GZ: DSB-D213.470/0002-DSB/2017 vom 30.1.2017

[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 Enderledigung.

Mitteilung; Enderledigung

A. Verfahrensgang

1. Die Datenschutzbehörde leitete in Umsetzung des Prüfungsschwerpunktes 2016 mit Schreiben an die Gemeinnützige Y*** Landeskliniken Betriebsgesellschaft mbH (X***) vom 1. Juni 2016 ein amtswegiges Verfahren nach § 30 des Datenschutzgesetzes 2000 – DSG 2000 ein und übermittelte einen Fragebogen.

2. Die X*** nahm dazu mit Schreiben vom 15. Juli 2016 Stellung und führte – zusammengefasst – in einem ersten Abschnitt zunächst Näheres zu Organisation und Arbeitsweise der X*** aus, legte in weiterer Folge die Einhaltung datenschutzrechtlicher Vorschriften dar und zeigte in einem dritten Abschnitt die konkreten Datenanwendungen auf.

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

4. Die X*** nahm dazu mit Schreiben vom 17. Oktober 2016 Stellung.

5. Mit Schreiben der Datenschutzbehörde vom 11. November 2016 wurde die X*** informiert, dass am 29. November 2016 eine Einschau nach § 30 Abs. 4 DSG 2000 auf der Liegenschaft S*** (Uniklinikum Y***), durchgeführt und der Schwerpunkt der Einschau auf Zugriffsprotokollierungen sowie Berechtigungskonzepten, routinemäßiger Überprüfung der Zugriffe auf Patientendaten und allfälliger Mehrfachnutzung von EDV-Arbeitsplätzen durch verschiedene Bedienstete liegen werde.

6. Im Zuge dieser Einschau wurden von den Vertretern der X*** die Fragen dazu beantwortet, entsprechende Konzepte vorgelegt und Zugriffsberechtigungen an EDV-Arbeitsplätzen demonstriert.

7. Das Protokoll dieser Einschau wurde der X*** übermittelt.

8. Mit Schreiben der Datenschutzbehörde vom 10. Jänner 2017 wurde die X*** um zusätzliche Unterlagen, insbesondere Screenshots betreffend die Bearbeitungs- und Zugriffshistorie von Patientenakten, ersucht.

9. Mit Schreiben vom 12. Jänner 2017 wurden der Behörde die entsprechenden Unterlagen in Vorlage gebracht.

B. Sachverhaltsfeststellungen

Die Datenschutzbehörde geht von nachstehendem Sachverhalt aus, der sich aus den vorgelegten Stellungnahmen sowie den Ausführungen und behördlichen Feststellungen im Rahmen der Einschau ergibt:

1. Die X*** ist Träger von zwei Universitätskliniken, zwei Landeskliniken sowie einem Institut für Sportmedizin des Landes Y*** und einer Sonderkrankenanstalt für Neurorehabilitation in Y***.

2. Die X**** verfügt über eine interne Datenschutzkommission (DSK). Diese ist eine unabhängige, weisungsungebundene Institution, welche über eine eigene Geschäftsordnung verfügt. Als übergeordnetes Organ besteht ein Datenschutzaufsichtsrat, welcher Tätigkeitsberichte der internen DSK erhält.

2. Zur Verwaltung von Patientendaten ist in den Einrichtungen der X*** das Krankenhausinformationssystem K*** im Einsatz, welches zur Sicherstellung der medizinischen Prozesse über Schnittstellen zu Subsystemen (z.B. Laborinformationssystem, etc.) verfügt.

3. Die Zugriffsrechte sind in Form eines X***-weiten Datenschutz- und Berechtigungskonzepts festgelegt. Innerhalb dieses Regelwerks werden die Zugriffsrechte je Rolle dargestellt, wobei das Rollenkonzept auf die jeweilige Berufsgruppe und die jeweilige Organisationseinheit abstellt und Berechtigungen nach dem Prinzip der „Erforderlichkeit“ vergeben werden. Ein K*** -Benutzer hat über seine Berufsgruppenrolle und die ihm zugeteilten Berechtigungen sich an Organisationseinheiten (Fachabteilung, Station, Ambulanz) anzumelden, die Berechtigung bestimmte Dokumente zu „seinen“ Patienten zu sehen/zu bearbeiten. Nur für diese, grundsätzlich sichtbaren Dokumente, kann der Benutzer auch die Historie abrufen. Es werden ausschließlich personifizierte Benutzerberechtigungen vergeben.

