TE Dsk Empfehlung 2017/2/1 DSB-D213.469/0006-DSB/2016

JUSLINE Entscheidung

Veröffentlicht am 01.02.2017

Norm

DSG 2000 §1 Abs1
DSG 2000 §1 Abs2
DSG 2000 §6 Abs1 Z1
DSG 2000 §6 Abs1 Z2
DSG 2000 §6 Abs1 Z3
DSG 2000 §6 Abs1 Z5
DSG 2000 §7 Abs1
DSG 2000 §8 Abs1 Z2
DSG 2000 §17 Abs1
DSG 2000 §30 Abs3
DSG 2000 §30 Abs6
DSG 2000 §18 Abs2 Z2
Tir KAG §15 Abs1 litd

Text

GZ: DSB-D213.469/0006-DSB/2016 vom 1.2.2017

[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.

Mitteilung; Enderledigung

A. Verfahrensgang

1. Die Datenschutzbehörde leitete in Umsetzung des Prüfungsschwerpunktes 2015/2016 mit Schreiben an die E***-Kliniken Gesellschaft m.b.H. (im Folgenden kurz: E***-Kliniken) vom 1. Juni 2016 ein amtswegiges Verfahren nach § 30 Abs. 3 des Datenschutzgesetzes 2000 – DSG 2000 ein und übermittelte einen Fragebogen.

2. Die E***- Kliniken nahm dazu mit Schreiben vom 27. Juni 2016 Stellung und führte – zusammengefasst – aus, dass sie unter ihrer datenschutzrechtlichen Verantwortung als Auftraggeberin [mehrere] Krankenanstalten [Angaben zu Art, Zahl und Standorten der Krankenanstalten aus Pseudonymisierungsgründen entfernt] betreibe und auf ausreichender

gesetzlicher Grundlage (insbesondere des Tir KAG) Daten, insbesondere zur Führung von Krankengeschichten, zu Abrechnungszwecken, zur Personalführung und für betriebswirtschaftliche Anwendungen, verarbeite. Primäre Betroffenenkreise seien Patienten und Mitarbeiter. Sowohl Krankengeschichten als auch Personalakten würden teilweise, wenn auch sukzessiv in der Bedeutung abnehmend, noch als Papierakten geführt. Die Geschäftsführung der E***- Kliniken werde in datenschutzrechtlichen Fragen im Tagesgeschäft durch 2 Datenschutzbeauftragte und in Grundsatzfragen durch eine mindestens zweimal jährlich tagende interne Datenschutzkommission beraten. Die Befugnisse des Personals seien intern näher geregelt (u.a. durch Verschwiegenheits- und Datenschutzerklärungen abgesichert), wobei technisch ein System rollen- und aufgabenspezifischer Zugriffsberechtigungen (von der Datenschutzkommission freigegebene „Berechtigungssysteme“) umgesetzt werde. Ein Zuwiderhandeln gegen gesetzliche und interne Beschränkungen bei der Datenverwendung ziehe disziplinäre Folgen nach sich. Kern der Patientendatenverwaltung sei das Klinische Informationssystem (kurz: KIS). Das KIS würde u.a. monatliche Auswertungen zu Querzugriffen (von Mitarbeitern anderer Abteilungen als jener, die einen Patienten behandle) liefern, die geprüft würden. Daten in Krankengeschichten würden aktualisiert (unter nachvollziehbarer Erfassung der verantwortlichen Mitarbeiter), als unrichtig oder nicht mehr aktuell erkannte Daten aber nicht vollständig gelöscht sondern ersetzt und für Archivzwecke umklassifiziert. § 15 Tir KAG schreibe bei Krankengeschichten zu stationären Aufenthalten eine mindestens dreißigjährige, sonst eine zehnjährige Speicherdauer vor. Patientendaten würden auf Grund gesetzlicher Vorschriften insbesondere an die Sozialversicherungsträger übermittelt, sonst auf Grund von Einzelzustimmung der Betroffenen (z.B. Arztbriefe an niedergelassene Ärzte). Datenübermittlungen an Empfänger in Drittstaaten (außerhalb des EWR) würden nur auf Grundlage von Einzelzustimmungen erfolgen. Die Videoüberwachung an den Standorten der E***- Kliniken sei 2015 neu und erweitert zur Eintragung im DVR gemeldet worden.

