

„Datenschutz als Innovati möglicher und Vertrauens

Im Titelinterview: Prof. Dr. Louisa Specht-Riemenschneider, Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Die aktuellen Reformen im Gesundheitswesen, insbesondere das Krankenhausversorgungsverbesserungsgesetz und die Digitalisierungsgesetze, zielen darauf ab, die Versorgung durch eine intensivere Datennutzung effizienter und qualitativ hochwertiger zu gestalten. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit steht dabei im Spannungsfeld zwischen dem Schutz hochsensibler Gesundheitsdaten und der Ermöglichung von Innovationen. Im Titelinterview mit „Monitor Versorgungsforschung“ spricht Prof. Dr. Louisa Specht-Riemenschneider über die „BfDI-Perspektive: Datenschutz, der Innovation und Patientenzentrierung gerecht wird“.

ionser-

sanker“

>> Ist das nicht ein Widerspruch in sich: Datenschutz als Innovationsförderer? Welche aufsichtsrechtlichen und beratenden Strategien verfolgt die BfDI, um zwischen berechtigten datenschutzrechtlichen Bedenken und vorgeschobenen Argumenten zu differenzieren und Datenschutz als integralen Qualitäts- und Vertrauensfaktor statt als pauschales Innovationshemmnis zu etablieren?

Es ist mir ein besonderes Anliegen, Datenschutz als Innovationsermöglicher und Vertrauensanker zu stärken und weiter zu etablieren. Deshalb setze ich auf frühe Information und Beratung, damit Datennutzung von Anfang an datenschutzkonform sein kann. Ich habe eine neue Organisationseinheit in der Behörde etabliert, die innovative Beratungsansätze erarbeitet, um Datenverarbeiter noch zielgerichteter und passender darin unterstützen zu können, das Datenschutzrecht einzuhalten. Mehr Beratung führt zu weniger Datenschutzrechtsverletzungen. Mit diesem Ansatz ist daher allen gedient: Betroffene werden weniger in ihren Grundrechten verletzt und Datenverarbeiter erhalten größere Rechtssicherheit. Außerdem richte ich derzeit eine Datenschutzreallaborsandbox ein, das ReguLab. Dieses wird in einer neuen Abteilung mit Schwerpunkt Dialog angesiedelt und soll bei der Entwicklung von datenschutzkonformen Lösungen ganz konkret helfen.

„Ich habe eine neue Organisationseinheit in der Behörde etabliert, die innovative Beratungsansätze erarbeitet, um Datenverarbeiter noch zielgerichteter und passender darin unterstützen zu können, das Datenschutzrecht einzuhalten.“

Wo liegen die größten datenschutzrechtlichen Herausforderungen bei der praktischen Umsetzung des Gesundheitsdatennutzungsgesetzes (GDNG), insbesondere im Hinblick auf die Datenzugangs- und Koordinierungsstelle und die Wahrung von Zweckbindung und Datenminimierung bei der Zusammenführung vielfältiger Datenquellen?

Die Datenzugangs- und Koordinierungsstelle beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) soll ausweislich der Gesetzesbegründung künftig im gesamtgesellschaftlichen Interesse mehr vertrauensvolle Forschung an verknüpften Gesundheitsdatensätzen unterschiedlicher Datenhalter ermöglichen. Maßgeblich für die Verknüpfung der Daten unterschiedlicher Datenhalter ist die eindeutige Zuordnung von Informationen aus mehreren Datenquellen zu denselben Krankenversicherten. Diese Zuordnung kann im Einzelfall eine datenschutzrechtliche Herausforderung sein. Denn im Rahmen der Aufbereitung personenbezogener Gesundheitsdaten zur Sekundärnutzung müssen die Schnittmengen mehrerer Datensätze verschiedener Dateninhaber abgeglichen werden. Wenn etwa Abrechnungsdaten der Krankenkassen mit Daten aus Krebsregistern zusammengeführt werden, muss sichergestellt werden, dass dieselbe versicherte Person korrekt identifiziert wird, ohne dass zusätzliche Identifikationsmerkmale wie Name oder Anschrift offengelegt werden. Es muss sichergestellt werden, dass durch diesen Abgleich nicht auch Rückschlüsse außerhalb des Forschungsvorhabens über die Betroffenen gezogen werden, die den Betroffenen möglicherweise benachteiligen können. Eine Verknüpfung von Gesundheits- und Beschäftigtendaten könnte beispielsweise unbeabsichtigt Rückschlüsse auf krankheitsbedingte Fehlzeiten oder Leistungsfähigkeit einzelner Arbeitnehmer zulassen. Außerdem müssen die Datenverarbeitungen bei der Datenzugangs- und Koordinierungsstelle selbstverständlich mit dem Grundsatz der Datensparsamkeit und der Verpflichtung zu technisch-organisatorischen Maßnahmen im Einklang stehen. So sollte etwa bei der Bereitstellung von Forschungsdatensätzen eine datenschutzkonforme Pseudonymisierung erfolgen, bei der direkte Identifikatoren entfernt und der Zugriff auf Entschlüsselungslisten getrennt protokolliert wird.