4. Krankengeschichten werden in der X*** grundsätzlich digital geführt, jedoch besteht in den meisten klinischen Abteilung daneben auch noch ein Papierakt zu jedem Patienten.

Nach Fertigstellung der Krankengeschichte werden die Daten der gesamten Dokumentation gemeinsam elektronisch archiviert. Seit dem Jahr 2007 werden Akten nur mehr elektronisch aufbewahrt, teilweise wurden Akten nachgescannt. Personalakten werden nur zum Teil elektronisch geführt und archiviert. Daneben besteht auch ein Papierakt für jeden Mitarbeiter und wird dieser auch in Papierform archiviert.

5. Es gibt Betriebsvereinbarungen der Krankenanstalten der X*** betreffend die Auswertung von Datenzugriffen im Krankenhausinformationssystem sowie im Krankengeschichten-Archiv. Unberechtigte Zugriffe auf Patientendaten werden in Verdachtsfällen ausgewertet (manuelle Logfileauswertung). Im Rahmen der nächsten Sitzung der internen DSK ist geplant, die Grundsätze für die regelmäßige Zugriffskontrolle festzulegen.

6. Im Hinblick auf die herangezogenen Dienstleister gibt es Mitarbeitervereinbarungen. Darüber hinaus werden Dienstleistervereinbarungen geführt, anhand derer diese geprüft werden.

7. Protokolle zu Mitarbeitern über die Anmeldungen am Z***, direkte Zugriffe auf die Datenbank, Zugriffe auf bestimmte Module etc. sind derzeit mit einer Speicherdauer begrenzt (zwischen 4 und 26 Wochen). Die Speicherung der Zugriffe von Mitarbeitern auf Dokumente (Anlage, Bearbeiten, Drucken etc.) ist jedoch untrennbar mit der Speicherung des Dokumentes selbst verbunden und daher derzeit nicht begrenzt, weil auch die Speicherung der Dokumente derzeit nicht begrenzt ist.

8. In den Betriebsvereinbarungen zwischen der X*** und dem Betriebsausschuss des LKH, der X*** und dem Angestelltenbetriebsrat der T*** und der X*** und dem Gemeinsamen Betriebsrat der Landesklinik O*** wird ausgeführt, dass Protokoll über jede Datenverwendung geführt wird, damit man die tatsächlich durchgeführten Verwendungsvorgänge (Änderungen, Abfragen, Übermittlungen) im Hinblick auf die Zulässigkeit im notwendigen Ausmaß nachvollziehen kann. In Bezug auf die Protokollierung steht fest, dass ein Orbis-Benutzer die Berechtigung hat, bestimmte Dokumente zu „seinen“ Patienten zu sehen/zu bearbeiten. Im Rahmen dieser sichtbaren Dokumente kann der Benutzer die Bearbeitungshistorie abrufen. Dabei wird beim Öffnen einer Bearbeitungsgeschichte zu einem betreffenden Dokument sichtbar, welcher Mitarbeiter das Dokument angelegt, bearbeitet, vidiert, etc. habe. Es handelt sich dabei um eine so genannte „offene Protokollierung“.

9. Die Nutzerprofile ehemaliger Bediensteter werden nicht gelöscht, da die Löschung eines Mitarbeiters/Benutzers im Z*** derzeit technisch nicht von der Speicherung der Dokumente getrennt werden kann.

10. Für Patientendaten/Dokumente im Z*** gibt es derzeit keine Löschroutine. Es sind jedoch Lösungsansätze zur Umsetzung dieser Datenschutzanforderung in Prüfung und es hat diesbezüglich bereits Gespräche mit dem Z***-Hersteller gegeben. Man ist bemüht eine datenschutzfreundliche Lösung herbeizuführen.

11. Es kommt zu Mehrfachnutzungen von EDV-Arbeitsplätzen. Bedienstete sind angewiesen, sich auszuloggen, wenn sie den Arbeitsplatz verlassen.

12. Im Zuge der ELGA-Einführung ist eine Erhöhung der Passwortkomplexität geplant. Dabei soll ein Umstieg auf 8 Stellen und drei verschiedene Zeichen stattfinden. Der Passwortwechsel soll auch zukünftig alle 180 Tage durchgeführt werden.