3. Die Datenschutzbehörde forderte die E***- Kliniken mit Schreiben vom 20. September 2016 auf, zu ergänzenden Fragen Stellung zu nehmen.

4. Die E***- Kliniken nahm dazu mit Schreiben vom 4. Oktober 2016 Stellung.

5. Mit Schreiben der Datenschutzbehörde vom 11. November 2016 wurde die E***- Kliniken informiert, dass am 29. November 2016 eine Einschau nach § 30 Abs. 4 DSG 2000 im a.ö. Krankenhaus – ***kliniken B*** (kurz: ***kliniken B***), R***str. ****, **** B***, durchgeführt und der Schwerpunkt der Einschau auf Zugriffsprotokollierungen sowie Rollenkonzepten, routinemäßiger Überprüfung der Zugriffe auf Patientendaten, Überprüfung von herangezogenen Dienstleistern und allfälliger Mehrfachnutzung von EDV-Arbeitsplätzen durch verschiedene Bedienstete liegen werde.

6. Im Zuge dieser Einschau wurden von den Vertretern der E***- Kliniken die Fragen dazu beantwortet, entsprechende Konzepte vorgelegt, Zugriffsberechtigungen an EDV-Arbeitsplätzen demonstriert sowie die Überprüfung der Zugriffe dargelegt. Weiters wurde auch in der Sicherheitszentrale der ***kliniken B*** in die durchgeführte Videoüberwachung Einschau genommen.

7. Der Bericht über diese Einschau wurde der E***- Kliniken übermittelt. Diese nahm dazu mit Schreiben vom 23. Dezember 2016 Stellung.

B. Sachverhaltsfeststellungen

Die Datenschutzbehörde geht von nachstehendem Sachverhalt aus, der sich aus den vorgelegten Stellungnahmen sowie den Ausführungen im Rahmen der Einschau am 29. November 2016 ergibt:

1. Die E***- Kliniken ist (Stand: 24. Jänner 2017) Trägerin folgender Krankenanstalten im Land Tirol:

- a.ö. Krankenhaus – ***kliniken B***

- a.ö. Krankenhaus O***

[Angaben zu Art, Zahl und Standorten der weiteren Krankenanstalten aus Pseudonymisierungsgründen entfernt]

2. Zur Verwaltung von Patientendaten stehen in den genannten Krankenanstalten mehrere Datenverwaltungssysteme (Applikationen) zur Verfügung, die aus Software-Paketen verschiedener Unternehmen gebildet werden, was u.a. auf die Übernahme des früheren ***krankenhauses O*** zurückgeht. Den Kern der Patientendatenverwaltung bildet dabei das KIS. Das System KIS (Klinisches Informationssystem, http://www.t***.com/Produkte_und_Services/*** Bezeichnung der Software laut Bildschirmansicht auch „T***Clinical“) ist von einem amerikanischen Hersteller (T***

Corporation, mit Hauptsitz in *****, USA). Neben KIS/T***Clinical wird auch (z.B. in der Chirurgie im KH O***) W***DOC von W*** (http://www.w***.at/produkte-services/***, W*** Healthcare Software Ges.m.b.H., ****, office@w***.at) eingesetzt. Die darüber liegende allgemeine Benutzerebene ist das Betriebssystem MS-Windows 7 mit entsprechenden Nutzerprogrammen.

3. Für Host-Dienstleistungen steht auch ein externes Rechenzentrum zur Verfügung, das auf Kunden mit hohem Sicherheitsbedarf wie Banken und Spitäler spezialisiert ist. Ein System ist in B*** und ein anderes in O***. Die zwei Rechenzentren sind mit zwei exklusiven Standleitungen verbunden, die nur von ihnen genutzt werden. Die Leitungsführung verläuft nördlich und südlich [geografische Bezeichnung aus Pseudonymisierungsgründen entfernt] wegen der Hochwasserproblematik. Das zweite Rechenzentrum mit Spiegelung der Daten liegt auf einer anderen Höhenlage.