Wie stellt die BfDI sicher, dass die Prinzipien „Privacy by Design“ und „Privacy by Default“ von Anfang an bei der Konzeption neuer, zentraler Gesundheitsdatensammlungen – wie der Datenbank des Medizinischen Dienstes im Rahmen des KHVVG – implementiert werden?

Eine Sicherstellung von sicheren und datenschutzfreundlichen Lösungen geschieht auf verschiedenen Stufen. Erstens berate ich den Gesetzgeber im Vorfeld von Legislativmaßnahmen. Das gehört zu meinen gesetzlichen Aufgaben. Ich sensibilisiere ihn für datenschutzrechtliche Herausforderungen und zeige ihm datenschutzrechtskonforme Lösungen auf. Dazu nutze ich im Gesetzgebungsverfahren mein Stellungnahmerecht. Zweitens berate und beaufsichtige ich die jeweils datenschutzrechtlich verantwortliche Stelle bei der Umsetzung gesetzlicher Vorgaben. Die Stellen in meinem eigenen Zuständigkeitsbereich, die mit der Konzeption von Datenbanken beauftragt wurden, haben daher selbstverständlich jederzeit die Möglichkeit, sich mit konkreten Fragen und Konzepten an mich zu wenden. Je früher, desto besser und desto erfolgversprechender. Als Positivbeispiel meiner Beratungstätigkeit kann ich das Forschungsdatenzentrum Gesundheit nennen, mit dessen Betreiber, dem Bundesinstitut für Arzneimittel und Medizinprodukte, ich kontinuierlich Maßnahmen zur Gewährleistung des Datenschutzes abstimme.

Zu der von Ihnen erwähnten Datenbank: Der Gesetzgeber hat den Medizinischen Dienst Bund (MD Bund) im Rahmen des Krankenhausversorgungsverbesserungsgesetzes (KHVVG) damit beauftragt, eine standortbezogene Datenbank umzusetzen und zu betreiben. Die Verarbeitung und Veröffentlichung der Daten in der Datenbank erfolgt jedoch ohne Personenbezug. Damit sind in dieser Datenbank keine Gesundheitsdaten im Sinne von Art. 4 Nr. 15 DSGVO zu finden.

Welche technischen und organisatorischen Maßnahmen sind aus Ihrer Sicht unerlässlich, um den Zugriff auf die sensiblen Qualitäts- und Strukturdaten der geplanten zentralen Datenbanken rechtssicher

zu regeln und einen Missbrauch zu verhindern?

Pauschal lässt sich das nicht beantworten. Wenn Qualitäts- und Strukturdaten personenbeziehbar sind und in den Anwendungsbereich der DSGVO fallen, ist die jeweils datenschutzrechtlich verantwortliche Stelle nach Art. 32 DSGVO verpflichtet, den Zugang zu personenbezogenen Daten durch technisch-organisatorische Maßnahmen abzusichern. Das Schutzniveau muss der Verantwortliche für den konkreten Einzelfall ermitteln. Entscheidend kann sein, ob besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO verarbeitet werden. Soweit die Qualitäts- und Strukturdaten – wie im Falle der Datenbank des MD Bund – keinen Personenbezug aufweisen, ergibt sich jedenfalls aus der DSGVO keine Verpflichtung zur Implementierung besonderer technisch-organisatorischer Maßnahmen. Vorgaben zur IT-Sicherheit müssen aber natürlich stets beachtet werden.

