Stiftung Datenschutz; Karl-Rothe-Straße 10-14; 04105 Leipzig

Bundesministerium für Gesundheit

Referat 511

11055 Berlin

Per E-Mail an 511@bmg.bund.de

14. August 2023

Stellungnahme

zum Referentenentwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz – GDNG)

Die Stiftung Datenschutz fördert die Belange des Datenschutzes. Wir bedanken uns für die Möglichkeit einer Stellungnahme. Wegen der Kürze der zur Verfügung stehenden Zeit kann nur zu ausgewählten Aspekten des grundrechtlichen Datenschutzes Stellung genommen werden.

A. Grundsätzliche Anmerkungen

Einleitend soll betont werden, dass sich die Forschung mit Gesundheitsdaten durch Organisationen und der Schutz der personenbezogenen Daten der Betroffenen (Patientinnen und Patienten, Versicherte)) zwar nicht grundsätzlich widersprechen, aber doch in einem grundrechtlichen Spannungsverhältnis stehen, das im Rahmen der Gesetzgebung für eine Gesundheitsdatennutzung in Einklang zu bringen ist. So wird beispielsweise das Grundrecht auf Wissenschaftsfreiheit aus Art. 5 Abs. 3 GG, auf das sich Forschende berufen können, bei der Nutzung von personenbezogenen Gesundheitsdaten durch das Grundrecht der Betroffenen auf Datenschutz aus Art. 8 Abs. 1 der EU-Grundrechtcharta, insbesondere in seiner Ausprägung als Recht auf informationelle Selbstbestimmung aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1Absatz 1 Grundgesetz eingeschränkt.

Aufgabe des Datenschutzrechts bzw. der datenschutzrechtlichen Bestimmungen ist es, den Ausgleich der negativen Folgen, die durch den Zugriff einer Organisation (Datennutzende) auf personenbezogene Daten und durch deren weitere Nutzung erfolgt, zu gewährleisten. Die Bedingungen, unter denen personenbezogener Daten genutzt werden dürfen, ist zum Schutz der Grundrechteträgerinnen und -träger maßgeblich in der Datenschutz-Grundverordnung geregelt.

Den datenschutzrechtlichen Bestimmungen eines GDNG kommt entsprechend die Funktion zu, die Datenverarbeitung bei Nutzung von Gesundheitsdaten nach Maßgabe der DSGVO so zu regeln, d.h. unter Bedingungen zu stellen, dass dabei einerseits das durch die Verarbeitung

für die Betroffenen realisierte Risiko weitestgehend eingeschränkt und kontrolliert werden kann und andererseits Verarbeitungen, deren Risiken unverhältnismäßig und mit den Grundrechten und Grundfreiheiten der Betroffenen nicht in Einklang zu bringen sind, ausgeschlossen werden.

Im Folgenden wird zum vorgelegte Entwurf daher dahingehend Stellung genommen, ob es dem Entwurf - ausgehend von der Beantwortung der Frage, welche Risiken durch die jeweils spezifische Verarbeitung für die Betroffenen erzeugt werden - gelingt, Kriterien für die Verarbeitungsbefugnisse durch die Gesetzgebung so festzuschreiben, dass dem Verantwortlichen aufgegeben wird, die Verarbeitung (grundrechtlich) zu rechtfertigen, die Verarbeitung minimal invasiv zu gestalten und Schutzmaßnahmen zur Verringerung der operativen Risiken zu implementieren und dauerhaft zu betreiben.[1] Dabei müssen der Schutz der Daten als Zweck der IT-Sicherheit der Organisation und der Schutz der Grundrechte und Grundfreiheiten als der Zweck der datenschutzrechtlichen Regelungen betrachtet und gewährleistet werden.

