TE Dsk Empfehlung 2016/5/18 DSB-D213.398/0003-DSB/2016

JUSLINE Entscheidung

Veröffentlicht am 18.05.2016

Norm

DSG 2000 §1 Abs1
DSG 2000 §1 Abs2
DSG 2000 §4 Z2
DSG 2000 §6 Abs1 Z5
DSG 2000 §7 Abs1
DSG 2000 §30 Abs3
DSG 2000 §30 Abs6
DSG 2000 §50d Abs1
StKAG §36 Abs7

Text

GZ: DSB-D213.398/0003-DSB/2016 vom 18.5.2016

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

Hinweis: Es handelt sich um zwei Erledigungen. Die eigentliche Empfehlung befindet sich unterhalb der abschließenden Erledigung.

Enderledigung

A. Verfahrensgang

1. Die Datenschutzbehörde leitete in Umsetzung des Prüfungsschwerpunktes 2015 mit Schreiben an die (K***s) vom 3. September 2015 ein amtswegiges Verfahren nach § 30 des Datenschutzgesetzes 2000 (DSG 2000) ein und übermittelte einen Fragebogen.

2. Die K***s, nahm dazu mit Schreiben vom 22. September 2015 Stellung und führte – zusammengefasst – aus, dass die Rechtsgrundlagen für die Verarbeitung von Patientendaten in den jeweiligen DVR-Meldungen angeführt seien, die Aufbewahrung patientenbezogener Daten gemäß § 36 Abs. 7 StKAG 30 Jahre bzw. 10 Jahre betrage, und technische sowie organisatorische Datensicherheitsmaßnahmen (z.B. ein durch die interne Datenschutzkommission beschlossenes Berechtigungskonzept, Zugriffsprotokollierung, keine Inanspruchnahme von Cloud-Services, keine privaten Endgeräte) vorhanden seien. Weiters wurde die Unternehmensstruktur der K***s als Rechtsträgerin von ** Krankenanstalten und ** ****pflegezentren erklärt. Es gebe eine (interne) Datenschutzkommission. Die

Datensicherheitsmaßnahmen seien in einer eigenen internen Richtlinie („Datensicherheitsvorschriften DSG 2000“) geregelt (Bemerkung: darin findet sich z.B. Inhalt der alle zwei Jahre stattfindenden Mitarbeiterbelehrung, Verweis auf Richtlinien zur Installation und Nutzung von PCs und Peripheriegeräten, Befassung der internen Datenschutzkommission bei neuen Datenverarbeitungsprojekten etc.).

3. Die Datenschutzbehörde forderte die K***s mit Schreiben vom 6. November auf, zu ergänzenden Fragen Stellung zu nehmen.

4. Die K***s nahm dazu mit Schreiben vom 24. November 2015 Stellung und übermittelte ergänzende Unterlagen.

5. Speziell zur Anwendung der im Datenverarbeitungsregister unter Auflagen registrierten mobilen Videoüberwachung gab die K***s an, dass diese einmal, konkret im Juni 2015 für zwei Wochen im Einsatz war und zwar aufgrund vermehrter Medikamentendiebstähle in der Abteilung J*** [Anmerkung Bearbeiter: genaue Bezeichnung der Einheit aus Pseudonymisierungsgründen gelöscht].

6. Mit Schreiben der Datenschutzbehörde vom 26. Februar 2016 wurde die K***s informiert, dass am 8. April 2016 eine Einschau nach § 30 Abs. 4 DSG 2000 auf den Liegenschaften xxxxxxxxxx in H*** und yyyyyyyyyy in H*** , durchgeführt und der Schwerpunkt der Einschau auf Zugriffsprotokollierungen sowie Rollenkonzepten, routinemäßiger Überprüfung der Zugriffe auf Patientendaten, Überprüfung von herangezogenen Dienstleistern, allfälliger Mehrfachnutzung von EDV-Arbeitsplätzen durch verschiedene Bedienstete sowie Übermittlung/Überlassung von Daten in Drittstaaten, und der Verwendung einer mobilen Videoüberwachung liegen werde.

7. Im Zuge dieser Einschau wurden von den Vertretern des K***s Präsentationen zu den Themen vorbereitet, Fragen dazu beantwortet, aber auch auf aktuelle Fragestellungen (ARD Morgen Magazin „simulierter Hackingangriff“ auf Medizinpumpe) eingegangen, Zugriffsberechtigungen an EDV-Arbeitsplätzen demonstriert sowie die routinemäßige Überprüfung der Zugriffe dargelegt.