„Ich spreche lieber von ‚Data Protection by Design Prinzipien', die tief in die Architektur und Prozesse einfließen."

Welche spezifischen datenschutzrechtlichen Risiken identifizieren Sie bei der routinemäßigen Erhebung von ePROMs (digitale patientenberichtete Endpunkte), oft über private Endgeräte, und welche konkreten Empfehlungen geben Sie zur Gewährleistung von Datensicherheit, transparenter Einwilligung und Zweckbindung dieser sehr persönlichen Gesundheitsinformationen?

ePROMS kommen in der Regel bei Leistungserbringern außerhalb meiner Zuständigkeit zur Anwendung. Meine Zuständigkeit ist grundsätzlich auf öffentliche Stellen des Bundes beschränkt, während niedergelassene Ärzte, Krankenhäuser und andere Leistungserbringer als kommunale oder private Stellen der Aufsicht der Landesdatenschutzbehörden unterliegen. Für Fragen und Empfehlungen zur Gewährleistung von Datensicherheit ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) die kompetente und zuständige Bundesbehörde.

Welche datenschutzrechtlichen Vorgaben sind entscheidend für die Gestaltung der Datenverarbeitung zwischen Akteuren der sektorenübergreifenden Versorgung, insbesondere im Hinblick auf die klare Definition von Verantwortlichkeiten (Joint Controllership vs. Auftragsverarbeitung)?

Sektorenübergreifende Versorgung ist zu Allererst eine Frage der Leistungserbringung. Die Beaufsichtigung von datenschutzrechtlichen Vorgaben der Leistungserbringerinstitutionen liegt bei den Landesdatenschutzbehörden. Damit eine Übermittlung von Gesundheitsdaten zwischen verschiedenen Akteuren DSGVO-konform stattfinden kann, braucht es zunächst eine rechtliche Grundlage, die die Datenübermittlung erlaubt. Dabei ist es wichtig, dass die Übertragungswege sicher sind und Verschlüsselungen benutzt werden. Im Bereich der Leistungserbringenden hat der Gesetzgeber im Zusammenhang mit der Verarbeitung personenbezogener Daten in der elektronischen Patientenakte Vorschriften geschaffen, die eine Vernetzung von bestimmten Leistungserbringenden gestattet, wenn für diese ein Zugang zur Telematikinfrastruktur (TI) besteht. Welche Leistungserbringenden an die TI angeschlossen werden, ist eine Entscheidung des Gesetzgebers. Ich halte es für essentiell, hier klare Regelungen vorzusehen, die gut verständlich sind. Die datenschutzrechtliche Verantwortlichkeit lässt sich anhand der allgemeinen Regelungen der DSGVO bestimmen. Daneben hat der Gesetzgeber auch die Möglichkeit, die Verantwortlichkeit ausdrücklich zu regeln. Das ist zum Beispiel bei der ePA passiert. Hier hat der Gesetzgeber in § 341 Abs. 4 SGB V festgelegt, dass die Krankenkassen die verantwortlichen Stellen für die ePA sind. Sie müssen also dafür sorgen, dass das Datenschutzrecht eingehalten wird.

Wie bewerten Sie die datenschutzrechtlichen Implikationen eines Systems, das Versorgungs- und Ergebnisdaten systematisch nutzt, um potenziell ineffektive Leistungen („low value care") zu identifizieren und zu reduzieren, und welche Schutzmechanismen sind erforderlich, um die Fairness solcher Analysen zu gewährleisten?