B. Zweck des vorgelegten Referentenentwurfs

Der vorgelegte Referentenentwurf zu einem Gesundheitsdatennutzungsgesetz soll u.a. den Zugang für Organisationen zu dezentral und zentral gehaltenen Gesundheitsdaten bei anderen Stellen verbessern und eine Verknüpfung der dort zu einer gesetzlich versicherten Person vorliegenden Gesundheitsdaten wie z.B. Diagnosen, Behandlungen, Operationen, Arzneimittel, Zuzahlungen, Krankengeld-Informationen und viele andere Kosten- und Leistungsdaten sowie Geburtsjahr, Geschlecht und Postleitzahl bei den Organisationen ermöglichen. Dazu soll eine zentrale Datenzugangs- und Koordinierungsstelle (Artikel 1, § 1 GDNG-E) geschaffen werden, die einen Katalog über verfügbare Datenarten führt und zwischen den beteiligten datenhaltenden und datensuchenden Stellen vermittelt sowie Anträge auf Datenzugang nach Maßgabe des § 2 Abs. 2 GDNG-E prüft und genehmigt.

C. Artikel 1 – Gesundheitsdatennutzungsgesetz

1. Zwecke der Verarbeitung

Soweit in § 2 GDNG-E die Rechtgrundlage für eine Verknüpfung von Daten des Forschungsdatenzentrums und der Krebsregister geregelt wird, fehlt es an einer klaren Zweckbestimmung. Jedes Datenverarbeitungsverfahren einschließlich einer Weiterverarbeitung hat sich nach Maßgabe des Art. 5 Abs. 1 Buchstabe b DSGVO i.V.m. Art. 6 Abs. 1 S. 1 Buchstabe e und Abs. 3 Buchstabe b DSGVO auf festgelegte, eindeutige und legitime Zwecke zu beziehen. Dies gilt auch für wissenschaftliche Forschungszwecke. So wäre näher zu bestimmen, unter welchen Bedingungen ein Forschungsvorhaben nach § 2 Abs. 1 GDNG-E vorliegt. Erst dann kann festgestellt werden, ob eine Erforderlichkeit der Verarbeitung i.S. der Art. 6 Abs. 1 S. 1 Buchstabe e und Abs. 3 Buchstabe b DSGVO gegeben ist. Damit geht eine positive Feststellung einher, dass ein öffentliches Interesse an der Verarbeitung im Rahmen des Forschungsvorhabens besteht. Es wäre z.B. festzulegen, ob eine Nutzung allgemeinwohlorientiert oder auch rein kommerziell erfolgen darf. Eine Feststellung, dass „kein überwiegendes öffentliches Interesse an einem Unterlassen der Verknüpfung und gemeinsamen Verarbeitung der Dateien besteht“, wie dies § 2 Abs. 2 Nr. 3 GDNG-E vorsieht,

[1] *Bock*, Es geht um Macht, in: Privacy in Germany 02.22, S. 50.

reicht zur Erfüllung der Vorgaben aus Art. 6 Abs. 1 S. 1 Buchstabe e und Abs. 3 Buchstabe b DSGVO nicht aus.

2. Verknüpfung von Gesundheitsdaten

Informationen über Krankheit, Therapie und Heilungserfolg sind wichtig für das Verständnis von Krankheitsverläufen und die Weiterentwicklung von Medikamenten. Solche Informationen können oft statistisch und damit anonym erhoben und genutzt werden. Informationen, die auf eine bestimmbare Person rückführbar sind, stehen hingegen unter dem besonderen Schutz des Datenschutzrechts, dessen Aufgabe und Ziel es ist, die Grundrechte und Freiheiten von Menschen zu gewährleisten. Auch bei einer Privilegierung der Verarbeitung personenbezogener Daten zu Forschungszwecken im Gesundheitswesen sind angemessene Sicherungsmaßnahmen vorzusehen. Art. 89 Abs. 1 DSGVO benennt die Pseudonymisierung als eine mögliche Maßnahme. Weitere besondere Sicherungsmaßnahmen lässt der Gesetzentwurf noch vermissen.

