Entscheidende Behörde

Datenschutzkommission

Entscheidungsdatum

09.10.2013

Geschäftszahl

K213.220/0009-DSK/2013

Text

[Anmerkung Bearbeiter: Namen (Firmen), (Internet-)Adressen, Aktenzahlen (und dergleichen), Rechtsformen und Produktbezeichnungen etc. sowie deren Initialen und Abkürzungen können aus Pseudonymisierungsgründen abgekürzt und/oder verändert sein. Offenkundige Rechtschreib-, Grammatik- und Satzzeichenfehler wurden korrigiert.]

E M P F E H L U N G

Die Datenschutzkommission hat unter dem Vorsitz von Dr. SPENLING und in Anwesenheit der Mitglieder Dr. SOUHRADA-KIRCHMAYER, Mag. MAITZ-STRASSNIG, Mag. ZIMMER, Mag. HUTTERER und Dr. GUNDACKER sowie des Schriftführers Dr. SCHMIDL in ihrer Sitzung vom 9. Oktober 2013 folgenden Beschluss gefasst:

Aus Anlass einer Eingabe betreffend die EDV-gestützte Patientendokumentation „P[…]dok“ des a.ö. Bezirkskrankenhauses X. ergeht gemäß § 30 Abs. 6 DSG 2000 zur Herstellung des rechtmäßigen Zustands die folgende Empfehlung […]:

1. [Das] Bezirkskrankenhaus X. möge die Zugriffsberechtigung auf die in der EDV-gestützten Patientendokumentation „P[…]dok“ verarbeiteten Patientendaten so gestalten, dass die zugreifende Person nur Einblick in jene Daten erhält, die für die Erfüllung ihrer Aufgaben berufsgruppenspezifisch erforderlich sind.

2. Für die Umsetzung dieser Empfehlung wird eine F r i s t von z w ö l f Mo n a t e n gesetzt.

Rechtsgrundlagen: § 1 Abs. 1 und 2, § 4 Z 1 und 2, § 14 Abs. 1 und 2 und § 30 Abs. 2 und 6 des Datenschutzgesetzes 2000 – DSG 2000, BGBl. I Nr. 165/1999 idgF.

G r ü n d e f ü r d i e s e E m p f e h l u n g

A. Verfahrensgang und Sachverhaltsfeststellungen

Folgender Sachverhalt wird festgestellt:

1. Die Datenschutzkommission richtete am 25. Juli 2013 das folgende – auszugsweise wiedergegebene – Schreiben an das a.ö.

Bezirkskrankenhaus X. (BKH X.):

„1. Die Datenschutzkommission hat eine Eingabe zum Anlass genommen, ein amtswegiges Prüfverfahren gemäß § 30 des Datenschutzgesetzes 2000 – DSG 2000 gegen das a.ö.

Bezirkskrankenhaus X. einzuleiten.

Es besteht der begründete Verdacht, dass in Bezug auf die EDVgestützte Patientendokumentation „P[…]dok“ die gemäß § 14 DSG 2000 vorgeschriebenen Datensicherheitsmaßnahmen nicht oder nicht gänzlich eingehalten werden.

[…]

Insbesondere besteht der Verdacht, dass der Zugang zu Patientendaten durch diverse Personen auch ohne konkreten Anlass möglich ist.

Bei Gesundheitsdaten handelt es sich um „sensible Daten“ im Sinne des § 4 Z 2 DSG 2000, die einem besonderen Schutz unterliegen (vgl. dazu § 9 DSG 2000).

2. Sie werden ersucht, dazu innerhalb einer F r i s t von v i e r W o c h e n ab Erhalt dieses Schreibens allgemein schriftlich Stellung zu nehmen und insbesondere auf folgende Fragen einzugehen:

a) Gibt es im a.ö. Bezirkskrankenhaus X. einen Datenschutzbeauftragten bzw. eine Person, der der Aufgabenbereich Datenschutz (mit)obliegt?

b) Welche Daten werden in P[…]dok gespeichert?

c) Wer hat Zugang zu P[...]dok? Nur ärztliches Personal oder auch nichtärztliches Personal?

d) Werden Zugriffe protokolliert?

