realisiert. Muss beispielsweise vor jeder Verwendung (nicht nur beim Einschalten des Gerätes) die PIN eingegeben werden, reduzieren sich die Missbrauchsmöglichkeiten drastisch.

8. Horrorvideo - Falsche Facebook-Datenschutzeinstellungen

Benutzer nachlässig eingerichteter Datenschutzeinstellungen bei sozialen Netzwerken wie Facebook können sich ein allgemeines (http://www.youtube.com/watch?v=aqo0B-KJ0Ko) oder sogar mit den eigenen Einstellungen personalisiertes (http://thomaslachetta.wordpress.com/2011/11/04/facebook-horror-video-i-dare-you-www-takethislollipop-com/) Horrorvideo ansehen, dass die Phantasie dafür öffnen kann, wie lebenspraktisch extrem es werden kann, wenn man allzu sorglos mit Datenschutzeinstellungen umgeht.

9. Informationspflichten bei Datenschutzpannen

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat ein umfassendes Merkblatt zum Umgang mit Datenpannen erstellt. Dort wird erläutert, was und wie nach § 42 a BDSG den Betroffenen und der

Aufsichtsbehörde gemeldet werden muss. Das Merkblatt kann wie folgt geladen werden: http://www.datenschutz-berlin.de/content/themen-a-z/informationspflicht-nach-42-a-bdsg

10. Prüfung der eigenen Webpräsenz

Der Verband der deutschen Internetwirtschaft hat das Projekt Initiative-S gestartet. Das Angebot richtet sich an kleine und mittlere Einrichtungen, deren Internetpräsenz als Trojanerschleuder missbraucht werden könnte. Eine Anmeldung mit Domainnamen und Mailadresse startet eine kostenfreie Prüfung der eigenen Webseite. Mehr unter: https://www.initiative-s.de/index.html

11. Gewalt gegen Kinder und Jugendliche – Erkennen und Handeln

Das bayerische Staatsministerium für Arbeit und Sozialordnung hält eine Broschüre mit 164 Seiten bereit, die praktische Erläuterungen enthält, Gewalt gegen Kinder und Jugendliche im Rahmen der eigenen Arbeit zu erkennen: http://www.verwaltung.bayern.de/egov-portlets/xview/Anlage/4040841/Gewalt%20gegen%20Kinder%20und%20Jugendliche%20-%20Erkennen%20und%20Handeln.pdf

Datenschutzkenntnisse gut? Testen Sie sich selbst!

Fragestellung: Im Rahmen einer Patientenuntersuchung stellen Sie bei einem Kind zahllose Hämatome fest? Müssen Sie die Polizei einschalten?

Antwort A: Nein, ich unterliege der strafbewehrten Schweigepflicht (Patientengeheimnis).

Antwort B: Das entscheide ich selbst.

Antwort C: Ja, Kindesmisshandlung und- vernachlässigung ist stets anzuzeigen.

Lösung: Sie müssen nicht die Polizei einschalten, aber Sie können. Denn es liegt wieder eine gegenwärtige Gefahr für Leib und Leben des Kindes vor (§ 34 StGB, rechtfertigender Notstand). Es ist nicht absehbar, dass die Hintergründe und Ursachen für die festgestellten Hämatome beseitigt sind. Träger sozialer Einrichtungen sollen im Übrigen beachten, dass in vielen Bundesländern (z. B. Bremen, Hamburg, Schleswig-Holstein etc.) Vereinbarungen zwischen Bundesland und Träger geschlossen wurden, die eine unverzügliche Einschaltung des Jugendamtes verlangen. Das neue Bundeskinderschutzgesetz hat darüber hinaus auch noch neue Möglichkeiten durch die Nutzung einer anonymen Jugendamt-Hotline eröffnet.

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