Gem. Art. 89 Abs. 1 DSGVO stehen Verarbeitungen von personenbezogenen Daten zu Forschungszwecken zudem unter dem Vorbehalt der Einhaltung des Grundsatzes der Datenminimierung. Dies bedeutet, dass eine Verarbeitung so ausgestaltet werden soll, dass zur Erreichung der Zwecke besonders wenig personenbezogene Daten erforderlich werden. Kann ein Zweck auch durch die Nutzung anonymer Daten erreicht werden, so soll dieser Weg i.S.d. Art. 89 Abs. 1 S. 4 DSGVO verfolgt werden. Eine solche Regelung sieht der Entwurf bislang nicht vor.

In der Gesetzesbegründung wird zutreffend davon ausgegangen, dass „durch die Zusammenführung der Daten zusätzliche Informationen zu den Versicherten generiert werden, die in Abwägung zur Notwendigkeit für die Beantwortung der Forschungsfrage erneut bewertet werden“[2] müssten. Es wird begrüßt, dass eine Prüfung durch die Datenzugangs- und Koordinierungsstelle bereits *vor* der Verknüpfung erfolgen soll. Allerdings lassen die Anforderungen aus § 2 Abs. 2 Nr. 1 bis 3 GDNG-E gerade nicht erkennen, dass durch die Zusammenführung entstehende zusätzlicher Informationen im Rahmen der Prüfung Berücksichtigung finden sollen. Eine solche Regelung wäre einzuführen.

3. Pseudonymisierung und anlassbezogene Forschungskennziffer, § 2 Abs. 5-9 GDNG-E

Es wird begrüßt, dass die Verarbeitung von verknüpften Gesundheitsdaten durch den Datennutzenden in einer im Einzelfall festzulegenden sicheren Verarbeitungsumgebung einer öffentlichen Stelle stattfinden soll. Die Voraussetzungen für eine solche Verarbeitungsumgebung sollen durch die Datenzugangs- und Koordinierungsstelle als Konzepte erarbeitet (§ 1 Abs. 2 Nr. 8 Buchstabe a GDNG-E) und durch Rechtsverordnung ohne Zustimmung durch das Bundesministerium für Gesundheit (§ 2 Abs. 9 GDNG-E) bestimmt werden. Die Übermittlungen der beantragten Daten durch die datenhaltenden Stellen soll zusammen mit einer anlassbezogenen Forschungskennziffer erfolgen. Auch die Bedingungen hierfür sollen noch erarbeitet werden. Anlassbezogene Kennziffern, die keine sprechende Zuordnung zu einer Person erlauben, sind grundsätzlich vorzuziehen.

[2] Referentenentwurf des Bundesministeriums für Gesundheit, S. 28.

Für eine sichere Pseudonymisierung ist das verwendete Verfahren maßgeblich. Eine schwache Pseudonymisierung bietet für Gesundheitsdaten keinen hinreichenden Schutz. Bei Gesundheitsdaten haben die betroffenen Personen generell einen hohen Schutzbedarf, der durch die verwendeten IT-Komponenten umzusetzen ist. Für die technischen Maßnahmen - wie eine Pseudonymisierung - bedeutet dies, dass das durch die Verarbeitung vermittelte Risiko für den Betroffenen durch die Gestaltung der Verarbeitung und die technischen und organisatorischen Maßnahmen soweit zu verringern ist, bis das Schutzniveau den Anforderungen der DSGVO, insbesondere den Grundsätzen aus Art. 5 Abs. 1 DSGVO entspricht. Kann mit nur wenigen Datenpunkten eine Re-Identifizierung erfolgen, reicht die Vorgabe einer Pseudonymisierung nicht aus.[3] Es ist vielmehr sicherzustellen, dass auch Betroffene, die unter seltenen Krankheiten oder bestimmten Kombinationen von Krankheiten oder untypischen Krankheitsverläufen leiden, oder die in einer dünn besiedelten Gegend leben, ein angemessenes Schutzniveau gewährleistet wird. Eine solche Maßgabe für die Ausgestaltung der Rechtsverordnung durch das Bundesministerium für Gesundheit, ist dem vorgelegten Referentenentwurf nicht zu entnehmen.