4. Die Medikation ist noch nicht in strukturierter Form abgebildet, sie wird ebenso wie Temperaturverlauf/Fieberkurve, Blutdruckwerte etc. am Behandlungsort erfasst. Erst dann wird diese Information gegebenenfalls in die (elektronische) Krankengeschichte übertragen. Mit neuer Software soll diese Lücke in Zukunft abgedeckt werden (W***DOC hat bereits eine entsprechende Funktion).

5. Die E***- Kliniken orientieren sich für Sicherheitszwecke seit 2011 an den Standards der Normen laut ISO 27000-Reihe. Die Firma K*** hat eine Analyse durchgeführt, eine förmliche Zertifizierung ist für 2018 geplant.

6. Es gibt zwei definierte Standardarbeitsplätze, einen im Verwaltungsbereich, bei dem die individuelle Authentifizierung mit Benutzername und Passwort erfolgt. Einen zweiten Standardarbeitsplatz gibt es für mehrfach genutzte Geräte in der Station/Ambulanz/Leitstelle. Hier erfolgt Zugang über eine allgemeine Authentifizierung auf „Microsoftebene“, dann wieder mit Benutzernamen und Passwort (insbesondere KIS). Benutzername und Passwort stellen die Zugangsbarrieren dar, Schlüsselkarten oder sonstige Token stehen nur für Raumzugänge in Verwendung. Eine Authentifizierung mit Karte ist geplant.

7. Ein Passwort besteht aus 8 Zeichen, eine Änderung erfolgt 1x jährlich. Die Begründung für diese relativ lange Zeitspanne: es soll vermieden werden, dass das Passwort irgendwo am Arbeitsplatz aufgeschrieben wird, was erfahrungsgemäß passiert, wenn man öfter das Passwort ändern müsste. Passwortänderungen: Die Serversysteme sind gekoppelt an die MS-Office Directive (= eigenes Portal für Benutzerverwaltung). Eine Änderung des Passworts auf jedem einzelnen System wäre zu zeitaufwändig. Mit einem neuen Passwort werden zeitgleich alle Anwendungen umgestellt. Es gibt auch eine Dienstanweisung, den Bildschirm zu sperren. Mittlerweile achten die Mitarbeiter darauf, dass Geräte nicht offen sind. Da im KIS sensible Daten verarbeitet werden, loggt das System hier User nach längstens 20 Minuten automatisch aus. Außerdem sperrt sich der Bildschirm bei Nichtbenutzung automatisch nach 30 Minuten (auf MS Win 7-Ebene).

8. Es gibt im KIS verschiedene Suchfunktionen, z.B. nach „Patient“. Bei der Funktion „Aktenzugriff“ sieht man, wer aller auf eine Person zugegriffen hat. Jeder Patient kann Zugriffe auf seine Akte in ausgedruckter Form beantragen; eine Datenschutzvertrauensperson überprüft einmal pro Monat die Querzugriffe.

9. Es gibt keine Zahl, wie viele externe unberechtigte Zugriffsversuche es gegeben hat. Derzeit ist aber kein Vorfall bekannt, bei dem die Firewall durchdrungen worden wäre.

10. Das Berechtigungssystem (siehe auch Beilage./B zum Bericht über die Einschau am 29.11.2016) bildet ein Rollenverständnis ab, geht jedoch davon aus, dass nicht jede Arbeit, die Zugang zu sensiblen Daten bedingt, von einem Arzt erledigt werden muss. Ein behandelnder Arzt erstellt ein KIS-Dokument (z.B. Befund, OP-Bericht), der Oberarzt signiert es elektronisch, dann wird das Dokument freigegeben. Der Angehörige einer Usergruppe (z.B. Schreibkraft, Arzt) hat jeweils die Rechte, die er zum Arbeiten braucht, was aber auch bedeuten kann, dass die Schreibkraft, die einen Befund schreibt, Zugang zu sensiblen Daten hat. Patienten können aber auch verschiedenen Abteilungen zugewiesen werden. Bei jeder Abteilung muss der Arzt alle Befunde in einer Übersicht zusammenfassen können. Dies ist im Modus des Berechtigungssystems eingebaut. In diese Entscheidung war die interne Datenschutzkommission eingebunden. Die Gewährleistung einer hohen Behandlungsqualität steht im Vordergrund. Es gibt 9 Sicherheitsstufen mit verschiedenen Rollen. Das Berechtigungssystem ist sehr komplex. Es sind nur die Patienten sichtbar, die auf der Station behandelt werden.

