

DaSuMed

Datenschutzinfos für medizinische und soziale Einrichtungen



Liebe Kolleginnen und Kollegen,

Sie lesen gerade die erste Ausgabe von **DaSuMed** mit aktuellen Datenschutzinfos. Zukünftig informiere ich Sie über aktuelle Entwicklungen, Trends und wichtige Urteile für Ihren Arbeitsbereich in medizinischen oder sozialen Einrichtungen, ergänzt durch ein Schwerpunktthema und eine Rubrik zum Überprüfen der eigenen Kenntnisse.

Mit besten Grüßen, Mark Rüdlin

Die datenschutzrechtlichen Neuigkeiten der letzten Wochen:

1. Neues Landesdatenschutzgesetz (LDSG) in Schleswig-Holstein

Am 27.01.2012 trat eine überarbeitete Fassung des LDSG in Schleswig-Holstein in Kraft. Folgende Neuerungen finden sich dort:

- In der Regelung zu den technisch organisatorischen Maßnahmen (§ 5 LDSG) werden moderne Datenschutzziele festgelegt.
- In § 7 LDSG wurde die bisher weitgehend wirkungslose Regelung zu den Verfahrensverzeichnissen geändert. Diese werden künftig durch das ULD im Internet allgemein zugänglich gemacht.
- Durch eine Änderung des § 8 Abs. 2 LDSG wurde für gemeinsame Verfahren und Abrufverfahren erstmals eine einheitliche datenschutzrechtliche Verfahrensverantwortlichkeit eingeführt.
- Die Normierung der Videoüberwachung wurde an die neueren Regelungen im Bundesdatenschutzgesetz und in anderen Ländern angepasst (§ 20 LDSG).
- Erstmals ins LDSG eingeführt wurde eine materiell rechtliche Regelung zur Veröffentlichung von Daten im Internet (§ 21).
- Ebenfalls neu im LDSG ist die Regelung zu Informationspflichten bei unrechtmäßigen Übermittlungen (sog. Breach Notification, § 27a).
- Die Rechtsstellung des/der Landesbeauftragten für Datenschutz (LfD) und seiner/ihrer Dienststelle, also des ULD, wurde geändert: Der/die LfD unterliegt nun keinerlei Rechts- und Fachaufsicht mehr.
- Der Tätigkeitsbericht des ULD ist nur noch alle

zwei Jahre zu erstellen (§ 39 Abs. 5 LDSG).

2. EU Datenschutzrichtlinien Novelle

- Zukünftig soll ein EU-weit geltendes Gesamtregelwerk für den Datenschutz geschaffen werden. Unnötige administrative Anforderungen sollen beseitigt werden.
- Eine Reihe von Vereinfachungen sind geplant.
- Bürgerrechte sollen gestärkt werden, insbesondere das „Recht auf Vergessen werden“ in Bezug auf Onlinedienste.
- Außerhalb der EU statt findende Bearbeitungen von personenbezogenen Daten durch auf dem EU-Markt aktive Unternehmen unterliegen zukünftig den EU-Vorschriften unterliegen.
- Die Unabhängigkeit der nationalen Datenschutzbehörden soll gestärkt werden. Unter anderem werden Bußgelder drastisch erhöht.

3. Neue Gesetzesvorhaben

BMJ und BMG haben einen Referentenentwurf für ein

Gesetz zur Verbesserung der Rechte von Patientinnen und Patienten (**Patientenrechtgesetz**) vorgelegt. Mit der Neuregelung sollen Patientenrechte transparent, verlässlich und ausgewogen gestaltet und in der Praxis möglichst problemlos gewährleistet werden. Der Entwurf orientiert sich hierbei am Leitbild des mündigen Patienten, der jedoch oftmals nicht wüsste, welche Rechte ihm tatsächlich zustünden, da diese im Wesentlichen dem Richterrecht unterliegen. Das Dienstvertragsrecht im 8. Titel des BGB soll um einen neuen Untertitel „Behandlungsvertrag“ ergänzt werden, der in den §§ 630a bis 630h BGB-E die bisherigen richterlich entwickelten Grundsätze des Arzthaftungs- und Behandlungsrechts festschreiben soll. Dabei sollen Informations- und Aufklärungspflichten gegenüber dem Patienten, die Pflicht zur Dokumentation der Behandlung, das Akteneinsichtsrecht und die Beweislastverteilung bei Behandlungsfehlern in ihren Grundzügen geregelt werden. Ferner sollen die Rechte der Patienten gegenüber Leistungsträgern und die Patientenbeteiligung durch Änderung einiger Vorschriften im SGB

V, im KHG und der PatBeteiligungsV gestärkt werden.