Ein Schutz der Betroffenen wird auch nicht dadurch hinreichend gewährleistet, dass den Betroffenen eine Opt-Out Möglichkeit, d.h. ein Widerspruchsrecht aus der Verarbeitung angeboten wird. Gerade Menschen mit seltenen Krankheiten haben ein besonderes individuelle Interesse an Forschungsfortschritten. Dieses Interesse ist nachvollziehbar, darf aber nicht zu einer Herabsetzung des Grundrechtsschutzes bei der Verarbeitung führen. Dem durch wirkungsvolle Maßnahmen entgegen zu wirken, ist Aufgabe des Gesetzgebers.

4. Erweiterung der Verarbeitungsbefugnisse von Leistungserbringern der Gesundheitsversorgung, § 4 GDNG-E

In § 4 Abs. 1 GDNG-E sollte klargestellt werden, um welche Art Qualitätssicherung es sich als Zweck der Verarbeitung handeln soll. Die Regelung, die Möglichkeiten zur individuellen Abschätzung des Eintritts gesundheitlicher Risiken individueller Versicherter schafft, gibt Anlass, weitere Einschränkungen der Ergebnisse der Datennutzung vorzusehen, um den allgemeinen Zweck von Krankenkassen als Solidargemeinschaften sicherzustellen. Im Hinblick auf die Gesetzesbegründung sei angemerkt, dass Art. 9 Abs. 2 Buchstaben i und j DSGVO nach Auffassung des EDPB keine Rechtsgrundlagen der Verarbeitung darstellen, sondern eine Ausnahme vom generellen Verarbeitungsverbot der in Art. 9 Abs. 1 genannten Datenkategorien zu den dort genannten Zwecken.

5. Publikationspflicht bei Verarbeitung im öffentlichen Interesse, § 5 GDNG-E

Eine Publikationspflicht der Ergebnisse von Forschungsprojekten in anonymisierter Form, die mit öffentlichen Geldern gefördert wurden oder auf Grundlage gesetzlicher Verarbeitungsvorschriften möglich werden, wird grundsätzlich begrüßt. Wünschenswert wäre, wenn auch Hinweise für begründete Ausnahmefälle, in denen die Datenzugangs- und Koordinierungsstelle von einer Veröffentlichungspflicht befreien kann, aufgenommen würden.

Unklar bleibt, warum in der Überschrift des Entwurfs zu § 5 auf das öffentliche Interesse an der Verarbeitung und nicht auf das öffentliche Interesse an der Publikation abgehoben wird.

[3] *Rehak*, Zentralisierte Gesundheitsdaten, netzpolitik.org 19.05.2023, abrufbar unter https://netzpolitik.org/2023/grundrechte-report-2023-zentralisierte-gesundheitsdaten/.

Auch in der Begründung des Entwurfs wird für die Publikationspflicht auf das erhebliche öffentliche Interesse an der Bekanntmachung, Qualitätsprüfung und Dokumentation wissenschaftlicher Erkenntnisse abgestellt.

D. Art. 2 - SGBV-E

1. Forschungsdatenzentrum Gesundheit

Die Zentralisierung aller Abrechnungsdaten der gesetzlich Krankenversicherten in einer einzigen Datenbank beim Forschungsdatenzentrum Gesundheit stellt ein erhebliches Risiko für die Freiheiten und Rechte der Betroffenen dar.[4] Für die im Gesundheitsdatennutzungsgesetz beschriebenen Zwecke, insbesondere die medizinische Forschung, würde es genügen, wenn die Daten dezentral gespeichert und nur projektbezogen temporär zusammengeführt würden.[5]

2. Freigabe der elektronischen Patientenakte ohne Einwilligung, § 363 Abs. 1, 5 SGBV-E

Die Daten aus der elektronischen Patientenakte der gesetzlich Versicherten soll zukünftig ohne Einwilligung der Versicherten zugänglich gemacht werden. Grundsätzlich ermöglicht die DSGVO über Art. 6 Abs. 1 S. 1 Buchstabe e i.V.m. Art. 89 Abs. 1 DSGVO eine solche gesetzliche Regelung, soweit angemessene Sicherheitsmaßnahmen (engl. safeguards) durch den Gesetzgeber vorgesehen werden. Ob dies der Fall ist, kann vorliegend nicht abschließend beurteilt werden, da eine das Gesetz begleitende Datenschutzfolgenabschätzung bislang nicht vorgelegt wurde. Tatsächlich wird durch diese gesetzliche Regelung der Grundrechtsschutz der gesetzlich Versicherten gegenüber dem der privat Versicherten abgesenkt.