C. Schlussfolgerungen der Datenschutzbehörde; rechtliche Beurteilung

1. Gegenstand des vorliegenden Verfahrens ist die Frage, ob die X*** 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 und allfälliger Mehrfachnutzung von EDV-Arbeitsplätzen durch verschiedene Bedienstete lag.

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

2. Das Ermittlungsverfahren ergab, dass datenschutzrechtliche Vorgaben im überwiegenden Ausmaß eingehalten werden.

Besonders hervorzuheben sind folgende Bemühungen der X***

a) das Vorhandensein schriftlicher Unterlagen zum Datenschutz bzw. zur medizinischen Dokumentation

b) das Vorhandensein einer internen unabhängigen DSK

c) das Vorliegen eines umfassenden Rollen- und Berechtigungskonzepts

d) das Vorhandensein eines umfassenden Protokollierungssystems

e) Überlegungen hinsichtlich der Löschungsroutine für Dokumente/Patientendaten

f) das Vorliegen eines Schemas nachdem bei aufgezeigten Missbrauchsfällen vorgegangen wird

3. Hinsichtlich

a) der Nichtdurchführung einer Löschung ehemaliger User,

b) der Nichtdurchführung regelmäßiger Zugriffskontrollen,

c) der fehlenden Löschroutine von elektronischen Krankengeschichten sowie von bestimmten Protokolldaten sowie

d) der fehlenden Zustimmung der Mitarbeiter im Rahmen des Zugriffs auf Protokolldaten („offene Protokollierung“) war jedoch die beiliegende Empfehlung auszusprechen.

E M P F E H L U N G

Die Datenschutzbehörde spricht aus Anlass der Überprüfung der Y*** Landeskliniken Betriebsgesellschaft m.b.H. (X***) folgende Empfehlung aus:

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

2. Die X*** möge geeignete Maßnahmen ergreifen, um eine effektive Zugriffskontrolle auf Patientendaten sicherzustellen. Die Bediensteten der X*** mögen darüber nachweislich in Kenntnis gesetzt werden.

3. Die X*** möge eine Löschroutine hinsichtlich der Löschung von Patientendaten in elektronisch geführten Krankengeschichten sowie von Protokolldaten implementieren.

4. Die X*** möge im Rahmen der Betriebsvereinbarungen betreffend Datenzugriffe die Zustimmung der Betroffenen für die „*offene Protokollierung*“ der Daten einholen.

5. Für die Umsetzung dieser Empfehlung wird eine Frist von sechs Monaten gesetzt.

Rechtsgrundlagen: §§ 1, 6, 8 und 30 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

Im Zuge des vorliegenden amtswegigen Prüfverfahrens, welches der Umsetzung des Prüfungsschwerpunktes 2015/2016 diente, wurden auch Fragen zur Vorgangsweise bei einem Austritt eines Mitarbeiters, zur regelmäßigen Überprüfung von Zugriffen auf Patientendaten sowie zur Löschroutine bei Krankengeschichten und Protokolldaten gestellt.

Dazu gab die X*** an, dass grundsätzlich bei einem Austritt keine Löschung des Nutzerprofils des austretenden Nutzers erfolge.

In Bezug auf die Überprüfung von Zugriffen auf Patientendaten wurde ausgeführt, dass diese in Verdachtsfällen erfolge.

Eine Löschroutine von Patientendaten, die in elektronisch geführten Krankengeschichten geführt werden, gebe es noch nicht, jedoch würden erste Überlegungen bereits angestellt. Für bestimmte Protokolldaten, die im Zusammenhang mit der Anmeldung am KIS, mit direkten Zugriffen auf die Datenbank und Zugriffen auf bestimmte Module stehen, gebe es spezifische Speicherdauern von 4 bis zu 26 Wochen. Hinsichtlich der sonstigen Daten gebe es keine Löschroutine.