Die aus dem Jahr 1995 stammende **EU-Datenschutzrichtlinie** soll überarbeitet werden. Ziele sind dabei die Stärkung der Online-Rechte des Einzelnen die Wahrung der Privatsphäre zu stärken und die digitale Wirtschaft Europas anzukurbeln.

Auf nationaler Ebene wird an einer **Novellierung des Telemediengesetzes** gearbeitet.

4. Testamentsregister

Zum Jahreswechsel wurde das zentrale Testamentsregister in Betrieb genommen. Recherchen können nun zentral erfolgen. Mehr unter:

www.testamentsregister.de

5. Datenschutzpanne in einem Hamburger Krankenhaus

Beim letzten Treffen der Datenschutzbeauftragten der Hamburger Krankenhäuser beim einschlägigen Kreis der Aufsichtsbehörde wurde folgendes Vorkommnis debattiert, das in jedem Krankenhaus oder sozialen Einrichtung so auch hätte passieren können:

Ein psychisch kranker Patient kam in die Notaufnahme eines Krankenhauses. Er wurde bis zum Eintreffen des Arztes sieben Minuten alleine in einem Behandlungsraum gelassen, in dem sich Patientenunterlagen und ein nicht gesperrter Bildschirmarbeitsplatz befanden. Der Patient behauptete später, er habe Daten anderer Patienten aufgerufen, gespeichert und auf einen externen Rechner übermittelt.

Der Wahrheitsgehalt konnte nicht geklärt werden. Das Krankenhaus reagierte auf diesen Vorfall mit folgenden Maßnahmen:

- Bildschirmschoner werden nach zwei Minuten automatisch aktiviert, der nur durch Eingabe des Passworts wieder entfernt werden kann.
- Die Möglichkeit, USB-Sticks zu nutzen, wurde unterbunden.
- Verpflichtung aller Mitarbeiter, beim Verlassen des Raumes sich aktiv vom System abzumelden.

In einigen Häusern wird bereits mit elektronischen Fingerabdruckscannern getestet, um das von allen als lästig empfundene Eingeben von Passwörtern

vermeiden zu können. Leider lassen sich noch nicht alle Subsysteme mit dieser Methode anbinden.

6. Datenschutzpanne IT-Dienstleister für soziale Einrichtungen

Auf den Servern des IT-Dienstleisters Rebus (einer Tochtergesellschaft der BRÜCKE) waren über Monate oder gar Jahre hinweg tausende Patientendaten aus Schleswig-Holstein frei zugänglich. Der Grund soll in organisatorischem Chaos und dem Einsatz handgestrickter Lösung bestanden haben. Die Sicherheit wurde nie überprüft.

7. Gefühlte Datensicherheit

Die Unternehmensberatung Ernst & Young hat die Ergebnisse ihrer diesjährigen »Global Information Security Survey« vorgestellt. An der Untersuchung nahmen 1700 Experten aus 52 Ländern teil. Gefragt wurde nach einer Einschätzung zu den aktuellen Entwicklungen und Risiken in Bezug die Datensicherheit in den Unternehmen.

Es gibt eine deutliche Tendenz vieler Unternehmen, ihren Mitarbeitern auch außerhalb ihres Arbeitsplatzes

über das Internet Zugang zu den Geschäftsdaten zu gewähren. Damit steigt das Risiko für die Datensicherheit. 56 % aller befragten Unternehmen gab an, die Sicherheitsstrategien überprüfen oder modifizieren zu wollen.

8. Stellungnahme des Düsseldorfer Kreis zum Thema Datenschutz in Social Networks

Die deutschen Datenschutzbehörden, die sich im „Düsseldorfer Kreis“ zusammengeschlossen haben, unterstützen die Position des ULD (Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein). Das ULD hatte zuvor festgestellt, dass das Betreiben von Facebook-Fanseiten gegen das deutsche Datenschutzrecht verstößt und hatte begonnen, dagegen vorzugehen und von Facebook (und anderen Anbietern) praktische Verbesserung der Datenschutzbelange eingefordert.

