Vorabkontrollstellungnahme zu dem klinischen Patientenmanagementsystem der Europäischen Kommission (KPMS)

Fall 2017-0804

***

Die Europäische Kommission ist für die EU-weite Nutzung und Speicherung von Patientendaten zu seltenen Krankheiten in einer Software verantwortlich. Auch wenn der gesamte Verarbeitungsprozess auf einer ausdrücklichen Einwilligung beruht, sollte die Datenschutzerklärung noch verbessert werden, um die Gesetzesgrundlage und/oder Rechtmäßigkeit des Verarbeitungsvorgangs und auch die Möglichkeit der Ausübung der Rechte auf Löschung und Sperrung widerzuspiegeln. Darüber hinaus sollte ein Aufbewahrungszeitraum und/oder ein Zeitraum, in dem Gesundheitsdienstleister die Notwendigkeit der weiteren Aufbewahrung der Daten überprüfen, definiert und einige Sicherheitsmaßnahmen verstärkt werden.

***

Brüssel, 6. November 2017

Postanschrift: Rue Wiertz 60 – 1047 Brüssel, Belgien
Dienststelle: Rue Montoyer 30 – 1000 Brüssel, Belgien
E-Mail: edps@edps.europa.eu – Website: www.edps.europa.eu
Tel.: +32 2283-1900 – Fax: +32 2283-1950

1) Sachverhalt

Das klinische Patientenmanagementsystem („KPMS“) ist eine web-basierte klinische Softwareanwendung, die zur Unterstützung der Europäischen Referenznetze („ERN“) im Bereich komplexer Krankheiten, die selten sind oder eine geringe Prävalenz aufweisen („seltene Krankheiten“), entwickelt wurde. Diese insgesamt vierundzwanzig (24) ERN sind grenzübergreifende virtuelle Netze von in Europa tätigen Gesundheitsdienstleistern, die der Diagnose und Behandlung von Patienten mit seltenen Krankheiten dienen sollen.[1] Als seltene Krankheiten gelten solche Krankheiten, die eine Prävalenz von höchstens fünf von 10 000 Personen haben.[2]

Mit dieser Software können daher Gesundheitsdienstleister[3] in Europa Informationen austauschen. Diese von einem Unterauftragnehmer entwickelte Anwendung wird von der Kommission verwaltet.

Das KPMS enthält demnach medizinische Daten von Patienten, die an einer seltenen Krankheit leiden.

1.1. Die Nutzer

Es gibt zwei Arten von Nutzern, die mit dem KPMS arbeiten.

Zum einen wird es von Mitarbeitern der Kommission benutzt, die für die Verwaltung und technische Betreuung des Systems zuständig sind, wie beispielsweise die Beseitigung von Problemen und Sicherheitsstörungen. Diese sind als „Nutzer“ in der Anwendungssoftware enthalten.

Und zum anderen gibt es die *tatsächlichen* Nutzer, nämlich die Gesundheitsdienstleister. Diese Nutzer gehören zu einem Krankenhaus, das Mitglied eines ERN ist („Gesundheitszentrum“). Darüber hinaus kann es auch lokal am Pflegeort tätige Fachkräfte geben, die zu einem Krankenhaus gehören, das nicht Mitglied eines ERN ist („Gastbenutzer“). Während Nutzer, die zu einem Krankenhaus gehören, das ERN-Mitglied ist, direkt auf die Daten der Anwendung zugreifen können, ist der Zugriff für Gastbenutzer auf das *unbedingt notwendige* Maß begrenzt und wird nur mit der Zustimmung des verantwortlichen ERN-Koordinators gewährt. Die Nutzer erstellen für organisatorische Zwecke „Anträge auf Einrichtung von Gremien“ und

[1] In Artikel 12 Absatz 1 der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 „über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung“ ist Folgendes vorgesehen: „Die Kommission unterstützt die Mitgliedstaaten beim Aufbau Europäischer Referenznetzwerke zwischen Gesundheitsdienstleistern und Fachzentren in den Mitgliedstaaten, insbesondere im Bereich seltener Krankheiten. Die Netzwerke beruhen auf der freiwilligen Teilnahme ihrer Mitglieder, die gemäß den Rechtsvorschriften des Mitgliedstaats, in dem die Mitglieder niedergelassen sind, an den Tätigkeiten der Netzwerke teilnehmen und zu diesen Tätigkeiten beitragen, und stehen jederzeit offen für neue Gesundheitsdienstleister, die sich anschließen möchten, sofern diese Gesundheitsdienstleister alle [...] Bedingungen und Kriterien erfüllen.“ (ABl. L 88 vom 4.4.2011, S. 45).