8. Das Protokoll dieser Einschau wurde der K***s übermittelt. Diese nahm dazu mit Schreiben vom 3. Mai 2016 Stellung.

B. Sachverhaltsfeststellungen

Die Datenschutzbehörde geht von nachstehendem Sachverhalt aus, der sich aus den vorgelegten Stellungnahmen sowie den Ausführungen, übermittelten Präsentationsfolien und dem Resüméeprotokoll im Rahmen der Einschau am 8. April 2016 ergibt:

1. Die K***s ist Träger von ** Krankenanstalten und ** ****pflegezentren in U***.

2. Eine für alle Datenschutzangelegenheiten in der K***s zuständige Datenschutzkommission besteht aus 8 Mitgliedern und 8 Ersatzmitgliedern, die in Ausübung ihrer Tätigkeit für die Datenschutzkommission weisungsfrei gestellt sind. Die Tätigkeit der Datenschutzkommission mit einer eigenen Geschäftsstelle basiert auf einer eigenen Geschäftsordnung. Ihre Mitglieder kommen aus dem ärztlichen Bereich, dem Pflegepersonal, der Rechtsabteilung und dem Betriebsbereich. Sie werden vom Vorstand der K***s bestellt. Patienten und Bedienstete können sich jederzeit an die Datenschutzkommission wenden.

3. Zur Verwaltung von Patientendaten steht in den Krankenanstalten ein einheitliches Patientenverwaltungssystem „***Med-Doku***“ zur Verfügung; für die Landespflegezentren wird „***Med-Doku***“ im Herbst 2016 eingeführt.

4. Das Patientenverwaltungssystem „***Med-Doku***“ unterscheidet zwischen verschiedenen Berufsgruppen, aber auch innerhalb einer Berufsgruppe (z.B. ärztliches Personal: „Ärztlicher Leiter“, „Fachärzte“, „Stationsärzte“, „Turnusärzte“; Pflegepersonal: DGKP Station, DGKP Ambulanz, jeweils Pflegehelfer etc.). Für die Berechtigungsvergabe gibt es ein eigenes von der internen Datenschutzkommission genehmigtes Berechtigungskonzept, das dem Grundsatz folgt, dass Mitarbeiter nur in der Art und in jenem Umfang Daten verwenden dürfen, als dies zur Erfüllung ihrer Aufgaben notwendig ist. Jede Änderung oder Ergänzung im Berechtigungskonzept bedarf der Freigabe durch die interne Datenschutzkommission.

5. Für die konkrete Berechtigungsvergabe auf Grundlage des Berechtigungskonzeptes wird ein schriftliches Formular ausgefüllt, das vom Antragsteller und Dienststellenleiter zu unterfertigen ist. Userdaten (d.h. die Zuordnung, dass das Benutzerkennzeichen z.B. „j2ki7oc“ Dr. N*** N*** zugeordnet war) werden auch nach Ausscheiden des betreffenden Mitarbeiters aus Dokumentations- bzw. Nachweiszwecken nicht gelöscht.

6. Zugriffe auf das Patientenverwaltungssystem werden protokolliert (Aufrufe, Änderungen aber auch Ausdrucke) und zwar je Landeskrankenhaus und Patient. Die routinemäßige Überprüfung ist in der internen K***s Richtlinie RiLi 1009.8097 „Überprüfung der protokollierten Zugriffe auf Patientendaten im ***Med-Doku***, Prüfung von Verdachtsfällen, arbeitsrechtliche Konsequenzen und Informationsanspruch“ festgehalten. Jedes K***s Haus hat einmal pro Monat die Auswertung einer Stichprobe zu erstellen. Das Ergebnis ist eine Liste der potentiell unplausiblen Zugriffe (als potentiell unplausibel gelten Zugriffe, wenn der Zugreifende einer anderen Organisationseinheit angehört oder der Zugriff unter Einrechnung eines 7-tägigen Vorlaufzeitraumes und eines 28-tägigen Nachlaufzeitraums stattgefunden hat). Diese automationsunterstützt erstellte Liste unplausibler Zugriffe wird vom „Arbeitsmedizinischen Dienst“ händisch hinsichtlich der dienstlichen Notwendigkeit der Zugriffe überprüft. Ergibt sich der Verdacht, dass für einen Zugriff keine dienstliche Notwendigkeit bestand, wird der Fall an das „Personalmanagement“ weiter gereicht, das eine Stellungnahme einfordert und – im Fall, dass tatsächlich ein unbefugter Zugriff erfolgte – die Steuerung allfälliger arbeitsrechtlicher Konsequenzen übernimmt. Der bei weitem überwiegende Teil unberechtigter Zugriffe betrifft Mitarbeiter, die Abfragen im „Kollegenkreis“ vornehmen. Zugriffsprotokolle werden drei Jahre nach dem letzten Zugriff auf die Daten eines Patienten gelöscht.