Ein solches System wurde mir bislang noch nicht zur Prüfung vorgelegt. Eine grundsätzliche „Freigabe" oder „Genehmigung" durch die Datenschutzaufsichtsbehörden für den Start solcher Systeme ist vom Gesetzgeber auch leider nicht mehr vorgesehen. Seit Inkrafttreten des Digitalgesetzes noch vor meinem Amtsantritt im Jahr 2024 kann ich Maßnahmen zum Schutz personenbezogener Daten von Versicherten nicht mehr proaktiv gegenüber der gematik einfordern. Ich kann aber auch in dieser Hinsicht erläutern und beraten und häufig werde ich damit auch gehört. Aber es besteht eben keine gesetzliche Verpflichtung mehr, meinen Rat zu befolgen. Insofern bleibt mir nur, mir im Rahmen einer Kontrolle konkret anzuschauen, ob das System im Betrieb so läuft, wie es soll.

Wie wägen Sie den Grundsatz der Datenminimierung (z. B. durch Stichproben) gegen die Forderung nach qualitativ hochwertigen, validierten Daten für Sekundärzwecke (Forschung und Steuerung) ab, um Fehlsteuerungen zu vermeiden?

Datenverarbeitungen zu wissenschaftlichen Forschungszwecken sind in der DSGVO an mehreren Stellen privilegiert. So bestehen Ausnahmen vom Grundsatz der Zweckbindung und dem Grundsatz der Speicherbegrenzung. Außerdem sind die Bestimmtheitsanforderungen an die Einwilligung als Rechtsgrundlage der Datenverarbeitung im Forschungskontext gelockert. In der wissenschaftlichen Forschung sind datenschutzkonforme Einwilligungen in Form eines „broad consent" zulässig. Das bedeutet, dass eine Einwilligung auch für zukünftige, noch unbekannte Forschungszwecke verwendet werden kann. Als Ausgleich sieht die DSGVO die Einhaltung „geeigneter Garantien" vor. Verantwortliche, die Daten zu Sekundärzwecken nutzen wollen, müssen daher geeignete Maßnahmen treffen, um möglicherweise bestehende Risiken der Datenverarbeitung zu beschränken. Diese Maßnahmen müssen aber auf den Einzelfall zugeschnitten sein. In Betracht kommen insbesondere die Anonymisierung sowie Pseudonymisierung der Daten.

Welche „Privacy by Design"-Prinzipien müssen bei Innovationsprojekten (z. B. des Innovationsfonds) von Anfang an verankert

Zitationshinweis
Specht-Riemenschneider, L., Roski, R., Stegmaier, P.: „Datenschutz als Innovationsermöglicher und Vertrauensanker“, in „Monitor Versorgungsforschung“ (01/26), S. 18–21. http://doi.org/10.24945/MVF.01.26.1866-0533.2792

werden, damit deren Datenmodelle überhaupt transfer- und skalierfähig auf Millionen Versicherte sind?

Um Datenmodelle von Beginn an transfer- und skalierfähig auf Millionen Versicherte zu gestalten, müssen „Privacy by Design“-Prinzipien, ich spreche lieber von „Data Protection by Design“-Prinzipien, tief in die Architektur und Prozesse einfließen. Diese Prinzipien umfassen, dass bei der Planung und den Design-Prozessen der Datenschutz am Anfang der Planungsprozesse stehen sollte. Datenschutzrisiken sollten frühzeitig erkannt und entsprechende Maßnahmen zur Abwendung dieser Risiken eingebaut werden. Datenschutz kann und sollte dabei als eine Kernfunktion der Projektlösung verstanden werden. Besonders dann, wenn Ende-zu-Ende-Sicherheit berücksichtigt wird, sodass Daten zu jeder Zeit sicher sind, von der Erhebung über die Verwendung bis hin zur Weitergabe und Löschung. Die Versicherten und die Menschen, die die Daten der Versicherten verwenden, sollten als Nutzende im Mittelpunkt stehen. Datenschutz muss außerdem in den Voreinstellungen vorgesehen sein, also „Data Protection by Default”. Alle Maßnahmen sollten für die Nutzenden nachvollziehbar und überprüfbar sein. Und die Gestaltung darf nicht dazu führen, dass eine Einwilligung der Nutzenden „erzwungen“ wird. Dabei ist es mir sehr wichtig, zu betonen, dass eine nutzerfreundliche Handhabe durchaus datenschutzkonform gewährleistet werden kann.