[2] Siehe Erwägungsgrund Nr. 55 der oben genannten Richtlinie (Fußnote 1).

[3] In Artikel 3 Buchstabe g der oben genannten Richtlinie (Fußnote 1) sind Gesundheitsdienstleister als „jede natürliche oder juristische Person oder sonstige Einrichtung, die im Hoheitsgebiet eines Mitgliedstaats rechtmäßig Gesundheitsdienstleistungen erbringt“ definiert.

benennen „Gremiumsleiter“.[4] Die Gesundheitsdienstleister können als Nutzer der Software Gremien einrichten und an Gremien teilnehmen, um an der Erstellung spezifischer Dossiers mitzuwirken.

Die Gesundheitsdienstleister müssen sich zunächst durch EU-Login authentifizieren, um Zugriff auf die Anwendung zu erhalten.[5] Die Kommission stellt (über den Unterauftragnehmer) diesen Zugriff bereit und ist daher direkt für die Verarbeitung der Verwaltungsdaten der Gesundheitsdienstleister[6] verantwortlich.

Für die Registrierung der Nutzer, um auf das KPMS zugreifen zu können, wird der Authentifizierungs- und Identitätsmanagementdienst der Kommission verwendet. Nach Erstellung eines EU-Login-Kontos wird dieses Nutzerkonto mithilfe eines elektronischen Servicetools, dem Autorisierungsdienst SAAS2, der im Verantwortungsbereich der Kommission liegt, autorisiert.[7] Dieses Tool wird zur Autorisierung einer begrenzten und identifizierten Nutzergruppe auf ERN-Ebene verwendet, denen jeweils genau definierte Rollen zugeordnet sind; nur autorisierte Nutzer werden mithilfe dieses Tools in dem KPMS aktiviert.

1.2. Die Datenkategorien

Es gibt zwei Kategorien von Daten, die in dem KPMS verarbeitet werden.

Die Gesundheitsdienstleister verschlüsseln zunächst die echten Verwaltungsdaten der Patienten im KPMS, die zu der Rubrik „identifizierende Daten“ gehören. Dies umfasst die folgenden Daten: Name, Nachname, Geschlecht, Geburtsort und -datum und Bildungsniveau.

Danach pseudonymisiert der Gesundheitsdienstleister unter der Rubrik „Konsultationsersuchen“ den Namen des Patienten und ersetzt ihn durch einen Nicknamen, der dem wirklichen Namen des Patienten in keiner Weise ähnlich sein darf. Andere Gesundheitsdienstleister, die in anderen Gesundheitszentren arbeiten, haben nur Zugang zu diesem Nicknamen und den medizinischen Daten, ohne auf die wirklichen, unter „identifizierende Daten“ gespeicherten Angaben zugreifen zu können.[8] Folgende medizinische Daten werden verarbeitet: Konsultationsersuchen, Beschreibungen von Krankheitsepisoden, Diagnosen seltener Krankheiten, Komorbiditäten, phänotypische und genetische Merkmale und Biobanken, familiäre Vorgeschichte, Gesundheitsverhalten, Allergien und Unverträglichkeiten, Vorgeschichte von Krankheiten und Störungen, besondere Behandlungsmethoden und Eingriffe, Vorgeschichte von Operationen, Transplantationen und verabreichten Medikamenten. Auch Abbildungen, Bilder und Videoaufzeichnungen werden verarbeitet. Etwaige Markierungen oder Kennzeichnungen, die Rückschlüsse auf die Identität des Patienten zulassen, werden mithilfe von Anonymisierungsmethoden von den eingefügten Abbildungen entfernt und durch ihre einzigartige ID ersetzt.

[4] Gastbenutzer können nicht als Gremiumsleiter fungieren.

[5] Die Nutzer verwalten ihr Passwort und ihre EU-Login-Daten selbst.

[6] EU-Login-Benutzername, Vor- und Nachname, Name des Gesundheitsdienstleisters, das Krankenhaus oder Gesundheitszentrum, Name des ERN, berufliche E-Mail-Adresse und Land.

[7] Genauer gesagt, der Generaldirektion Gesundheit und Lebensmittelsicherheit der Kommission.

[8] Für jeden Patienten erzeugt das System bei Aufnahme in das KPMS automatisch eine einzigartige ID. Nur die Mediziner und Gesundheitsexperten in einem bestimmten Gesundheitszentrum oder Krankenhaus können diese ID einsehen.

