Netzwerk Datenschutzexpertise GbR
Dr. Thilo Weichert
Waisenhofstr. 41
D-24103 Kiel
Tel.: +49 431 9719742
E-Mail: weichert@netzwerk-datenschutzexpertise.de

DR. THILO WEICHERT, WAISENHOFSTR. 41, 24103 KIEL

An das
Bundesministerium für Gesundheit
11055 Berlin

Kiel, den 04.12.2025

per Mail: poststelle@bmg.bund.de

Stellungnahme zum Referentenentwurf des Bundesministeriums für Gesundheit (BMG) „Entwurf eines Gesetzes zur Stärkung von Medizinregistern und zur Verbesserung der Medizinregisterdatennutzung
Ihre Web-Veröffentlichung, Stand 27.10.2025,
https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/M/Medizinregistergesetz_RefE.pdf

Sehr geehrte Damen und Herren,

zu dem oben im Betreff genannten Gesetzentwurf nehme ich wie folgt Stellung:

I. Normative Grundlagen

Die Intention des Gesetzentwurfs, **strukturierte Gesundheitsdaten aus Medizinregistern** zur Qualitätssicherung, Krankheitsbekämpfung und für die Forschung zur Verfügung zu stellen, wird begrüßt. Die Initiative reiht sich ein in europäische und nationale Regelungen, die darauf abzielen die Sekundärnutzung von Gesundheitsdaten zu erleichtern. Hierzu bestehen schon der Europäische Gesundheitsdatenraum (European Health Data Space – EHDS), das Gesundheitsdatennutzungsgesetz (GDNG) sowie Regelungen im Sozialgesetzbuch fünf (SGB V) insbesondere zum Forschungsdatenzentrum Gesundheit (FDZ) in den §§ 303a ff. SGB V.

Der Entwurf setzt eine Vorgabe der **Koalitionsvereinbarung** der schwarz-roten Bundesregierung von April 2025 um: „Zur besseren Datennutzung setzen wir ein Registergesetz auf und verbessern die Datennutzung beim Forschungsdatenzentrum Gesundheit. Gleichzeitig ist der Schutz von sensiblen Gesundheitsdaten unabdingbar. Deshalb wirken wir auf eine konsequente Ahndung von Verstößen hin“ (S. 111).

Der Koalitionsvertrag anerkennt die **besondere Schutzbedürftigkeit** von Gesundheitsdaten. Diese findet ihre rechtliche Grundlage in Art. 9 Abs. 1 Europäische Datenschutz-Grundverordnung (DSGVO), wonach u.a. die Verarbeitung besonderer Kategorien personenbezogener Daten, wozu genetische Daten, Gesundheitsdaten und Daten zum Sexualleben gehören, grundsätzlich untersagt wird. Als Ausnahme dieses Grundsatzes ist in Art. 9 Abs. 2 DSGVO vorgesehen, dass auf gesetzlicher Grundlage eine Verarbeitung erlaubt ist, wenn dies z.B. erforderlich ist gemäß dem „Recht der sozialen Sicherheit und des Sozialschutzes“ (lit. b), „zum Schutz lebenswichtiger Interessen“ (lit. c), „aus Gründen eines erheblichen öffentlichen Interesses“ (lit. g), „für Zwecke der Gesundheitsvorsorge“ oder für „die Versorgung und Behandlung im Gesundheits- und Sozialbereich“ (lit. h), „aus Gründen

des öffentlichen Interesses im Bereich der öffentlichen Gesundheit“ (lit. i) oder für wissenschaftliche oder historischen Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1“ (lit. j).

In Art. 89 Abs. 1 DSGVO werden „**geeignete Garantien**“ gefordert, die sicherstellen, „dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird“.

Das geplante Medizinregistergesetz (MRG-E) regelt nicht die Nutzung der Daten für primäre (Behandlungs-)Zwecke, sondern eine **Weiterverarbeitung für sekundäre Zwecke**. Dies bedarf einer gesetzlichen Grundlage für die Erfüllung einer Aufgabe, „die im öffentlichen Interesse liegt“ (Art. 6 Abs. 1 lit. c, e DSGVO), wobei die Verarbeitung „in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen“ muss (Art. 6 Abs. 3 DSGVO, vgl. S. 52). Diese anderen Zwecke müssen mit dem ursprünglichen Zweck „vereinbar“ sein, wobei insbesondere das Verhältnis „zwischen den betroffenen Personen und dem Verantwortlichen“, „die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen“ sowie „das Vorhandensein geeigneter Garantien“ berücksichtigt werden müssen (Art. 6 Abs. 4 DSGVO).

Das Verhältnis der Betroffenen zu den primär Verantwortlichen in Gesundheitseinrichtungen, den Ausübenden von Heilberufen, wird spezifisch geschützt durch das **Patientengeheimnis**, das in § 203 Strafgesetzbuch (StGB), in § 9 Musterberufsordnung der Ärztekammern (MBOÄ) sowie in vielen weiteren Regelungen Eingang gefunden hat. Die Geltung des Patientengeheimnisses wird in Art. 9 Abs. 3 DSGVO ausdrücklich anerkannt.

Die durch die DSGVO gemachten Vorgaben sind bei der Normierung der Verarbeitung von Daten in Medizinregistern verbindlich.

II. Grundüberlegungen

Das geplante MRG soll ein wesentlicher Baustein zur Schaffung einer validen Datengrundlage im Gesundheitswesen und zur Entwicklung des EHDS sein. Hierfür soll ein **Zentrum für Medizinregister** (ZMR) im Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) eingerichtet werden, das ein Medizinregisterverzeichnis führt und Medizinregister in einem spezifischen Verfahren qualifizieren kann.