9. Je jünger, desto gefährdeter – Umgang mit sozialen Netzwerken

Die schlechte Nachricht: Über die Hälfte aller Jugendlichen zwischen 12 und 19 Jahren sind täglich in einem sozialen Netzwerk

aktiv. Mehr als die Hälfte kennt die Allgemeinen Geschäftsbedingungen (AGB) des genutzten Netzwerkes nicht. Immerhin nutzen 79 % die Privatsphäre-Einstellungen, die den Zugriff Dritter einschränkt. Viele Nutzer hinterlassen intensiv Spuren. 65 % haben eigene Fotos oder Video eingestellt. 2/5 laden auch Bilder von Freunden oder Familie hoch. Jeder Zweite gibt seine E-Mail-Adresse bekannt.

Die gute Nachricht: mit steigendem Alter wächst die Sensibilität im Umgang mit der Datenpreisgabe.

Dieses Verhalten hat auch Auswirkungen im Umgang mit Patienten und Klienten. Immer häufiger kommt es vor, dass über soziale Netzwerke Kontakt zu ehemaligen Patienten und Klienten gehalten wird und in der Kommunikation auch Bezug auf andere genommen wird. Dies führt zu einer Gefährdung des strafbewehrten Patientengeheimnisses.

10. Vertrauen in den Datenschutz

77 % aller Deutschen vertrauen den Krankenkassen in Punkto Datenschutz. Verlierer sind soziale Netzwerke

mit einer Vertrauensquote von 14 %. Über die tatsächlichen Leistungen und Maßnahmen wird nichts ausgesagt. Dies unterstreicht die große Bedeutung des Patientendatenschutzes.

11. Selbstauskunft

Mit der Novellierung des Bundesdatenschutzgesetzes (BDSG) wurde das Bürgerrecht zur Selbstauskunft gestärkt. Jeder Bundesbürger hat das Recht, einmal jährlich eine Selbstauskunft bei Institutionen wie Adresshändlern, Inkassofirmen oder Schufa zu bekommen. Ein neuer Webdienst vereinfacht dieses Prozedere. Auf der Seite selbstauskunft.net kann mit wenigen Klicks bei 79 Stellen eine Selbstauskunft beantragt werden.

12. Klage gegen Zensus 2011 abgewiesen

Gegen die im Mai 2011 begonnene Volkszählung hatte ein Einwohner geklagt. Im Gegensatz zum Jahr 1983 hatte das Verwaltungsgericht Neustadt die Rechtmäßigkeit des Zensus attestiert.

13. Internetsperren sind rechtswidrig

Der EuGH hat in einem Urteil vom 24.11.2011 festge-

stellt, dass ein nationales Gericht einem Anbieter von Internetzugangsdiensten (dies kann auch ein Krankenhaus oder ein Suchthilfeeinrichtungsträger sein) nicht verpflichten kann, ein Filtersystem einzuführen, um das Herunterladen unzulässiger Dateien zu verhindern. Die Anbieter werden also davon freigelassen, polizeiliche Aufgaben zum Schutz des Urheberrechts wahrnehmen zu müssen.

14. Kein Cloud-Computing für Einrichtungen im Gesundheitswesen

Die EU Netzsicherheitsagentur Enisa bemängelt den leichtfertigen Umgang mit Cloud-Computing. Beim Cloud-Computing wird Speicherplatz bei einem Unternehmen angemietet. Häufig ist dabei unklar, wo Daten tatsächlich gespeichert werden. Handelt es sich dann auch noch um ein nicht-europäisches Unternehmen, sind die in Europa geltenden Datenschutzstandards nicht mehr gewährleistet.

Die Nutzung von Cloud-Computing für Patienten- oder Klientendaten verstößt gegen europäisches Datenschutzrecht und be-

gründet die Strafbarkeit einer Schweigepflichtverletzung gemäß § 203 StGB.

15. Betrieblicher Datenschutzbeauftragter

Der Bundesbeauftragte für den Datenschutz hat die Neuauflage „Die Datenschutzbeauftragten in Behörde und Betrieb“ veröffentlicht. Die Broschüre

kann von der Seite www.bfdi.bund.de geladen werden.

„Personenbezogenen Daten“ – Wissen Sie was damit gemeint ist?

Bestimmt haben Sie diesen Begriff – personenbezogene Daten – schon mal gehört. Den meisten fällt dann ein, dass das was mit Datenschutz zu tun hat. Aber was? Das soll Sie gleich erfahren.