e) Ist der Zugriff auf Patientendaten für alle Zugreifenden im gleichen Ausmaß möglich oder gibt es Zugangsbeschränkungen für bestimmte Gruppen? Hat bspw. das ärztliche Personal einen erweiterten Zugriff?

f) Wie wird sichergestellt, dass Zugriffe nur anlassbezogen und zweckbezogen erfolgen?

g) Sind die Computergeräte, über welche der Zugang zu P[…]dok erfolgt, besonders geschützt, etwa in eigenen Räumen untergebracht, der Zugang durch Passwörter abgesichert, oder sind diese Geräte allgemein zugänglich?“

2. Das BKH X. nahm zu diesem Schreiben mit E-Mail vom 7. August 2013 wie folgt Stellung (auszugsweise Wiedergabe):

„Sehr geehrte Damen und Herren, bezugnehmend auf Ihre Anfrage GZ: DSK-K213.220/0002-DSK/2013 dürfen wir wie folgt antworten:

a) Datenschutzbeauftragter : A.B.

b) Welche Daten werden in P[…]dok gespeichert?

Identifikationsdaten:

Name, Geburtsdatum, Adresse

administrative Daten:

Versicherungsdaten,

Bewegungsdaten (Aufenthaltsdatum, Ambulanzbesuchsdaten, Stations-/Abteilungszuordnung)

Daten zur Leistungsverrechnung mit SV-Träger

medizinische Daten:

Notfalldaten (Allergien),

allgemeine anamnestische Daten,

abrechnungsrelevante Diagnosen und Therapien,

Befunde, Laborwerte und andere diagnostische und therapeutische Daten, Bilddokumentation (Endoskopie, OP, Wundmanagement)

c) Zugang zu P[…]dok haben nur Mitarbeiter, denen ein individueller Zugangsschlüssel eingeräumt wurde. Solche Zugangsschlüssel wurden den medizinisch/pflegerisch tätigen Mitarbeitern eingeräumt, sowie den mit Dokumentation und Leistungsverrechnung betrauten Mitarbeitern. Ebenso Mitarbeitern, die mit besonderen Aufgaben zB Hygiene, Sturzanalyse u.ä. betraut sind.

d) Sämtliche Zugriffe auf Befunde und Bilddokumentation in P[…]dok werden protokolliert (IP-Adresse, Benutzername, Datum und Uhrzeit). Neben dem Zugriff auf Befunde, etc werden aber auch sämtliche Aktivitäten (zB Aufruf von Suchprogrammen, Tabellarische Übersicht über Aufenthalte oder vorhandene Dokumente, etc) protokolliert.

Jeder Mitarbeiter besitzt eine eigene, individuelle Benutzerkennung (keine Gruppenbenutzer für P[…]dok, wie sie unseres Wissens in vielen anderen Einrichtungen immer noch üblich sind) und ein nur ihm bekanntes Schlüsselwort. Die Mitarbeiter sind verpflichtet, sich beim Verlassen des Arbeitsplatzes im System abzumelden. Seit ca 2-3 Jahren findet eine automatische Abmeldung nach 10 Minuten Inaktivität statt.

e) Mitarbeiter, die nicht im klinischen Bereich tätig sind, haben keinen Zugriff auf die Daten. Ärzte, Therapeuten und Pflegekräfte haben grundsätzlich dieselben technischen Zugriffsmöglichkeiten, sind jedoch durch Dienstvorschriften darauf eingeschränkt nur in bestimmte Daten und nur zu bestimmten Zwecken Einsicht zu nehmen bzw. Verwendungen zu machen. Eine früher versuchte technische Einschränkung (Ärzte greifen nicht auf Pflegedokumente zu, Pflegekräfte greifen nur auf Pflegedokumente zu) ist gescheitert und hätte in vielen Fällen eine unzureichende Patientenversorgung bedingt, bei der betreuungswichtige Information dem betreuenden Personal vorenthalten geblieben wäre.

f) Per Dienstanweisung und Verschwiegenheitsverpflichtung ist festgelegt, dass Zugriffe nur anlassbezogen und zweckbezogen erfolgen. Die Einhaltung dieser Anweisung wird durch Stichprobenkontrollen im Rahmen des Rechtszulässigen überprüft. Ebenfalls finden Datenschutz-Schulungen zur Sensibilisierung der Mitarbeiter monatlich statt und es ist jeder Mitarbeiter verpflichtet, mindestens alle zwei Jahre eine Schulung zu besuchen.