11. Eine Einschau (Station Neurologie *2) hat keine Widersprüche zur Darstellung laut oben 7. bis 10. ergeben.

12. Die Kontrollen der Zugriffsberechtigung erfolgen teils systematisch (Querzugriffe, Überprüfung durch Datenschutzvertrauenspersonen oder Abteilungsleiter an Hand automatischer Auswertungen), teils auf Basis von Zufallskontrollen. Die Mitarbeiter können ihre eigenen und die Krankengeschichten ihrer Patienten überprüfen und sind aufgefordert, Auffälligkeiten zu melden. Stichprobenkontrollen an Hand zufällig ausgewählter Krankengeschichten erfolgen nicht. Die Zugriffe auf Patientendaten werden protokolliert und sind für andere Zugriffsberechtigte sichtbar.

13. In den letzten fünf Jahren wurden sechs Verwarnungen gegen Mitarbeiter wegen unautorisierter Datenzugriffe ausgesprochen.

14. Auskunftsverlangen kommen im Bereich der E***- Kliniken eher selten vor (ein Auskunftsverlangen nach § 26 DSG 2000 in fünf Jahren). Oft ergeht die Rückfrage, was der Anfragende möchte. Meistens liegt ein Konfliktfall um die Behandlung vor, manchmal wird auch eine Abänderung bzw. Richtigstellung von Befunden u.a. verlangt. Das System „T***Clinical“ startet nach einer gewissen Zeit die Langzeitarchivierung. Ein pdfA-Dokument kann nicht mehr verändert werden. Es können aber Änderungen angemerkt oder neue Dokumente erstellt werden. Bei einer konkreten Anfrage wird um Mitwirkung des Anfragenden ersucht. Häufiger sind Behauptungen, jemand habe zu Unrecht zugegriffen. Dann wird eine nähere Überprüfung unter Hinzuziehung von IT-Spezialisten hinzugezogen. Es gibt ein Formular für Betroffene mit Erläuterungen.

15. Bei einem Austritt von Mitarbeitern wird deren Benutzerprofil deaktiviert, es bleibt jedoch dauerhaft gespeichert.

16. Der internationale elektronische Datenverkehr der E***- Kliniken reicht nicht über den EWR hinaus und erfordert daher keine Genehmigungen der Datenschutzbehörde. Grundsätzlich werden bei ausländischen Patienten Befunde und Bildmaterial (sehr häufig betrifft dies Verletzte nach Ski-Unfällen) gleich dem Patienten mitgegeben. Eine Übermittlung erfolgt nur im Auftrag des Patienten bzw. mit dessen Zustimmung. Daten werden auch per Post nachgereicht, wenn ein Patient darum ersucht. Eine elektronische Übermittlung erfolgt nur im Auftrag des Patienten. Manchmal benötigt ein ausländischer Versicherer weitere Unterlagen. Dies läuft immer über den Patienten, der die Verfügungsgewalt über seinen Patientenakt hat. Rechtsgrundlage ist § 11a VersVG.

17. Die E***- Kliniken eröffnet einer Zahl unterschiedlicher Dienstleister (rund 141 personifizierte Zugänge), die sich vertraglich zur Einhaltung gesetzlicher und interner Datenschutzvorschriften verpflichten, für Service- und Wartungszwecke bereichsspezifischen Zugang zu ihren Datenverarbeitungssystemen. Zugang erfolgt mit Benutzername und Passwort. Es ist eine spezielle Internetverbindung erforderlich (Zugang mittels VPN durch die Firewall)