In § 3 BDSG findet sich eine kurze und knappe Beschreibung des Begriffs. Dort heißt es: *Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person.* Stoßen Sie auf eine Beschreibung zusammen mit einem Namen, dann haben Sie den klassischen und einfachen Fall vorliegen. Dabei spielt es keine Rolle, was über die Person im Einzelnen ausgesagt wird. Das gilt sowohl für den Hinweis „Psychiatriepatient“ als auch den damit verknüpften Geburtstag.

Wird der Name nicht genannt, ist aber trotzdem klar, wer gemeint ist, dann liegt auch ein Personenbezug vor. Beispiel: Wenn in einer Rundmail darum gebeten wird keine Schreibaufträge an die interne Schreibkraft

zu senden, weil diese Person noch sechs Wochen krank sein wird, dann wissen natürlich alle wer gemeint ist, wenn es sich um die einzige Schreibkraft im Haus handelt. Ähnlich bei E-Mail-Adressen wie buchhaltung3@krankenhaus.de. Außenstehenden erschließt sich das vielleicht nicht sofort, doch eine einfache Nachfrage klärt sofort vieles. Auch ein Bild gehört zu den personenbezogenen Daten, selbst dann, wenn kein Name dabei steht. Gleiches gilt für die Telefonnummer, selbst wenn zwei oder drei Personen sich ein Telefon teilen. Ein solcher Gruppenbezug führt zum gleichen Ergebnis.

Was ist die Folge der Eingruppierung zu den personenbezogenen Daten? Die Datenschutzbestimmungen sind zu beachten

Personenbezogene Daten sind:

- alles rund um einen Namen
- Eine Person charakterisierende Eigenschaften
- ggf. E-Mail-Adressen
- ggf. Telefonnummer
- Bilder

Story: Live From Bagdad – analoger und digitaler Datenschutz

Manchmal denke ich daran, dass die Telefone in meiner Kindheit grau waren, eine Wählscheibe hatten und einen schweren Hörer, der an einer gedrehten Schnur hing. Die Wählscheibe verursachte beim Wählen der Nummer so ein ratternd-klackerndes Geräusch, das ich heute noch im Ohr habe. Jede Einheit kostete einzeln und Ferngespräche waren teuer. Wollte ich meine Gastfamilie in Amerika anrufen, ging ich noch Ende der Achtziger Jahre in eine Telefonzelle und benutzte zur Kostenkontrolle eine Telefonkarte, die ich zuvor mit 50 Mark aufgeladen hatte.

Letztes Wochenende wurde ich wieder an die Telefone meiner Kindheit erinnert. Und an den Datenschutz. Beides fügte sich auf unterhaltsame Weise in einem langjährigen Freund zusammen, den ich kenne, seit wir beide dreizehn Jahre alt waren. Wir saßen in einem vollen Restaurant beim Essen ziemlich dicht neben einem Ehepaar um die sechzig, das sich geschlagene zwei Stunden anschwieg und dafür aber umso genauer unsere Unterhaltung mit zu hören schien. Mein Freund berichtete mir von seiner neuen Liebe, einem Amerikaner, der als IT-Spezialist in Bagdad für irgendeine Firma arbeitet, die wiederum Dienstleister für das Militär ist. Was genau er dort tut ist ein großes Geheimnis. Er habe auch viele Jahre als Immobilienmakler gearbeitet, nur so viel habe er noch verraten. Welche IT-Firma stellt einen 50jährigen ein, der vorher Makler war? sagte ich zu meinem Freund, den ich hier Hans nenne. Das hört sich für mich eher an, als ob du dich in einen Spion verguckt hättest.

Ich merkte an, dass ich mit so jemandem nicht ohne Weiteres online kommunizieren würde, als Hans berichtete, neulich habe sich sein E-Mail Programm so komisch verhalten und habe während des Schreibens seine Worte gelöscht. Soll doch dein Liebster mal für eine gesicherte Verbindung sorgen! sagte ich. Hans konnte meine Bedenken nicht so richtig nachvollziehen. Wen sollten denn schon ein paar Liebeserklärungen interessieren? Er hatte überhaupt keine Vorstellung davon, was technisch alles möglich ist, wenn erst mal jemand unberechtigten Zugriff auf seinen Rechner hat. Und er wähnte sich in Sicherheit – frei nach dem Motto, „Ich tue niemandem was, also wird mir auch niemand was tun“.