Die Möglichkeit, der Verarbeitung nach Maßgabe des § 363 Abs. 5 SGBV-E zu widersprechen, wird dadurch erschwert, dass der Widerspruch nur über die Benutzeroberfläche eines geeigneten Endgerätes erklärt werden kann. Damit wird dem Teil der gesetzlich Versicherten, der entweder keinen Zugang zu geeigneten Geräten hat oder sich mit der Nutzung schwertut, der analoge Weg des Widerspruchs abgeschnitten. Grundsätzlich sollen alle digital verfügbaren Möglichkeiten den Betroffenen auch analog zur Verfügung stehen. Der Gesetzgeber sollte daher auch eine analog Widerspruchsmöglichkeit vorsehen.

E. Datenschutzfolgenabschätzung nach Art. 35 DSGVO

Das Gesundheitsdatennutzungsgesetz führt zu einer Verarbeitung von Gesundheitsdaten in großem Umfang bei hohem Risiko. Die DSGVO sieht in diesen Fällen eine Datenschutzfolgenabschätzung nach Maßgabe des Art. 35 vor. Der Gesetzentwurf will die Nutzbarkeit von Gesundheitsdaten durch eine rechtliche und technische Regelung der Verknüpfbarkeit von Daten verbessern. Dabei geht es im Entwurf nicht nur um die Zusammenführung von Daten verschiedener Personen, sondern um die Verknüpfung der Daten zu einer Person aus unterschiedlichen Quellen. Dadurch entsteht die Möglichkeit, weitreichende und aussagekräftige Persönlichkeitsprofile zu erstellen. Das sog. Profiling ist bislang insbesondere im Kontext der Datenerfassung durch Sicherheitsbehörden und die Werbeindustrie bekannt. Die in diesem Kontext vorgetragenen Kritikpunkte und

[4] *Nadraq*, Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web, https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web.

[5] *Rehak*, in: Grundrechte-Report 2023, hrsg. v. Derin, Gössner et al., Frankfurt a.M. 2023, S. 32 (33).

Anforderungen für eine datenschutzkonforme Ausgestaltung gelten auch für den Gesundheitsbereich.[6]

Des weiteren erlaubt § 4 DGNG-E den Leistungserbringern explorative Analysen sowie § 287a ESGBV-E den Kranken- und Pflegekassen automatisierte Verarbeitungen zur (Früh-) Erkennung von Krankheiten. Wie diese ausgeführt werden sollen, bestimmt der Entwurf nicht näher. Automatisierte Verfahren zur Früherkennung werden den gesamten Datenbestand mittels Verfahren, wie sie z.B. beim Screeing oder auch durch die sog. Rasterfahndung[7] im Sicherheitsbereich bekannt geworden sind, auf Kennzeichen von Krankheitsmerkmalen durchsuchen. Diese Suchmethoden produzieren regelmäßig falsch positive Ergebnisse[8], die mit erheblichen Belastungen für die Betroffenen einhergehen.[9] Soweit der Gesetzentwurf die Voraussetzungen für solche Formen der Verarbeitung personenbezogener Daten nicht regelt, bzw. eine Risikoabschätzung noch im Rahmen einer weiteren Gesetzesbegründung nach Maßgabe des Art. 35 Abs. 10 DSGVO erfolgt, sollten für diese Verarbeitungen aufgrund der erheblichen Risiken für die Rechte und Freiheiten der Betroffenen Datenschutzfolgenabschätzungen verbindlich vorgesehen werden. Aus dem im Grundgesetz verankerten Recht auf informationelle Selbstbestimmung und aus dem Grundrecht auf Datenschutz in Artikel 8 der EU-Grundrechtecharta ergibt sich die staatliche Pflicht, Betroffene bei der Verarbeitung von Gesundheitsdaten angemessen vor negativen Folgen zu schützen. Ein solcher Schutz kann nur gewährleistet werden, wenn die absehbar hohen Risiken einer Verarbeitung und ihre Folgen angemessen in den Blick genommen werden und entsprechende technische und organisatorische Maßnahmen getroffen werden, *bevor* eine Verarbeitung besonderer Arten von personenbezogenen Daten erfolgt.