7. Die Speicherung der Daten erfolgt in drei gesicherten Rechenzentren am Standort der Holding und an zwei Standorten des Klinikum H***. Der IKT-Bereich der K***s und die Rechenzentren sind ISO 270001 zertifiziert.

8. Es sind ca. 30 Dienstleister für K***s tätig. Ein Dienstleister (Blutbank) stammt aus Deutschland. Sollte ein Fernzugriff zwecks Wartung notwendig sein, erfolgt dieser über „***-Access Lösung“ mit Zwei Faktor Authentifizierung (Passwort und SMS TAN).

9. K***s betreibt bei Arbeitsplätzen mit häufigem Benutzerwechsel (etwa Stationsstützpunkte und mobiler Pflegedokumentation) sogenannte „Terminalserver“, bei denen der Bildschirm gleichsam reines „Ein- und Ausgabegerät“ ist. Dabei kann die Anmeldung an jedem beliebigen Gerät vorgenommen werden: Man legt den/die Mitarbeiterausweis/Zutrittskarte auf kleine Kartenleser, gibt das Passwort ein, worauf sich die letzte Session automatisch öffnet (z.B. die im OP-Saal verwendete Session); zieht man die Mitarbeiterkarte weg, verschwindet die Session und der Einstiegsbildschirm erscheint.

10. Zur mobilen Videoüberwachung Juni 2015 J***: Hinsichtlich der Kennzeichnung der mobilen Videoüberwachung wurde seitens K***s auf die bestehenden „Schilder“ am Spitals- bzw. Hauseingang verwiesen. Eine eigene, gesonderte Kennzeichnung während des Einsatzes der mobilen Videoüberwachung erfolgte nicht. Auf Nachfrage, ob die Auswertung ein Ergebnis gebracht habe, wird angemerkt, dass mit dem Einsatz der Videoüberwachung der Medikamentenschwund aufgehört hätte.

C. Schlussfolgerungen der Datenschutzbehörde; rechtliche Beurteilung

1. Gegenstand des vorliegenden Verfahrens ist die Frage, ob K***s gesetzliche Regelungen hinsichtlich des Schutzes personenbezogener Daten einhält, wobei der Schwerpunkt des Verfahrens auf Zugriffsprotokollierungen sowie Rollenkonzepten, routinemäßiger Überprüfung der Zugriffe auf Patientendaten, Überprüfung von herangezogenen Dienstleistern, allfälliger Mehrfachnutzung von EDV-Arbeitsplätzen durch verschiedene Bedienstete sowie Übermittlung/Überlassung von Daten in Drittstaaten lag.

Bei Daten zur Gesundheit handelt es sich um sensible Daten im Sinne des § 4 Z 2 DSG 2000, die einem besondere Schutz unterliegen.

2. Das Ermittlungsverfahren ergab, dass datenschutzrechtliche Vorgaben überwiegend eingehalten werden.

Besonders hervorzuheben sind folgende Bemühungen der K***s:

a) das Vorhandensein interner Richtlinien für Datenschutz und Datensicherheit, die von der Datenschutzkommission freigegeben werden;

b) das Vorhandensein einer internen Datenschutzkommission samt eigener Geschäftsstelle, basierend auf einer Geschäftsordnung, deren Mitglieder aus dem ärztlichen Bereich, dem Pflegepersonal, der Rechtsabteilung und EDV-Bereich kommen, die jeweils für die Ausübung ihrer Tätigkeit weisungsfrei gestellt sind;