In den Betriebsvereinbarungen zwischen der X*** und dem Betriebsausschuss des LKH, der X*** und dem Angestelltenbetriebsrat der T*** und der X*** und dem Gemeinsamen Betriebsrat der Landesklinik O*** wird ausgeführt, es werde Protokoll über jede Datenverwendung geführt, damit man die tatsächlich durchgeführten Verwendungsvorgänge (Änderungen, Abfragen, Übermittlungen) im Hinblick auf die Zulässigkeit im notwendigen Ausmaß nachvollziehen könne. In Bezug auf die Protokollierung wurde daneben vorgebracht, dass ein Orbis-Benutzer über seine Berufsgruppenrolle und die ihm zugeteilte Berechtigung sich an Organisationseinheiten anzumelden, die Möglichkeit habe, bestimmte Dokumente zu „*seinen*“ Patienten zu sehen/zu bearbeiten. Im Rahmen dieser sichtbaren Dokumente könne der Benutzer die Bearbeitungshistorie abrufen. Dabei sei beim Öffnen einer Bearbeitungsgeschichte zu einem betreffenden Dokument sichtbar, welcher Mitarbeiter das Dokument angelegt, bearbeitet, vidiert, etc. habe. Es handle sich dabei um eine „*offene Protokollierung*“.

B. In rechtlicher Hinsicht folgt daraus:

I. Zu den Nutzerprofilen

1. Aufgrund des oben angeführten Sachverhaltes steht fest, dass Nutzer auch nach deren Austritt aus der X*** in Datenverarbeitungssystemen insoweit zeitlich unbefristet gespeichert bleiben, als lediglich deren Zugangsberechtigung gelöscht 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.

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.

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.

II. Zur regelmäßigen Zugriffskontrolle

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

Behandlung in der Krankenanstalt unterziehen (vgl. dazu die Empfehlungen vom 18. Mai 2016, GZ DSB-D213.399/0003-DSB/2016, sowie vom 23. Mai 2016, GZ DSB-D210.783/0004-DSB/2016, beide abrufbar im RIS).

2. 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.

3. Aufgrund des oben angeführten Sachverhaltes steht fest, dass die X*** zwar Zugriffe ordnungsgemäß protokolliert. Jedoch findet eine Überprüfung der durchgeführten Zugriffe hinsichtlich deren Rechtmäßigkeit nur in Verdachtsfällen statt.

Durch diese Kontrolle wird aber nicht sichergestellt, dass besonders schützenswerte Personengruppen (wie insbesondere eigene Bedienstete oder deren Angehörige bzw. öffentlich bekannte Personen), die sich einer Behandlung unterziehen (müssen), vor unberechtigten Zugriffen geschützt sind.

Überprüfungen in anderen Krankenanstalten durch die Datenschutzbehörde haben ergeben, dass effektive die Zugriffskontrollen auf verschiedene Arten ausgeführt werden können (vgl. dazu bspw. die Empfehlungen vom 17. Mai 2015, GZ DSB-D213.397/0005-DSB/2016, GZ DSB-D213.395/0003-DSB/2016 sowie jene vom 18. Mai 2016, GZ DSB-D213.398/0003-DSB/2016, abrufbar im RIS).

Zur Hintanhaltung unberechtigter Zugriffe empfiehlt es sich, die Bediensteten der X*** auf die Durchführung nachprüfender Zugriffskontrollen nachweislich aufmerksam zu machen.

III. Zur Implementierung einer Löschroutine

Wie unter I. dargelegt, dürfen Daten in personenbezogener Form nur zeitlich begrenzt aufbewahrt werden.

Die zulässige Aufbewahrungsdauer von Patientendaten bzw. von Protokolldaten richtet sich nach den einschlägigen Materiengesetzen.

Zur Sicherstellung, dass diese Daten nach Ablauf der zulässigen Speicherdauer gelöscht werden bzw. der Personenbezug beseitigt wird, war diese Empfehlung auszusprechen.

IV. Zur Einholung der Zustimmung für die „offene Protokollierung“

1. Aufgrund des oben angeführten Sachverhaltes steht fest, dass Orbis-Benutzer im Rahmen der zugeteilten Berufsgruppenrolle 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.

2. Um Sicherzustellen, dass es zu keiner Verletzung der schutzwürdigen Geheimhaltungsinteressen bei Verwendung von Protokolldaten kommt, ist daher im Rahmen der Betriebsvereinbarung die Zustimmung der Betroffenen gem. § 8 Abs. 1 Z 2 DSG 2000 einzuholen.

V. Zusammenfassung

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