18. Die E***- Kliniken hat seit 1999 ein mehrstufiges System zur internen Gewährleistung von Datenschutz und Datensicherheit. Die derzeit freiwillig von der Geschäftsführung bestellten Datenschutzbeauftragten (Mag. Markus C***, MSc, und Drin. Karin L***), die sich gegenseitig vertreten, haben Zugang zur Geschäftsführung und beraten diese und alle Abteilungen. Ihnen obliegt auch die Durchführung entsprechender Schulungen des Personals. Die Datenschutzbeauftragten werden bei allen operativen Fragen des Datenschutzes – die Entscheidungshoheit obliegt der Geschäftsführung – eingebunden. Sie berichten der internen Datenschutzkommission der E***- Kliniken. Diese besteht – neben den Datenschutzbeauftragten – aus entsandten Mitgliedern verschiedener Leitungsorgane und Gremien sowie des Betriebsrats (ca. 15 Mitglieder). Sie tagt mindestens zweimal pro Jahr und legt allgemein verbindliche Reglementierungen (z.B. das geltende KIS-Berechtigungssystem) fest bzw. gibt diese frei. Daneben gibt es noch Datenschutzvertrauenspersonen auf Abteilungs- bzw. Klinikebene, zu deren speziellen Aufgabe die Überprüfung der „Querzugriffe“ zählt.

19. Derzeit kommt diesen Personen und Gremien keine besonders garantierte unabhängige Stellung im Sinne des Art. 38 der Verordnung (EU) Nr. 2016/679 – Datenschutz-Grundverordnung (DSGVO) zu. Die E***- Kliniken werden mit Wirksamwerden der DSGVO dieses interne System den entsprechenden Vorgaben anpassen.

20. Das a.ö. Krankenhaus – ***kliniken B*** verfügt über ein umfassendes Videoüberwachungssystem für Sicherheitszwecke mit einer Vielzahl von Kameras mit und ohne Bildaufzeichnung (siehe Beilage./F zum Bericht über die Einschau am 29.11.2016). Die Einschau hat ergeben, dass keine Behandlungsräume überwacht werden und öffentliche Flächen gegebenenfalls durch eine „Maskierung“ ausgespart bzw. abgedeckt werden. Mit der Belegschaft wurde eine Betriebsvereinbarung abgeschlossen. Eine entsprechende Datenanwendung wurde registriert (DAN: 0*4*1*8/015) Die Auswertung von Bilddaten erfolgt nach dem 4-Augenprinzip. Es besteht eine Protokollierungsdatei (siehe Beilage./H zum Bericht über die Einschau am 29.11.2016), in der gegebenenfalls auch personenbezogene Daten

(z.B. Namen ausgeforschter Verdächtiger und Opfer) erfasst werden.

C. Schlussfolgerungen der Datenschutzbehörde; rechtliche Beurteilung

1. Gegenstand des vorliegenden Verfahrens ist die Frage, ob die E***- Kliniken 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 Videoüberwachung lag.

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

3. Das Ermittlungsverfahren ergab, dass datenschutzrechtliche Vorgaben im überwiegenden Ausmaß eingehalten werden. Bei der Einschau am 29. November 2016 sind keine Missstände aufgefallen, die zwingend Anlass für eine nähere (sachverständige) Überprüfung gegeben hätten.

4. Besonders positiv hervorzuheben sind folgende Maßnahmen der E***- Kliniken:

a. die Bestellung von Datenschutzbeauftragten,

b. das Vorliegen eines Rollen- und Berechtigungskonzeptes,

c. das Vorhandensein von zwei räumlich getrennten Rechnerstandorten mit der Fähigkeit zur Redundanz und entsprechend gesicherten Leitungsverbindungen.

5. Hinsichtlich der Nichtdurchführung einer Löschung ehemaliger User, sowie betreffend eine Verbesserung der Kontrolle der Zugriffe auf Patientendaten (einschließlich der offenen Protokollierung) und zur Meldung der Führung einer Datenanwendung betreffend Auswertung der Videoüberwachung war jedoch die beiliegende Empfehlung auszusprechen.

EMPFEHLUNG

Die Datenschutzbehörde spricht aus Anlass der Überprüfung der E***- Kliniken Gesellschaft m.b.H. (E***- Kliniken) folgende Empfehlung aus:

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

2. Die E***- Kliniken möge geeignete zusätzliche Maßnahmen ergreifen, insbesondere ein System stichprobenartiger Kontrollen der Verwendung der Daten nach dem Zufallsprinzip bestimmter Patienten einführen, damit eine rechtmäßige Verwendung der Patientendaten im Sinne des § 6 Abs. 1 Z 1, Z 2 und Z 3 DSG 2000 sichergestellt ist.