g) P[…]dok-Arbeitsplätze sind NICHT öffentlich zugänglich sondern in gesicherten oder beaufsichtigten Räumen aufgestellt und überdies mit einer automatischen Bildschirmsperre versehen und können nur durch Benutzer und Passwort entsperrt werden. Mitarbeiter sind per Dienstanweisung verpflichtet, beim Verlassen des Arbeitsplatzes diesen zu sperren. Nach 10 Minuten Inaktivität erfolgt seit ca 2-3 Jahren eine automatische Sperre, um den Folgen eines Vergessens der Absperrung vorzubeugen.

Ergänzend dürfen wir anmerken, daß uns der Datenschutz ein erhebliches Anliegen ist und wir aus diesem Grund unsere Mitarbeiter regelmäßig für die Thematik sensibilisieren.

Abschließend möchten wir auch anmerken, daß wir den Anlassfall für das Tätigwerden der DSK zu kennen glauben, und der betreffenden, beschwerdeführenden Mitarbeiterin mehrfach anhand der Protokolle dargelegt haben, daß die von ihr des Lesens von Befunden bezichtigten Kolleginnen und Kollegen de facto keine Dokumente geöffnet haben und diese daher auch nicht gelesen haben. Mit den Benutzerkennungen von Kollegen wurden aber tabellarische Übersichten zu den vorhandenen Dokumenten eingesehen und es gibt in drei Fällen keinen ersichtlichen, sachlichen Grund, weshalb eine solche Einsichtnahme erfolgt ist. Zwei der drei Kollegen wurden schriftlich ermahnt; eine Kollegin befindet sich aufgrund einer äußerst schweren Erkrankung im Langzeitkrankenstand, weshalb wir vorerst von einer Befassung dieser Kollegin mit der Thematik abgesehen haben. Eine Auskunft über Zugriffe, die länger als drei Jahre zurück liegen können wir der beschwerdeführenden Mitarbeiterin trotz ihres Drängens nicht anbieten.

[…]

Da sämtliche medizinische/pflegerische Daten in Akutsituationen (auch nachts oder an Wochenenden) unverzüglich einsehbar sein müssen, um eine sachgerechte Patientenversorgung zu gewährleisten, haben grundsätzlich alle im medizinischen Akutbereich tätigen Mitarbeiter die Möglichkeit, eine (durch Protokollierung nachverfolgbare) Einsichtnahme vorzunehmen. Wiewohl wir die Einhaltung der Datenschutzbestimmungen stichprobenmäßig prüfen, dürfen und müssen wir doch davon ausgehen, daß die Mitarbeiter unseres Hauses vorschriftsgemäß verhalten - auch hinsichtlich des Datenschutzes. Einzelverfehlungen lassen sich nicht grundsätzlich ausschließen, wir haben aber den Eindruck gewinnen können, daß unsere Kolleginnen und Kollegen verstehen, daß Datenschutz vor allem Personenschutz ist und mißbräuchliche Datenverwendung längst nicht mehr als Kavalierdelikt sehen, sondern als Vergehen und als Vertrauensbruch. Auch wissen unsere Mitarbeiter, daß Missbrauch wegen der Protokollierungsmöglichkeit entdeckt bzw. nachgewiesen werden kann.

Um das wahrscheinlich kaum vorkommende, aber theoretisch dennoch mögliche Ausspionieren von Schlüsselworten zu vermeiden, wird derzeit ein System zur Identifikation mit elektronischem Fingerprint an einer unserer Abteilungen getestet.

Für weitere Auskünfte stehen wir Ihnen gerne zur Verfügung

Mit freundlichem Gruß“

Beweiswürdigung: Diese Feststellungen ergeben sich aus den zitierten Schreiben der Datenschutzkommission sowie des BKH X.