Doch ein wenig nachdenklich geworden ob meiner Vorträge über IT-Sicherheit im Allgemeinen und die Bösartigkeit von Geheimdiensten im Besonderen zückte er dann kurz darauf – anscheinend völlig unbeeindruckt von unseren Mithörern – sein iPhone, warf Skype an und sagte, ich könne seinem Lover das mit der gesicherten Kommunikation ja gleich mal selber erklären, er hätte ihm eh noch einen Anruf versprochen. Ich lehnte dankend ab und verdrückte mich vorläufig auf die Toilette. Das hinderte Hans dann aber nicht, mir nach meiner Rückkehr ein verpixelttes Live-Bild aus Bagdad vor die Nase zu halten, auf dass der Amerikaner wenigstens einen optischen Eindruck von mir bekomme: „I show you my friend ...“ und dann folgten Liebeserklärungen in einem dicht besetzten Restaurant. Datenschutz? dachte ich seufzend. Privatsphäre? War da was?

Als wir ein paar Tage später noch mal darüber sprachen, regte sich mein Freund mehr über das lauschende Paar am Nebentisch auf, als über alle real bestehenden Szenarien der technischen Überwachung, die ich ihm geschildert hatte. Eigentlich würden wir doch bei einem simplen Res-

restaurantbesuch viel mehr von uns preisgeben, warum also noch Datenschutz? Weil unsere Geschichten nach dem Restaurantbesuch nur in den Köpfen der sprachlosen Alten sind, antwortete ich. Nicht online abrufbar, nicht verknüpfbar mit anderen Informationen über uns, nicht lebenslänglich gespeichert und für alle Welt verfügbar. Darum Datenschutz. Unter anderem.

© Paula Coehler

Datenschutzkenntnisse gut? Prüfen Sie sich selbst!

Fragestellung: Ein Servicetechniker meldet sich bei Ihnen und teilt mit, dass Ihr PC ausgetauscht werden müsse. Er werde Ihren abbauen und mitnehmen und in einer halben Stunde das neue Gerät aufbauen. Lassen Sie ihn arbeiten?

Antwort A: Nein, ich frage zuerst in der EDV-Abteilung nach, ob ein Servicetechniker bestellt wurde.

Antwort B: Wenn die EDV-Abteilung eines Servicetechniker beauftragt hat, dann bleibe ich mit dem Techniker im Raum bis er seine Arbeit beendet hat.

Antwort C: Ich habe genügend zu tun, der Servicetechniker soll tun, was er tun muss.

Richtige Antwort: Die Antworten A und B sind richtig, allerdings nur in Verbindung. Selbst wenn ein Servicetechniker beauftragt wurde sollte er nicht alleine mit Patienten- bzw. Klientenunterlagen gelassen werden.

Impressum:

Mark Rüdlin – Rechtsanwalt und Datenschutzbeauftragter

Struenseestr. 37 | 22767 Hamburg | Tel. 040 697972 -80 | Fax -90 | [mailto: ra@markruedlin.de](mailto:ra@markruedlin.de)

Nach wechselnden Tätigkeiten arbeite ich seit 2000 als Rechtsanwalt mit Ausrichtung auf Fragestellungen rund um die als EDV und als Datenschutzbeauftragter. Ich habe mich dabei immer auf medizinische und soziale Einrichtungen in Hamburg, Schleswig-Holstein, Niedersachsen und Baden-Württemberg konzentriert und kenne die Fragestellungen und Alltagsprobleme der Einrichtungen und Träger – insbesondere die damit verbundenen datenschutzrechtlichen Ausprägungen - aus eigener Anschauung.

Ich bin 1962 im fränkischen Ebern geboren. Seit Anfang der 80er Jahre lebe ich – von kurzen Unterbrechungen abgesehen - in Hamburg, der Stadt, die inzwischen zu meiner Heimat geworden ist. Ich bin verheiratet und habe zwei inzwischen erwachsene Kinder.

Zusammen mit meinem Kollegen Dirk Otto – Rechtsanwalt und Datenschutzbeauftragter in Berlin – habe ich den Anspruch, jede datenschutzrechtliche Fragestellung in medizinischen und sozialen Einrichtungen praxisnah und den Bedürfnissen der Einrichtung Rechnung tragend zu lösen.

Feedback: Ich freue mich sehr über Ihr Feedback, Ihre Anregungen und Wünsche für zukünftige Ausgaben dieses Newsletters. Bitte senden Sie diese an: ra@markruedlin.de