F. Review nach Art. 35 Abs. 11 DSGVO

Das Gesundheitsdatennutzungsgesetz sollte aufgrund der Schwere der Eingriffe in die Rechte und Freiheiten der Betroffenen bei der Verarbeitung besonderer Arten von personenbezogenen Daten neben einer Evaluierungspflicht der verantwortlichen Stellen auch eine Gesetzes-Evaluierung innerhalb eines angemessenen Zeitraums vorsehen.

G. Diskussionspunkte

Folgende Punkte werden innerhalb der Bundesregierung noch diskutiert, zu denen wir um eine ausdrückliche Rückmeldung gebeten wurden:

1. Die Vereinfachung des Verfahrens beim Zugang zu Daten der Kranken- und Pflegeversicherung für Forschungszwecken nach § 75 SGB X, soweit eine Einwilligung der betroffenen Versicherten vorliegt.
2. Die Widerspruchsrechte der Versicherten und diesbezügliche Informationen zur Transparenz für Verbraucher*innen.

---

[6] Grundlegend EDPB, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01.

[7] *Schulzki-Haddouti*, Alltäglich Rasterfahndung, in: c't 2010, https://www.heise.de/news/Alltaegliche-Rasterfahndung-890108.html.

[8] Eine falsch-positiv-Rate (auch Ausfallrate; englisch fallout oder false positive rate) gibt den Anteil der fälschlich als positiv klassifizierten Objekte an, die in Wirklichkeit negativ sind. Ein tatsächlich Gesunder wird dann zu Unrecht als krank diagnostiziert.

[9] *McKinney, Sieniek, Godbole et al.:* International evaluation of an AI system for breast cancer screening. In: Nature 577, 89–94 (2020).

Zu 1.
Die Einwilligung ist eine der möglichen Rechtfertigungen, in die Grundrechte der Betroffenen einzugreifen. Sie wird weder in Art. 8 der EU Grundrechte-Charta noch in der DSGVO privilegiert. Im deutschen Verfassungsrecht wird das Grundrecht auf informationelle Selbstbestimmung hingegen oftmals mit dem Grundrecht auf Datenschutz gleichgesetzt. Grundlage des Grundrechts auf informationelle Selbstbestimmung ist der Gedanke, dass die Kontrolle und Beherrschbarkeit der Entscheidungen, die die eigene Person betreffen, als Ausfluss des allgemeinen Persönlichkeitsrechts und der Menschenwürde erachtet werden. Kontrolle und Beherrschbarkeit von Sachverhalten und Entscheidungen gelingen aber in erster Linie, wenn die Entscheidung informiert erfolgt. Die Wirksamkeit einer datenschutzrechtliche Einwilligung nach Art. 7 DSGVO ist daher gem. Art. 4 Nr. 11 DSGVO eine freiwillig, für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung. Eine hinreichende Informiertheit wird bei der Komplexität und Vielfalt von Forschungsvorhaben nicht gegeben sein. Die Erfüllung aller Merkmale muss im Einzelfall, also für jede einzelne Person, und für die jeweils konkreten Zwecke nachweisbar sein. Dies ist für die verfolgten Zwecke des GDNG kaum umsetzbar. Zudem ist eine Einwilligung gegenüber Behörden und bei behördlichen Maßnahmen nur dann zulässig, wenn sie nicht im klassischen Subordinationsverhältnis erfolgt, weil in diesen Fällen nicht von einer Freiwilligkeit i.S. des Gesetzes auszugehen ist.