B. In rechtlicher Hinsicht folgt daraus

1. anzuwendende Rechtsvorschriften

Die relevanten Vorschriften des DSG 2000 lauten auszugsweise:

Die Verfassungsbestimmung des § 1 Abs. 1 und 2 DSG 2000 lautet samt Überschrift:

„Grundrecht auf Datenschutz

§ 1. (1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.“

§ 4 Z 1 und 2 DSG 2000 lautet:

„**§ 4.** Im Sinne der folgenden Bestimmungen dieses Bundesgesetzes bedeuten die Begriffe:

1. „Daten“ („personenbezogene Daten“): Angaben über Betroffene (Z 3), deren Identität bestimmt oder bestimmbar ist; „nur indirekt personenbezogen“ sind Daten für einen Auftraggeber (Z 4), Dienstleister (Z 5) oder Empfänger einer Übermittlung (Z 12) dann, wenn der Personenbezug der Daten derart ist, daß dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann;

2.„sensible Daten“ („besonders schutzwürdige Daten“): Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben;“

§ 14 Abs. 1 und 2 DSG 2000 lautet samt Überschrift:

„Datensicherheit

Datensicherheitsmaßnahmen

§ 14. (1) Für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, sind Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Dabei ist je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, daß die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, daß ihre Verwendung ordnungsgemäß erfolgt und daß die Daten Unbefugten nicht zugänglich sind.

(2) Insbesondere ist, soweit dies im Hinblick auf Abs. 1 letzter Satz erforderlich ist,

1. die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festzulegen,

2. die Verwendung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden,

3. jeder Mitarbeiter über seine nach diesem Bundesgesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren,

4. die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters zu regeln,

5. die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln,

6. die Berechtigung zum Betrieb der Datenverarbeitungsgeräte festzulegen und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abzusichern,

7. Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können,

8. eine Dokumentation über die nach Z 1 bis 7 getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern.

Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei der Durchführung erwachsenden Kosten ein Schutzniveau gewährleisten, das den von der Verwendung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

[…]“

§ 30 Abs. 2 und 6 DSG 2000 lautet samt Überschrift:

„Kontrollbefugnisse der Datenschutzkommission

§ 30. […]

(2) Die Datenschutzkommission kann im Fall eines begründeten Verdachtes auf Verletzung der im Abs. 1 genannten Rechte und Pflichten Datenanwendungen überprüfen. Hiebei kann sie vom Auftraggeber oder Dienstleister der überprüften Datenanwendung insbesondere alle notwendigen Aufklärungen verlangen und Einschau in Datenanwendungen und diesbezügliche Unterlagen begehren.

[…]

(6) Zur Herstellung des rechtmäßigen Zustandes kann die Datenschutzkommission, sofern nicht Maßnahmen nach den §§ 22 und 22a oder nach Abs. 6a zu treffen sind, Empfehlungen aussprechen, für deren Befolgung erforderlichenfalls eine angemessene Frist zu setzen ist. Wird einer solchen Empfehlung innerhalb der gesetzten Frist nicht entsprochen, so kann die Datenschutzkommission je nach der Art des Verstoßes von Amts wegen insbesondere

1. Strafanzeige nach §§ 51 oder 52 erstatten, oder

2. bei schwerwiegenden Verstößen durch Auftraggeber des privaten Bereichs Klage vor dem zuständigen Gericht gemäß § 32 Abs. 5 erheben, oder

3. bei Verstößen von Auftraggebern, die Organe einer Gebietskörperschaft sind, das zuständige oberste Organ befassen. Dieses Organ hat innerhalb einer angemessenen, jedoch zwölf Wochen nicht überschreitenden Frist entweder dafür Sorge zu tragen, dass der Empfehlung der Datenschutzkommission entsprochen wird, oder der Datenschutzkommission mitzuteilen, warum der Empfehlung nicht entsprochen wurde. Die Begründung darf von der Datenschutzkommission der Öffentlichkeit in geeigneter Weise zur Kenntnis gebracht werden, soweit dem nicht die Amtsverschwiegenheit entgegensteht.“

2. rechtliche Schlussfolgerungen

2.1. Der Datenschutzkommission ist die Wichtigkeit einer elektronischen Patientendokumentation und die Rolle, die diese im täglichen Dienstbetrieb einer Krankenanstalt spielt, bewusst. Jedoch hat der Betrieb einer solchen Dokumentation – schon aufgrund der Tatsache, dass Gesundheitsdaten sensible Daten im Sinne des § 4 Z 2 DSG 2000 sind – im Einklang mit den Bestimmungen des DSG 2000 – insbesondere des Grundrechts auf Datenschutz gemäß § 1 DSG 2000 – zu erfolgen. Eine Verletzung im Grundrecht auf Datenschutz wird immer dann vorliegen, wenn unbefugt oder ohne konkreten Anlass auf Patientendaten zugegriffen wird.