c) die Erstellung eines jährlichen Datenschutzberichts der internen Datenschutzkommission, der dem Vorstand der K***s, den Anstaltsleitungen, dem Zentralbetriebsrat und der ****[Anmerkung Bearbeiter: Bezeichnung einer Lehr- und Ausbildungseinrichtung aus Pseudonymisierungsgründen entfernt] H*** vorzulegen ist;

d) das Vorliegen eines Rollen- und Berechtigungskonzeptes, freigegeben durch die interne Datenschutzkommission;

e) das Vorhandensein eines umfassenden Protokollierungssystems für Zugriffe aller Art;

f) die routinemäßige, monatliche Überprüfung durch automationsunterstützte Selektion unplausibler Zugriffe und dem darauf folgenden händischen „Nachgehen" dieser Zugriffe betreffend deren dienstlicher Notwendigkeit; zusätzlich auch die Beschwerdemöglichkeit von jedermann an die interne Datenschutzkommission, wenn der Verdacht von Verletzungen nach dem DSG 2000 besteht;

g) das Vorliegen eines Passwortsystems, das Komplexitätsanforderungen an ein Passwort stellt;

h) die ISO 27001 Zertifizierung aller drei räumlich getrennter Rechenzentren und des IKT Bereichs der K***s;

i) die „Terminal-Server" Lösung für den schnellen Arbeitsplatzwechsel mit Zutrittskartenleser als zusätzliche Absicherung;

j) die Überprüfung herangezogener Dienstleister und die Absicherung des fallweisen Remote-Zugriffs mit Zwei Faktor Authentifizierung (SMS TAN und Passwort);

k) die Betrauung der internen Revision mit der Durchführung von Netzwerkaudits, simulierten Hackerangriffen und der Sensibilisierung im Mitarbeiterbereich für dieses Thema;

l) ein konsequentes „Rollenkonzept" und ein gelebtes „Rollenverständnis" dahingehend, dass es einem Mitarbeiter, wenn er Patient ist, nicht gestattet ist, seine „eigenen" Daten abzufragen, sondern dass er dafür den „den normalen Geschäftsprozessweg als Patient zur Erlangung der Information gehen muss";

3. Hinsichtlich der Nichtdurchführung einer Löschung ehemaliger User und der Kennzeichnung der mobilen Videoüberwachung war die beiliegende Empfehlung auszusprechen.

EMPFEHLUNG

Die Datenschutzbehörde spricht aus Anlass der Überprüfung der m.b.H. (K***s) folgende Empfehlung aus:

1. Die K***s möge geeignete Maßnahmen ergreifen, damit Nutzerprofile ehemaliger Bediensteter nicht zeitlich unbefristet in Datenverarbeitungssystemen gespeichert bleiben.

2. Die K***s möge bei einer allfälligen künftigen (mobilen) Videoüberwachung dies in geeigneter Weise - und zwar in unmittelbarer Nähe - kennzeichnen und für jedermann ersichtlich so montieren, dass jeder potentiell Betroffene, der sich einem überwachten Objekt nähert, die Möglichkeit hat, der Videoüberwachung auszuweichen.

3. Für die Umsetzung von Spruchpunkt 1 dieser Empfehlung wird eine Frist von sechs Monaten gesetzt.

Rechtsgrundlagen: §§ 1, 6, 30, 50d des Datenschutzgesetzes 2000 – DSG 2000, BGBl. I Nr. 165/1999 idgF.

Gründe für diese Empfehlung

A. Verfahrensgang

Im Zuge des vorliegenden amtswegigen Prüfverfahrens, welches der Umsetzung des Prüfungsschwerpunktes 2015 diente, wurden unter anderem

- Fragen zur Vorgangsweise bei einem Austritt eines Mitarbeiters und
- zu den Umständen der mobilen Videoüberwachung gestellt.

K***s gab an, dass bei einem Austritt das Nutzerprofil des austretenden Nutzers deaktiviert werde, sodass dieser keinen Zugriff mehr auf Daten habe. Es erfolge jedoch keine Löschung der Zugangsdaten des Nutzers, um auch nach dessen Austritt dessen Tätigkeiten im Datenverarbeitungssystem nachvollziehen und dokumentieren zu können.

Betreffend der mobilen Videoüberwachung wegen Medikamentendiebstahls in den Räumlichkeiten der Abteilung für J*** im Juni 2015 verwies K***s auf die bestehenden Schilder am Spitals- bzw. Hauseingang. Eine eigene, gesonderte Kennzeichnung der mobilen Videoüberwachung erfolgte nicht.