3. Die E***- Kliniken möge im Wege einer Betriebsvereinbarung die Zustimmung der Betroffenen für die „offene Protokollierung“ der Daten (Sichtbarkeit von Zugriffen auf Patientendaten durch andere berechtigte Nutzer) einholen.

4. Die E***- Kliniken möge dafür sorgen, dass in oder ergänzend zur DAN:0*4*1*8/015 (Videoüberwachung) die Protokollierung der Auswertung der Videoüberwachung im Anlassfall mit allen dabei erfassten Datenarten im Datenverarbeitungsregister (DVR) offengelegt wird.

5. Für die Umsetzung der Punkte 1. bis 3. dieser Empfehlung wird eine Frist von sechs Monaten, für jene von Punkt 4. eine Frist von drei Monaten gesetzt.

Rechtsgrundlagen: §§ 1, 6, 8, 17, 30 und 50a Abs. 5 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 2015/2016 diente, wurden auch Fragen zur Vorgangsweise bei einem Austritt eines Mitarbeiters und zur Überprüfung der Zugriffsberechtigungen gestellt sowie eine Einschau vorgenommen, bei der auch der Umfang der

Videoüberwachung überprüft worden ist.

Die Feststellungen der Datenschutzbehörde sind in der angeschlossenen abschließenden Erledigung festgehalten.

B. In rechtlicher Hinsicht folgt daraus:

1. Aufgrund des festgestellten Sachverhaltes steht fest, dass bei einem Austritt die Nutzerberechtigungen des austretenden Nutzers deaktiviert werden, sodass dieser keinen Zugriff mehr auf Daten hat. Es erfolgt jedoch keine Löschung des Nutzers, da nach Ansicht der E***- Kliniken die Datenverwendung nachvollziehbar bleiben müsse (z.B. im Fall von Schadenersatzansprüchen). Nutzer bleiben insoweit auch nach deren Austritt aus der E***- Kliniken in Datenverarbeitungssystemen zeitlich unbefristet gespeichert, als vorangegangene Tätigkeiten des Nutzers 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.

2. 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.

§ 15 Abs. 1 lit d) Tir KAG bezieht sich, wie schon aus der Überschrift abzuleiten ist, auf Patientendaten, nämlich die „Führung von Krankengeschichten und sonstigen Vormerkungen“. Eine Pflicht zur zeitlich befristeten längeren (dreißigjährigen) oder gar unbefristeten Verarbeitung von Nutzerdaten kann daraus nicht abgeleitet werden.

3. 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.

4. Es entspricht dem Amtswissen der Datenschutzbehörde, dass es in Krankenanstalten immer wieder zu unberechtigten Zugriffen auf Patientendaten durch eigene Mitarbeiter kommt. Ein unberechtigter Zugriff wird regelmäßig dann vorliegen, wenn ohne dienstliche Notwendigkeit (etwa aus Interesse) auf Patientendaten zugegriffen wird. Derartige Zugriffe treten insbesondere – wie Überprüfungen der Datenschutzbehörde ergeben haben – dann auf, wenn bspw. eigene Mitarbeiter, deren Angehörige oder öffentlich bekannte Personen sich einer Behandlung in der Krankenanstalt unterziehen.

Aufgrund des Ergebnisses des Prüfverfahrens steht fest, dass E***- Kliniken ein System zur Überprüfung von Zugriffen auf Patientendaten entwickelt und umgesetzt hat. Dieses verlässt sich jedoch nach Ansicht der Datenschutzbehörde in einem zu hohen Maß auf Zufallsfunde sowie auf das Ergebnis der routinemäßigen Sichtung von Querzugriffen.

Gemäß § 6 Abs. 1 Z 1 DSG 2000 dürfen Daten nur nach Treu und Glauben und auf rechtmäßige Weise verwendet werden.

Gemäß § 6 Abs. 1 Z 2 DSG 2000 dürfen Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden.