1.3. Pseudonymisierung

In technischer Hinsicht werden die Gesundheitsdaten der Patienten zunächst in das KPMS eingestellt und anschließend pseudonymisiert.[9] Bei der Einrichtung eines neuen Patienten in dem KPMS generiert das System automatisch als Kennung eine ID1. Diese ID1 wird dann entweder in der Krankenhausakte des Patienten übernommen oder der Nutzer ersetzt die ID1 durch die in der Krankenhausakte hinterlegte ID des Patienten. Wenn der Gesundheitsexperte die Gesundheitsdaten zur Einrichtung eines Diskussionsforums eingeben möchte, vergibt er in einem zweiten Schritt einen Nicknamen für den betreffenden Patienten. Durch die Verwendung eines Nicknamens anstelle der ID1 werden die Pseudonymisierungsebenen des KPMS noch weiter verstärkt. Wie bereits erwähnt, werden die pseudonymisierten Daten dann zur Besprechung des Falles in einem Diskussionsforum und Beurteilung der Patientenakte anderen Nutzern des KPMS zugänglich gemacht. Der Zugriff auf die ID1 des Patienten bleibt dabei ausschließlich dem jeweiligen Gesundheitszentrum und den jeweiligen Gesundheitsexperten vorbehalten. Die anderen Gesundheitszentren und Nutzer können nur den Nicknamen des Patienten sehen. Eine Löschung von Patientendaten aus dem KPMS kann nur das Gesundheitszentrum/Krankenhaus vornehmen, das den betreffenden Patienten in das System aufgenommen hat.

1.4. Einverständniserklärungen und Zugriff auf Daten

Der Patient muss zur Aufnahme in die Softwareanwendung dem Gesundheitsdienstleister gegenüber ausdrücklich und eindeutig seine Einwilligung erklären.[10] Dazu gibt es ein Formular mit dem Namen „*patient consent form for data sharing in European Reference Network for Rare Diseases for Patient care and creation of rare disease registries*“ [Einwilligungserklärung des Patienten zum Austausch von Daten innerhalb des Europäischen Referenznetzwerkes für seltene Krankheiten zum Zwecke der Patientenbehandlung und Erstellung von Registern seltener Krankheiten]. Diese Einwilligungserklärung enthält drei Felder: Das erste betrifft die Einwilligung des Patienten in den Austausch der Daten, das zweite seine Einwilligung in die Aufnahme in die Datenbank und das dritte die Einwilligung in eine mögliche Kontaktierung des Patienten zu Forschungszwecken. Die Patienten müssen jeweils direkt in dem Feld „I consent“ [Ich bin einverstanden] oder in dem Feld „I do not consent“ [Ich bin nicht einverstanden] unterschreiben.

Der für die Aufnahme der Patientendaten in die Datenbank verantwortliche Gesundheitsdienstleister kann nur dann das KPMS nutzen, wenn er ausdrücklich angibt, dass

[9] „Pseudonymisierung“ bedeutet, dass personenbezogene Daten in einer Weise verarbeitet werden, dass sie ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

[10] Der Begriff Einwilligung ist in dem Delegierten Beschluss der Kommission wie folgt definiert: „aufgeklärte Einwilligung im Rahmen der Europäischen Referenznetzwerke bezeichnet jede ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgte explizite Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit dem Austausch ihrer persönlichen und ihrer Gesundheitsdaten zwischen Gesundheitsdienstleistern und Mitgliedern eines Europäischen Referenznetzwerkes gemäß diesem delegierten Beschluss einverstanden ist.“ Siehe Artikel 2 Buchstabe e des Delegierten Beschlusses der Kommission vom 10. März 2014 „über die Kriterien und Bedingungen, die Europäische Referenznetzwerke und Gesundheitsdienstleister, die sich einem Europäischen Referenznetzwerk anschließen möchten, erfüllen müssen“ (ABl. L 147 vom 17.05.2014, S. 1).

der Patient diese Einwilligungserklärung ausgefüllt hat.[11] Diese Formulare liegen in allen Amtssprachen der Europäischen Union vor. Die ausgefüllten Einwilligungserklärungen werden nicht in das KPMS hochgeladen, sondern verbleiben bei dem Gesundheitsdienstleister.