B. In rechtlicher Hinsicht folgt daraus:

1. Nutzerdaten:

a) Aufgrund des oben angeführten Sachverhalts steht fest, dass Nutzer auch nach deren Austritt aus der K***s in Datenverarbeitungssystemen insoweit zeitlich unbefristet gespeichert bleiben, als lediglich deren Zugangsberechtigung deaktiviert wird, Tätigkeiten des Nutzers aber weiterhin nachvollzogen werden können.

Die Datenschutzbehörde anerkennt, dass dies insofern erforderlich sein könnte, um auch nach dem Austritt eines Mitarbeiters nachvollziehen zu können, welche Handlungen der Nutzer im System gesetzt hat. Auch erscheint dies erforderlich, um Behandlungen von Patienten, die von einem Nutzer in das Patientenverwaltungssystem einzutragen sind, lückenlos zu dokumentieren und den Behandlungsverlauf somit nachweisbar darlegen zu können.

b) Jedoch widerspricht eine zeitlich nicht befristete Speicherung personenbezogener Daten dem Grundsatz des § 6 Abs. 1 Z 5 DSG 2000.

Auch der EGMR hat in seiner Rechtsprechung ausgesprochen, dass die unbegrenzte bzw. zeitlich nicht näher eingeschränkte Speicherung personenbezogener Daten eine Verletzung von Art. 8 EMRK darstellt (vgl. dazu bspw. das Urteil vom 18. April 2013, M.K. gg. Frankreich, Nr. 19522/09, Rz 35 f mwN). Auch wenn sich die zitierte Rechtsprechung auf strafrechtlich relevante Daten bezieht, so sind die darin dargelegten Grundsätze nach Ansicht der Datenschutzbehörde allgemein auf die Verwendung personenbezogener Daten anzuwenden.

c) Es ist somit Sache eines Auftraggebers eine Frist vorzusehen, die einerseits das Bedürfnis der Dokumentation der Handlungen ehemaliger Nutzer aber auch die Vorgabe der zeitlich begrenzten Speicherung personenbezogener Daten berücksichtigt, und nach deren Ablauf personenbezogene Daten ehemaliger Nutzer gelöscht werden.

2. (Mobile) Videoüberwachung

Eingangs wird darauf hingewiesen, dass nach Auffassung der Datenschutzbehörde Videoüberwachungen grundsätzlich nicht intentional verdeckt durchgeführt werden dürfen und in örtlicher Nähe geeignet zu kennzeichnen sind, da andernfalls der Intention des Gesetzgebers aus der Kennzeichnung gemäß § 50d DSG 2000 – nämlich, dass diese dem potentiell Betroffenen ein Ausweichen ermöglichen soll – nicht Rechnung getragen wäre.

Eine verdeckte Videoüberwachung zum Zweck des Nachweises von Medikamentenschwund ist demnach von den Bestimmungen des DSG 2000 nicht gedeckt.

Keine Kennzeichnungsverpflichtung besteht lediglich bei Videoüberwachungen im Rahmen der Vollziehung hoheitlicher Aufgaben, die nach § 17 Abs. 3 DSG 2000 von der Meldepflicht ausgenommen sind, was vorliegend jedoch nicht der Fall ist.

Es ist somit Aufgabe eines Auftraggebers, eine Videoüberwachung derart zu kennzeichnen, dass der Vorgabe des § 50d DSG 2000 Rechnung getragen wird.

3. Empfehlung

Es war folglich gemäß § 30 Abs. 6 DSG 2000 zur Herstellung des rechtmäßigen Zustandes die obige Empfehlung zu erteilen. Die Frist scheint für die Umsetzung dieser Empfehlung angemessen.

Schlagworte

Empfehlung, Amtswegiges Prüfverfahren, Krankenanstalt, Trägerorganisation, Speicherdauer von Nutzerprofilen, Videoüberwachung, Kennzeichnung, Ausweichmöglichkeit

Anmerkung

Es handelt sich um zwei Erledigungen (Enderledigung und Empfehlung) unter einer Geschäftszahl (GZ). Beide sind im RIS zu einem Dokument zusammengefasst worden.

European Case Law Identifier (ECLI)

ECLI:AT:DSB:2016:DSB.D213.398.0003.DSB.2016

Zuletzt aktualisiert am

30.05.2016