Sie können nun eine Frage an eine hochrangige Verbändevertreter:in der Pharmaindustrie rund um das Megathema Datenschutz/-verfügbarkeit stellen, die in einer der kommenden Ausgabe von „Monitor Versorgungsforschung“ beantwortet wird. Welche wäre das?

Mich würde ganz konkret interessieren, wie meine Behörde und ich dazu beitragen können, dass Datenschutz weniger als Hemmnis und mehr als Standortvorteil und Ermöglicher von Innovation wahrgenommen wird.

Frau Prof. Dr. Louisa Specht-Riemenschneider, danke für das Gespräch. <<

Das Interview führten MVF-Herausgeber Prof. Dr. Reinhold Roski und MVF-Chefredakteur Peter Stegmaier.



Prof. Dr. Louisa Specht-Riemenschneider

ist seit September 2024 Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. Sie war zuvor Inhaberin des Lehrstuhls für Bürgerliches Recht, Recht der Datenwirtschaft, des Datenschutzes, der Digitalisierung und der Künstlichen Intelligenz der Rheinischen Friedrich-Wilhelms-Universität Bonn. Sie studierte Rechtswissenschaft in Bremen, promovierte und habilitierte in Freiburg und hatte anschließend Professuren in Köln und Passau inne. Als Direktorin leitete sie sowohl das Institut für Handels- und Wirtschaftsrecht der rechts- und staatswissenschaftlichen Fakultät sowie das Zentrum für Medizinische Datennutzbarkeit und Translation (ZMDT). Zudem begleitete sie die Gründung des Dateninstituts unter Federführung des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) und des Bundesministeriums des Innern und für Heimat (BMI).

55,7% mit geringer Health Literacy

>> Die gute Nachricht der Studie „Gesundheitskompetenz in Zeiten gesellschaftlicher Unsicherheiten”: In den letzten fünf Jahren hat sich die Gesundheitskompetenz in Deutschland um 3,1 Prozentpunkte verbessert. Wer die Ergebnisse des HLS-GER-3-Studie, durchgeführt von der Universität Bielefeld (Interdisziplinäres Zentrum für Gesundheitskompetenzforschung (IZGK) in Kooperation mit der Charité – Universitätsmedizin Berlin und der Hertie School Berlin, etwas genauer liest, wird aber dennoch nicht ganz begeistert sein. Nach der neuen Studie, dem Health Literacy Survey Germany 3 (HLS-GER 3), weisen immerhin 55,7% der Bevölkerung in Deutschland eine geringe Gesundheitskompetenz auf. In der zurückliegenden Studie, dem HLS-GER 2, waren es noch 58,8%. Im Einzelnen verfügen im HLS-GER 3:

- 18,1% der Bevölkerung in Deutschland über eine exzellente und 26,3% über eine ausrei-chende Gesundheitskompetenz (zuvor waren es 14,7% und 26,5%),
- 28,6% (30,4%) über eine problematische und 27,1% (28,4%) über eine inadäquate Gesundheitskompetenz.

Zudem ist die Gesundheitskompetenz nach wie vor ungleich in der Bevölkerung verteilt. Zu den Gruppen, die überdurchschnittlich häufig über eine geringe Gesundheitskompetenz verfügen, gehören Menschen (Angaben im Vergleich zum Vorjahr):

- mit niedrigem Sozialstatus: 73,3% (71,9%),
- mit finanzieller Deprivation: 72,3% (72,9%),
- mit niedrigem Bildungsniveau: 71,1% (78,3%),
- ab 65 Jahren: 62,8% (65,1%),
- mit mehreren chronischen Erkrankungen: 61,6% (65,1%). <<

MD stellt 3.301 Fehler fest

>> 12.304 fachärztliche Gutachten zu vermuteten Behandlungsfehlern hat der Medizinische Dienst im Jahr 2024 bundesweit erstellt. In jedem 4. Fall (3.301 Fälle) stellten die Gutachter:innen einen Behandlungsfehler mit Schaden fest. In jedem 5. Fall (2.825 Fälle) war der Fehler ursächlich für den erlittenen Schaden. Das geht aus der aktuellen Jahresstatistik zur Behandlungsfehlerbegutachtung des Medizinischen Diensts hervor. <<

Link: https://t1p.de/diyeg