Zugriff darauf haben nur die Gesundheitsdienstleister, die vorab durch die Kommission authentifiziert wurden und vorab die ausdrückliche schriftliche Einwilligung zum Hochladen der Informationen erhalten haben. Wie in einem von dem Direktor als dem für die Verarbeitung der Daten im KPMS Verantwortlichen unterzeichneten Vermerk angegeben, haben weder die Kommission noch der Unterauftragnehmer zu irgendeiner Zeit Zugriff auf die Patientendaten.[12] Es werden also weder in dem Authentifizierungs- und Identitätsmanagementdienst der Kommission noch in dem Autorisierungsdienst SAAS2 Patientendaten verarbeitet.

1.5. Aufbewahrungsfrist

Für die medizinischen Daten, die von Gesundheitsdienstleistern eingegeben werden, ist keine Aufbewahrungsfrist festgelegt, sondern sie werden so lange wie erforderlich aufbewahrt.

1.6. Sicherheitsmaßnahmen

[....]

2) Rechtliche Prüfung

Diese Stellungnahme zur Vorabkontrolle[13] gemäß Artikel 27 der Verordnung (EG) Nr. 45/2001[14] („Verordnung“) befasst sich vorrangig mit Aspekten, die im Hinblick auf die Einhaltung der Verordnung problematisch sind oder ansonsten einer genaueren Betrachtung bedürfen. Bezüglich der in dieser Stellungnahme nicht behandelten Aspekte sieht der EDSB aufgrund der ihm vorliegenden Unterlagen keinen Äußerungsbedarf.

---

[11] Patienten müssen für jede der unterschiedlichen Arten der Einwilligung ein Kästchen ankreuzen. In den Benutzerhandbüchern und anderen praktischen Dokumentationsunterlagen wird darauf hingewiesen, dass das Aufnahmeformular nur dann gespeichert werden kann, wenn das Kästchen „consent for care“ [Patienteneinwilligung] angekreuzt ist und damit bestätigt wird, dass eine gültige Einwilligung des Patienten vorliegt. Die Einwilligungserklärung enthält drei verschiedene Kästchen, mit denen die drei Arten der Einwilligung erteilt werden.

[12] Siehe „Commission access to ERN-CPMS system“ [Zugriff der Kommission auf das KPMS der ERN]. Elektronisch unterschriebener Aktenvermerk vom 1.9.2017 [Ares Referenznummer (2017) 4283273].

[13] Gemäß Artikel 27 Absatz 4 der Verordnung hat der EDSB seine Stellungnahme innerhalb von zwei Monaten nach Eingang der Meldung abzugeben (Aussetzungen fallen nicht unter diese Frist). Die Meldung ist am 8. September 2017 eingegangen. Die Stellungnahme des EDSB erfolgt daher zum 8. November 2017. Am 8. September 2017 übermittelte der Datenschutzbeauftragten („DSB“) der Europäischen Kommission per E-Mail eine Meldung zur Vorabkontrolle der als klinisches Patientenmanagementsystem („KPMS“) bezeichneten Datenverarbeitung.[13] Am 14. September 2017 bestätigte der EDSB per E-Mail den Erhalt der Meldung und stellte dabei fünf Zusatzfragen. Diese beantwortete der DSB der Kommission in seiner E-Mail vom 18. September 2017 und schlug dabei zwei Termine für eine Demonstration des Systems vor. Diese Demonstration fand am 28. September bei der Generaldirektion SANTE statt.

[14] ABl. L 8 vom 12.1.2001, S. 1.

Der Verarbeitungsvorgang fällt unter Artikel 27, da es sich dabei um sensible Daten, genauer gesagt Gesundheitsdaten, handelt und die Rechte und Freiheiten des Betroffenen dadurch beeinträchtigt werden könnten.

2.1 Rechtmäßigkeit des Verarbeitungsvorgangs

Zunächst sollte klargestellt werden, dass es sich bei dem System um zwei unterschiedliche Verarbeitungsvorgänge handelt.

Der erste Verarbeitungsvorgang besteht in der Erhebung und Bearbeitung von Verwaltungsdaten durch Nutzer der Kommission (über ihren Unterbeauftragten). Da es sich bei der Verarbeitung dieser Daten lediglich um eine administrative Tätigkeit handelt, die sich ausschließlich auf Identifikationsdaten der Gesundheitsdienstleister bezieht, fällt dieser Verarbeitungsvorgang nicht unter Artikel 27 Absatz 2 der Verordnung, sodass diesbezüglich keine Vorabkontrolle erforderlich ist.