Zu. 2.
Die Wahrnehmung eines Widerspruchsrecht sollte keine erhebliche Hürde darstellen. Das Recht sollte sowohl analog, d.h. schriftlich oder zu Protokoll in Person, als auch digital wahrgenommen werden können.
Im Kontext von Gesundheitsdaten sollten die Rollen der Betroffenen zudem zutreffend bezeichnet werden. Es wird sich in diesem Anwendungskontext nur in seltenen Fällen um Verbraucherïnnen handeln, sondern zumeist um Patientïnnen und Versicherte.

H. Sanktionierung
Es wird im Begleitschreiben vom 4. August 2023 ausgeführt, das Bundesministerium für Gesundheit strebe an, im Gesundheitsdatennutzungsgesetz auch den Schutz personenbezogener Gesundheitsdaten als besonders sensible Daten zu verbessern.
Daher werde angestrebt, im Gesundheitsdatennutzungsgesetz die unbefugte Offenbarung, Weitergabe und Nutzung von Gesundheitsdaten, die für Forschungszwecke verfügbar gemacht wurden, strafrechtlich zu sanktionieren. Eine solche Sanktionierung sei dringend geboten, um die Interessen der Bürgerinnen und Bürger zu wahren. In möglichen weiteren Maßnahmen zum Schutz personenbezogener Gesundheitsdaten müssen nach Auffassung des Bundesministeriums für Gesundheit auch diejenigen einbezogen werden, die diese Gesundheitsdaten erfassen, verarbeiten oder mit diesen arbeiten. Eine gemeinsame Positionierung der Bundesregierung zur Umsetzung werde zeitnah erfolgen. Dies wird begrüßt. Jedoch ist dazu grundsätzlich anzumerken, dass auch eine strafrechtliche Sanktionierung der Nutzung von personenbezogenen Gesundheitsdaten stets nur eine schwache Form des Schutzes der Freiheiten und Grundrechte der Betroffenen darstellt. Nicht nur können Gesetze geändert werden und eine Sanktionierung entfallen, sondern es bleibt auch fraglich, welche präventive Wirkung eine strafrechtliche Sanktionierung entfalten kann. Angesichts eines hohen monetären

Wertes von Gesundheitsdaten auf dem Schwarzmarkt im Darknet[10] und Angreifern aus dem Ausland bleibt der tatsächliche Schutz der Freiheiten und Grundrechte durch eine Sanktionierung in diesen Sachverhalten aus. Der Wert für Angreifer und damit die Problematik von Gesundheitsdaten ergibt sich aus dem Umstand, dass diese Daten stets mit dem Menschen verknüpft bleiben, weil sie eine eindeutige Identifizierung der natürlichen Person ermöglichen oder bestätigen, vgl. Art. 4 Nr. 14 DSGVO. Während eine Kontonummer ersetzt werden kann, ist dies bei identifizierenden Gesundheitsdaten, insbesondere den biometrischen Daten, nicht möglich. Angriffsziele sind dabei nicht mehr nur Gesundheitsorganisationen wie Krankenhäuser, sondern auch Forschungseinrichtungen.[11] Während eine Strafbewehrung eine abschreckende Wirkung auf sogenannte Innentäter haben kann, die mit internen Berechtigungen auf die Systeme und Daten zugreifen, bleibt eine Sanktionierung bei Angriffen aus Drittländern wirkungslos. Im Hinblick auf eine Zunahme durch Angriffe von Innentätern erscheint eine Strafbewehrung sinnvoll. Eine Sanktionierung kann aber immer nur flankierende Schutzmaßnahme sein. Das datenschutzrechtliche Risiko einer unbefugten Verarbeitung wird damit nicht wirksam erfasst. Dies gelingt allein durch technische und organisatorische Maßnahmen, die Zugriffe auch auf pseudonymisierte Daten protokollieren und unberechtigte Weiterverarbeitungen verhindern.

[10] Vgl. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-cybersicherheit-2021.html.

[11] https://www.heise.de/hintergrund/Gesundheitsdatenbanken-und-die-virtuelle-Verwundbarkeit-des-Patienten-7532452.html?seite=3.