2.2. § 14 DSG 2000 normiert Datensicherheitsmaßnahmen, die von allen Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, zu treffen sind. § 14 Abs. 1 DSG 2000 verlangt insbesondere, dass Daten unbefugten Personen nicht zugänglich sind, wobei § 14 Abs. 1 leg. cit. auch berücksichtigt, dass Datensicherheitsmaßnahmen von jedem Auftraggeber oder Dienstleister individuell angepasst zu ergreifen sind, nämlich in Relation zur Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit. Bei einem Bezirkskrankenhaus, dessen Träger der „Gemeindeverband Bezirkskrankenhaus X." ist, der wiederum aus den Gemeinden des politischen Bezirks X. besteht […], ist in Bezug auf Datensicherheitsmaßnahmen und auf die Möglichkeit von deren Ausgestaltung ein strenger Maßstab anzulegen, zumal es sich bei den in P[…]dok gespeicherten Daten um sensible Daten handelt.

2.3. Das BKH X. gibt zwar an, dass der Zugang zu P[…]dok Mitarbeitern nur mittels eines individuellen Zugangsschlüssels eingeräumt wird, sämtliche Zugriffe protokolliert werden, P[…]dok-Arbeitsplätze nicht öffentlich zugänglich sind und per Dienstanweisung und Verschwiegenheitsverpflichtung festgelegt ist, dass Zugriffe nur anlass- und zweckbezogen erfolgen, wobei die Einhaltung dieser Dienstanweisung stichprobenartig erfolgt. Es wird jedoch auch ausgeführt, dass Ärzte, Therapeuten und Pflegekräfte grundsätzlich dieselben technischen Zugriffsmöglichkeiten haben und dass es – trotz bestehender Dienstanweisungen – drei dokumentierte Fälle gibt, in welchen ein Zugriff ohne sachlichen Grund für eine Einsichtnahme erfolgte.

Für die Datenschutzkommission steht daher fest, dass der Schutz von Patientendaten vor unbefugten und grundlosen Zugriffen mittels Dienstanweisung sowie stichprobenartiger Kontrolle von deren Einhaltung nicht ausreichend gewährleistet ist.

Es wird weiters vom BKH X. ausgeführt, dass ärztliches und nicht-ärztliches Personal grundsätzlich über dieselben technischen Zugriffsmöglichkeiten verfügen. Während es nach Ansicht der Datenschutzkommission für ärztliches Personal sowie u.a auch für das Pflegepersonal durchaus relevant und zweckmäßig sein kann, die gesamte Krankengeschichte eines Patienten zu kennen, kann derselbe Bedarf für das übrige (nichtärztliche) Personal (bspw. Therapeuten) nicht in jedem Fall als notwendig und erforderlich angesehen werden.

Der Datenschutzkommission ist bekannt, dass Patientenverwaltungssysteme in Krankenanstalten derart gestaltet werden können, dass jedem Benutzer eine eigene Rolle mit unterschiedlichen Zugriffsberechtigungen zugeordnet werden kann, wobei die Rollenverteilung auch so weit gehen kann, dass selbst ärztliches Personal nur Zugriff auf die Daten jener Patienten hat, die in jener Station behandelt werden, auf welcher der zugreifende Arzt seinen Dienst versieht (vgl. dazu bspw. das vom Allgemeinen Krankenhaus der Stadt Wien verwendete System „AKIM").

Es wird daher empfohlen, die Zugriffsberechtigungen technisch so zu gestalten, dass die zugreifende Person nur Einblick in jene Daten erhält, die für die Erfüllung ihrer Aufgaben berufsgruppenspezifisch erforderlich sind, sodass ein unbefugter und grundloser Zugriff auf Patientendaten nicht möglich ist.

3. Die Frist von zwölf Monaten erscheint in Anbetracht der Tatsache, dass die gesamte elektronische Patientenverwaltung einer grundlegenden Überarbeitung bedarf, angemessen.