Die zweite Art der Verarbeitung wird von den Gesundheitsdienstleistern ausgeführt. Dabei handelt es sich um die Eingabe von und den Zugriff auf Patientendaten sowie die Änderung, die Heranziehung und den Abruf derselben.[15] Dieser Verarbeitungsvorgang erfolgt ausschließlich durch die Gesundheitsdienstleister, die für die Einholung der Einwilligungserklärungen verantwortlich sind, findet jedoch auf einer von der Kommission verwalteten Plattform statt. Die Kommission ist über ihren Unterbeauftragten für die Speicherung und Sicherheit der Daten zuständig und ist daher gemeinsam mit dem Gesundheitszentrum des Gesundheitsdienstleisters, das den Patienten behandelt und die Daten verarbeitet, mitverantwortlich. Die Kommission und die Gesundheitszentren sind somit für die Verarbeitung Mitverantwortliche. Die vorliegende Vorabkontrollstellungnahme ist auf den zweiten, von den Gesundheitsdienstleistern durchgeführten Verarbeitungsvorgang ausgerichtet, da er unmittelbar Gesundheitsdaten im Sinne von Artikel 27 Absatz 2 Buchstabe a der Verordnung betrifft.

Die Verarbeitung ist aus zwei Gründen rechtmäßig.

Der eine Grund ist, dass gemäß Artikel 5 Buchstabe a der Verordnung die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich sein muss, die aufgrund der Verträge zur Gründung der Europäischen Gemeinschaften oder anderer aufgrund dieser Verträge erlassener Rechtsakte im öffentlichen Interesse ausgeführt wird. Die Europäischen Referenznetzwerke werden auf der Grundlage von Artikel 12 der Richtlinie über die „Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung“ eingerichtet.[16] Außerdem wird in der Verordnung über ein drittes Aktionsprogramm der Union im Bereich der Gesundheit[17] als eine

[15] Wie bereits erwähnt, sind diese Daten für alle Gesundheitsdienstleister mit Ausnahme derjenigen, die dem Krankenhaus angehören, aus dem die Daten ursprünglich stammen, pseudonymisiert.

[16] Siehe Fußnote 1.

[17] Verordnung (EU) Nr. 282/2014 des Europäischen Parlaments und des Rates vom 11. März 2014 „über ein drittes Aktionsprogramm der Union im Bereich der Gesundheit (2014-2020) und zur Aufhebung des Beschlusses Nr. 1350/2007/EG“ (ABl. L 86 vom 21.3.2014). In Anhang I Nummer 4.2 sind die thematischen Förderungsprioritäten aufgeführt, darunter auch die „Unterstützung von Mitgliedstaaten, Patientenverbänden und Interessengruppen durch koordinierte Maßnahmen auf Unionsebene, um Patienten, die unter seltenen Krankheiten leiden, wirksam helfen zu können. Dazu gehören der Aufbau von Referenznetzwerken (im Einklang mit Nummer 4.1), unionsweite Informationsdatenbanken und Register für seltene Krankheiten auf der Grundlage gemeinsamer Kriterien.“

der Prioritäten die Unterstützung von Patienten, die an seltenen Krankheiten leiden, genannt, wozu auch „der Aufbau von Referenznetzwerken [...], unionsweite Informationsdatenbanken und Register für seltene Krankheiten auf der Grundlage gemeinsamer Kriterien“ gehören. Damit besteht eine Rechtsgrundlage für die Einrichtung des KPMS.

Der zweite Grund für die Rechtmäßigkeit der Verarbeitung ist die Tatsache, dass sie auf der ausdrücklichen Einwilligung des Betroffenen beruht und damit die Bestimmung in Artikel 5 Buchstabe d der Verordnung erfüllt: Patienten müssen entweder in dem Feld, mit dem sie ihre Einwilligung bestätigen, oder in einem Feld, mit dem sie ihre Einwilligung verweigern, direkt unterschreiben. Sofern eines dieser Felder tatsächlich unterzeichnet ist, besteht kein Zweifel. Mit der ausdrücklichen Einwilligung des Patienten liegt eine rechtliche Grundlage für die Verarbeitung vor.