Gemäß § 6 Abs. 1 Z 3 DSG 2000 dürfen Daten nur soweit sie für den Zweck der Datenanwendung wesentlich sind, verwendet werden und über diesen Zweck nicht hinausgehen.

Gemäß § 6 Abs. 2 DSG 2000 trägt der Auftraggeber bei jeder seiner Datenanwendungen die Verantwortung für die Einhaltung der in Abs. 1 genannten Grundsätze; dies gilt auch dann, wenn er für die Datenanwendung Dienstleister heranzieht.

Die E***- Kliniken sollte daher ergänzend ein System von routinemäßigen stichprobenartigen Kontrollen hinsichtlich möglich unberechtigter Zugriffe entwickeln um sicherzustellen, dass die Verwendung von Patientendaten auf

rechtmäßige Weise im Sinne des § 6 Abs. 1 Z 1, Z 2 und Z 3 DSG 2000 erfolgt (siehe dazu auch die Empfehlung der Datenschutzbehörde vom 23. Mai 2016, GZ DSB-D210.783/0004-DSB/2016).

5. Aufgrund des festgestellten Sachverhaltes steht fest, dass KIS-Benutzer im Rahmen der zugeteilten Rolle und der dadurch erlangten Berechtigung auf die Protokolldaten „ihrer" Patienten zugreifen können. Da im Zuge dieser „offenen Protokollierung" die Namen aller Mitarbeiter angezeigt werden, die ebenfalls Teil der Bearbeitungshistorie einer Patientenakte sind, sind somit schutzwürdige Geheimhaltungsinteressen dieser Mitarbeiter betroffen. Bei einer derartigen Verwendung nicht-sensibler Daten sind die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nur in den unter § 8 Abs. 1 DSG 2000 festgelegten Fällen nicht verletzt.

Diese Praxis dient zwar einerseits in berücksichtigungswürdiger Weise der internen Kontrolle, bedarf aber andererseits als Eingriff in Geheimhaltungsinteressen der betroffenen Bediensteten einer stärkeren rechtlichen Absicherung.

Um sicherzustellen, dass es zu keiner Verletzung der schutzwürdigen Geheimhaltungsinteressen bei Verwendung von Protokolldaten kommt, ist daher im Rahmen einer Betriebsvereinbarung die Zustimmung der Betroffenen gem. § 8 Abs. 1 Z 2 DSG 2000 einzuholen (siehe dazu auch die Empfehlung vom 30. Jänner 2017, GZ DSB-D213.470/0002-DSB/2017, noch nicht im RIS).

6. Zur Protokollierung der Auswertung der Videoüberwachung ist folgendes festzuhalten:

Grundsätzlich hat die Datenschutzbehörde bei ihrer Einschau eine systematisch durchdachte, dem Gesamteindruck nach gesetzmäßig organisierte Videoüberwachung für Sicherheitszwecke vorgefunden.

Die Führung einer Protokollierungsdatei über die Ergebnisse der Auswertung der Bilddaten im Anlassfall, in die auch Namen von Verdächtigen oder Opfern eines gefährlichen Angriffs eingetragen werden, bildet aber, je nach Betrachtungsweise, eine Erweiterung der gemeldeten DAN: 0*4*1*8/015 oder eine eigene Datenanwendung, unterliegt aber jedenfalls der Meldepflicht gemäß § 17 Abs. 1 und § 18 Abs. 2 Z 2 DSG 2000 (Verwendung strafrechtlich relevanter Daten).

Eine entsprechende Meldung wird daher nachzuholen sein.

7. Es war folglich gemäß § 30 Abs. 6 DSG 2000 zur Herstellung des rechtmäßigen Zustandes die obige Empfehlung zu erteilen. Eine Frist von drei bzw. sechs Monaten scheint für die Umsetzung dieser Empfehlung angemessen.

Schlagworte

Empfehlung, Amtswegiges Prüfverfahren, Krankenanstalt, Trägerorganisation, Datenverwendung, Meldepflicht, Kontrollmaßnahmen, Prüfungsroutine, Betriebsvereinbarung, Speicherdauer von Nutzerprofilen, Videoüberwachung

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:2017:DSB.D213.469.0006.DSB.2016

Zuletzt aktualisiert am

20.02.2017