Der EDSB nimmt zur Kenntnis, dass der Patient mit der Einwilligungserklärung ausdrücklich seine Einwilligung erteilen muss.[18] Darüber hinaus ist diese Einwilligung in drei Teile untergliedert, sodass der Patient zum Beispiel dem Austausch identifizierter Daten zustimmen, gleichzeitig aber der Kontaktaufnahme zu Forschungszwecken widersprechen kann. Der EDSB hält diese Art der detaillierten und ausdrücklichen Einwilligung für eine optimale Vorgehensweise. Die Einwilligung hat ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage zu erfolgen[19], was hier der Fall zu sein scheint, da die Einwilligungserklärung Folgendes vorsieht: „If you chose not to give your consent this will not affect your care“ [Falls sie sich entscheiden, Ihre Einwilligung zu verweigern, so wird dies keinen Einfluss auf Ihre Gesundheitsversorgung haben] und „if you consent today you may withdraw consent later“ [Falls Sie Ihre Einwilligung heute erteilen, können Sie diese später widerrufen]. Des Weiteren heißt es in dem Formular: „[...] even if you choose not to give your consent your doctors will continue to take care of you to the best of their ability“ [Auch wenn Sie Ihre Einwilligung nicht erteilen, werden Ihre Ärzte mit Ihrer Behandlung nach besten Kräften fortfahren].

2.2 Datenqualität

Wie bereits erwähnt, handelt es hier um zwei verschiedene Datenbestände. Zum einen gibt es die wirklichen Patientendaten, die Angaben zum Namen, Nachnamen, Wohnort, Geburtsort und Geburtsdatum sowie Bildungsniveau des Betroffenen enthalten, und zum anderen den Nicknamen mit den dazugehörigen medizinischen Daten, die auch Zusatzinformationen zu der jeweiligen Krankheit beinhalten können, wie zum Beispiel Abbildungen, Videoaufzeichnungen und Ähnliches.

Gemäß Artikel 4 Absatz 1 Buchstabe c müssen personenbezogene Daten „den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und nicht darüber hinausgehen“. Diese Regelung setzt einen notwendigen Zusammenhang zwischen den Daten und ihrem Verwendungszweck voraus.

[18] Erwägungsgrund 12 des in Fußnote 6 erwähnten Delegierten Beschlusses der Kommission lautet wie folgt: „Um den Austausch personenbezogener Daten im Zusammenhang im Kontext [sic] der Netzwerke zu gewährleisten, könnten die Verfahren zur Erteilung der aufgeklärten Einwilligung vereinfacht werden mittels Verwendung eines einzigen gemeinsamen Einwilligungsmusters; dieses müsste den Anforderungen der Richtlinie 95/46/EG hinsichtlich der Einwilligung der von der Verarbeitung betroffenen Person entsprechen“.

[19] Artikel 29 Datenschutzgruppe, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011.

Der EDSB ist der Meinung, dass Informationen über das Bildungsniveau der betroffenen Person, die unter der Rubrik „identifizierende Daten“ erhoben werden, nicht immer für den verfolgten medizinischen Zweck notwendig und erheblich sind. Es sollte daher in der Anwendung angegeben werden, dass diese Daten nur dann erhoben werden, wenn sie für medizinische Zwecke erforderlich sind.[20] Darüber hinaus besteht die Möglichkeit, dass Patienten aufgrund von erhobenen Abbildungen und Videoaufzeichnungen identifizierbar sind (z. B. aufgrund von Abbildungen von Gesichtern oder Namen, die auf Abbildungen erkennbar sind). Die Gesundheitszentren sollten daher sicherstellen, dass auf Bildern so viel wie möglich und insbesondere wirkliche Namen ausgeblendet werden.

Der EDSB empfiehlt, Daten über das Bildungsniveau eines Patienten nur dann zu einzuholen, wenn diese erheblich und für medizinische Zwecke erforderlich sind. Außerdem sollten Bilder und andere identifizierende Informationen in Videoaufzeichnungen und Abbildungen soweit möglich ausgeblendet werden.

2.3 Information der betroffenen Personen

Hier gibt es zunächst den Datenschutzhinweis für Nutzer der Anwendung, also die Gesundheitsdienstleister, der gut und ausführlich ist. Des Weiteren gibt es für die Patienten die Einwilligungserklärung, die einen kurzen Datenschutzhinweis enthält, in dem es hauptsächlich um die Rechte der betroffenen Personen geht. Dabei werden aber nicht die in Artikel 11 und 12 der Verordnung 45/2001 aufgeführten Punkte angesprochen. Der Datenschutzhinweis informiert insbesondere weder über die Rechtsgrundlage und/oder Rechtmäßigkeit der Verarbeitung noch über die Fristen bezüglich der Ausübung von Auskunfts- und Berichtigungsrechten im Falle von Fehlern. Darüber hinaus enthält er auch keine Angaben zu dem Recht auf Sperrung und Löschung von Daten[21], das ebenfalls darin aufgeführt werden sollte. Ebenso fehlen Angaben zur zeitlichen Begrenzung der Speicherung.

Der EDSB empfiehlt daher, die „Einwilligungserklärung“ durch Hinzufügen der Angaben zur Rechtmäßigkeit der Verarbeitung, zu den Fristen zur Ausübung der Rechte, zu den Modalitäten bezüglich Sperrung und Löschung von Daten und zu einer angemessenen Aufbewahrungsfrist (beispielsweise in Form einer Liste mit Aufzeichnungspunkten) zu vervollständigen.

2.4 Sicherheit des Verarbeitungsvorgangs

Bei den für die Verarbeitung Verantwortlichen handelt es sich um Gesundheitsdienstleister (zusammen mit der Kommission als mitverantwortlicher Stelle). Der Begriff Gesundheitsdienstleister bezieht sich jedoch nicht nur auf Ärzte, sondern auf „jede natürliche oder juristische Person oder sonstige Einrichtung, die im Hoheitsgebiet eines Mitgliedstaats

[20] Diese Problematik wurde in der Sitzung vom 28. September 2017 angesprochen. Die Verantwortlichen der Anwendung bestätigten, dass diese Daten eine wichtige Rolle spielen können, wenn es um den geistigen Gesundheitszustand von Patienten geht oder wenn der Patient beispielsweise ein Arzt ist, der unter anderem ein besseres Verständnis der Fachterminologie besitzt.

[21] Allerdings wird in dem Datenschutzhinweis als Frist für die Sperrung/Löschung von Daten aufgrund einer begründeten und berechtigten Aufforderung seitens der betroffenen Person ein Zeitraum von vier Wochen genannt.

rechtmäßig Gesundheitsdienstleistungen erbringt".[22] Ärzte sind an eine Vertraulichkeitserklärung oder Ähnliches gebunden. Es ist jedoch nicht immer eindeutig der Fall, dass andere im Gesundheitsbereich Tätige ebenfalls an derartige Bestimmungen gebunden sind. Daher empfiehlt der EDSB, dass die Kommission als Mitverantwortliche sicherstellen sollte, dass alle Nutzer des KPMS eine ähnliche Vertraulichkeitserklärung unterzeichnen, wie sie für Ärzte üblich ist.[23]

Daher empfiehlt der EDSB, dass alle Nutzer des KPMS eine ähnliche Vertraulichkeitserklärung unterzeichnen sollten, wie sie für Ärzte üblich ist.

Der EDSB nimmt zur Kenntnis, dass die Gesundheitsdaten von Patienten in pseudonymisierter Form unter einem „Nicknamen" in dem System aufbewahrt werden. Dieser Nickname muss von dem Gesundheitsdienstleister vergeben werden, der angewiesen wird, „keine wirklichen Daten" in das für die Aufnahme von Patienten in das System auszufüllende Formular einzugeben. Diese Anweisung könnte noch durch einen ausdrücklichen Hinweis darauf verstärkt werden, dass der Nickname keinerlei Ähnlichkeit mit dem wirklichen Namen des Patienten haben darf. Der EDSB begrüßt die Tatsache, dass der für die Verarbeitung Verantwortliche in der Sitzung am 28. September 2017 angeboten hat, technische Maßnahmen zu ergreifen, mit denen automatisch Nicknamen herausgefiltert und zurückgewiesen werden, die teilweise den wirklichen Namen oder Nachnamen des Patienten enthalten.

Der EDSB empfiehlt der Kommission die Anweisung bezüglich der Nicknamen dahingehend zu verstärken, dass Gesundheitsdienstleister ausdrücklich dazu aufgefordert werden, sicherzustellen, dass diese keinerlei Ähnlichkeit mit den wirklichen Patientendaten haben.

[…]

2.5 Aufbewahrungsfrist

Gemäß Artikel 4 Absatz 1 Buchstabe e der Verordnung dürfen personenbezogene Daten „nur so lange, wie es für die Erreichung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, gespeichert werden." Personenbezogene Daten, die für „historische, statistische oder wissenschaftliche Zwecke über [längere Zeiträume] aufbewahrt werden [...], [sollten] entweder überhaupt nur in anonymisierter Form oder, wenn dies nicht möglich ist, nur mit verschlüsselter Identität der Betroffenen gespeichert werden".

Eine Aufbewahrungsfrist wird dabei nicht definiert. Der Kommission zufolge halten Gesundheitsdienstleister die Daten so lange wie nötig in dem KPMS vor.

Die Kommission sollte eine im Hinblick auf die Verarbeitungszwecke angemessene Aufbewahrungsfrist festlegen. Dabei könnte für Daten, die für Diagnose- und Behandlungszwecke verarbeitet werden und daher in dem KPMS wohl nur bis zur endgültigen Heilung des Patienten von Bedeutung sein dürften, eine andere Aufbewahrungsfrist gelten als

[22] Siehe Fußnote 3.

[23] Siehe hierzu „Leitlinien [des EDSB] für die Verarbeitung von Gesundheitsdaten am Arbeitsplatz durch Organe und Einrichtungen der Gemeinschaft", September 2009. Diese Leitlinien sehen als Empfehlung die „Verwendung von Verhaltenskodizes oder Vertraulichkeitserklärungen für alle an der Verarbeitung beteiligten Personen, die nicht zur Verschwiegenheit verpflichtet sind" vor.

für Daten, die für Forschungszwecke bestimmt sind, sofern die Patienten hierzu ihre Einwilligung gegeben haben.[24] Für die letztere Art der Verarbeitung könnte eine längere Aufbewahrungsfrist festgelegt werden, sofern diese Daten in einer sicheren anonymisierten und/oder verschlüsselten Form verwahrt werden. Eine andere Möglichkeit besteht darin, dass die Kommission die Gesundheitsdienstleister zur Überprüfung der Notwendigkeit der weiteren Aufbewahrung der Daten in regelmäßigen Abständen (z. B. alle 10 bis 15 Jahre nach ihrer Aufnahme in die Datenbanken) auffordert.

Der EDSB empfiehlt, einen konkreten Aufbewahrungszeitrum festzulegen, damit sichergestellt ist, dass Daten nicht länger als nötig aufbewahrt werden. Eine andere Möglichkeit besteht darin, die Gesundheitsdienstleister, die die Daten in das System eingeben, in regelmäßigen Abständen daran zu erinnern, die Notwendigkeit der weiteren Aufbewahrung der Daten zu überprüfen.

Empfehlungen

Der EDSB hat in dieser Stellungnahme mehrere Empfehlungen ausgesprochen, damit der Verordnung Genüge getan wird. Sofern diese Empfehlungen umgesetzt werden, besteht nach Auffassung des EDSB kein Anlass zu der Annahme, dass ein Verstoß gegen die Verordnung vorliegt.

Im Hinblick auf nachstehende **Empfehlungen** erwartet der EDSB deren **Umsetzung sowie dokumentierte Nachweise** dieser Umsetzung innerhalb von **drei Monaten** nach Ergehen dieser Stellungnahme:

- Erhebung von Daten über das Bildungsniveau eines Patienten nur dann, wenn diese für medizinische Zwecke erforderlich und erheblich sind, sowie Ausblendung von Bildern und anderen Nebeninformationen in Videoaufzeichnungen und Abbildungen soweit möglich;

- Vervollständigung der „Einwilligungserklärung“ durch Hinzufügen (beispielsweise in Form einer Liste mit Aufzeichnungspunkten) der Angaben zur Rechtmäßigkeit der Verarbeitung, zu den Fristen zur Ausübung der Rechte, zu den Modalitäten bezüglich Sperrung und Löschung von Daten und zu einer angemessenen Aufbewahrungsfrist;

- Sicherstellung, dass alle Nutzer des KPMS eine ähnliche Vertraulichkeitserklärung unterzeichnen, wie sie für Ärzte üblich ist;

- Verstärkung der Anweisung bezüglich der Nicknamen dahingehend, dass Gesundheitsdienstleister ausdrücklich dazu aufgefordert werden, sicherzustellen, dass diese keinerlei Ähnlichkeit mit den wirklichen Patientendaten haben;

- […]

[24] In den oben erwähnten Leitlinien heißt es, dass „bezüglich der Aufbewahrung medizinischer Daten [...] der EDSB generell der Auffassung [ist], dass in den meisten Fällen ein Zeitraum von 30 Jahren als das absolute Maximum für die Speicherung in diesem Zusammenhang gelten sollte.“ (Siehe Punkt 4).

- Festlegung einer konkreten Aufbewahrungsfrist, um sicherzustellen, dass die Daten nicht länger als notwendig verwahrt werden; oder aber regelmäßige Erinnerung der Gesundheitsdienstleister, die die Daten in das System eingegeben haben, daran, die Notwendigkeit der weiteren Aufbewahrung zu überprüfen.

Der EDSB begrüßt die Tatsache, dass die Kommission bereits im Nachgang zu der Sitzung vom 28. September mit der Umsetzung der Empfehlungen begonnen hat.

Brüssel, 6. November 2017

(unterzeichnet)

Wojciech RAFAŁ WIEWIÓROWSKI