Der Entwurf geht davon aus, dass das Gesetz auf 356 in Deutschland bestehende **Medizinregister** anwendbar sein kann und jedenfalls auf 276 aktiv betriebene Register tatsächlich Anwendung finden wird (S. 23 f.).

Qualifizierte Medizinregister sollen zum Erhalt, zur Speicherung und zur Weitergabe von **Gesundheitsdaten auf gesetzlicher Grundlage** befugt werden. Dies gilt auch für die Weitergabe an und Weiterverarbeitung durch Dritte in pseudonymisierter Form.

Damit greift der Entwurf die Regelung von **Art. 51 Abs. 1 EHDS** auf, wonach Gesundheitsdateninhaber ihre Daten zur Sekundärnutzung zur Verfügung zu stellen haben u.a. als Verantwortliche von „bevölkerungsbezogenen Gesundheitsdatenregistern, wie etwa Registern zur öffentlichen Gesundheit“ (lit. k), „medizinischen Registern und Mortalitätsregistern“ (lit. l) oder Registern für Arzneimittel und Medizinprodukte (lit.o).

Die Umsetzung des **EHDS** und insbesondere das **GDNG** weisen bisher noch starke Defizite auf, die das Netzwerk Datenschutzexpertise in einem Gutachten vom 13.03.2025 ausführlich dokumentiert hat:

https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2025_03_sekundaerntzg_gesdat.pdf

Diese Defizite betreffen nicht die **Bereitstellung von Gesundheitsdaten**. Über Jahre hinweg wurde zu Recht vor allem von der medizinischen Forschung reklamiert, dass die Rechtsgrundlagen für ihre Tätigkeit unzureichend sind. Der MG-E zielt ebenso wie der EHDS und das GDNG darauf ab, bessere gesetzliche Grundlagen für die Sekundärnutzung, etwa für Forschungszwecke, zu schaffen. Dass dieser Zweck mit dem Entwurf erreicht werden kann, mag der frühzeitigen und umfassenden Einbindung der „Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V." (TMF) in die Erarbeitung des MRG-E zuzuschreiben sein (S. 20 f.).

In den vergangenen Jahren wurde nicht nur von Datenschützern, sondern auch von Forschenden kritisiert, dass trotz der Beschränkungen des Datenzugangs für die Forschung der **Schutz der sensitiven Gesundheitsdaten** mangelhaft ist.[1] Das Fehlen von Datenschutzvorkehrungen kann das Vertrauen von Patienten in den Umgang mit ihren Daten und damit deren Kooperationsbereitschaft im Gesundheitsbereich beeinträchtigen. Die im Entwurf enthaltenen Regelungen zum Datenschutz der betroffenen Menschen sind mangelhaft; sie verstärken bestehende Defizite. Der Entwurf missachtet zentrale grundrechtliche Vorgaben sowie deren Konkretisierung in der europäischen Datenschutz-Grundverordnung (DSGVO, dazu im Detail unten unter III.).

Der MRG-E ist ein Baustein, mit dem der schon durch den EHDS und das GDNG vorgegebene **Paradigmenwechsel** weg zum Patientengeheimnis und hin zur extensiven Nutzung von Gesundheitsdaten vollzogen werden soll. Dieser Prozess ist mit hohen persönlichkeitsrechtlichen Risiken verbunden. Um diese zu erkennen und bei Eintritt von Fehlern und Schäden zu korrigieren, ist eine Evaluation der Sekundärnutzung geboten. Eine solche Evaluation ist jedoch im MRG-E nicht vorgesehen (S. 41). Ohne eine Befristung und eine Evaluierung werden die bestehenden Defizite des geplanten Gesetzes u.U. langfristig festgeschrieben.

Irritierend ist zudem, dass der Entwurf überhaupt nicht im Blick hat, dass es sich bei den geregelten Medizinregistern weitgehend um Datenvermittlungsdienste i.S.v. Art. 2 Nr. 11 **Data Governance Act** (DGA) handelt und dass deren Betreiber altruistische Organisationen i.S.v. Art. 17 DGA sind. Der DGA ist am 23.09.2023 in Kraft getreten. Datenaltruismus ist die freiwillige gemeinsam Nutzung von Daten auf der Grundlage der Einwilligung der Betroffenen oder der Erlaubnis der Dateninhaber gegen ein allenfalls kostendeckendes Entgelt für Ziele im allgemeinen Interesse wie u.a. die Gesundheitsversorgung (Art. 2 Nr. 16 DGA). Der DGA macht verbindliche Vorgaben für Datenvermittlungsdienste (Art. 10-12 DGA) sowie zum Datenaltruismus (Art. 16 ff. DGA), insbesondere zur Eintragung und Registrierung (Art. 17-19 DGA), zur Transparenz (Art. 20 DGA) und zum Schutz von Betroffenen und Dateninhabern (Art. 21 DGA). Diese Vorgaben gehen teilweise über die Regelungen des MRG-E hinaus und stehen teilweise hierzu im Widerspruch. Daraus ergeben sich nicht nur Verstöße und Regelungsdefizite zur DSGVO, sondern auch zum DGA und damit zu weiteren europarechtlichen Vorgaben.

Die vorliegende Stellungnahme bezieht sich insbesondere auf die kritik- und damit verbesserungsbedürftigen Regelungsvorschläge. Werden in der vorliegenden Stellungsnahme Angaben zu Paragraphen oder Seiten gemacht, so beziehen diese sich auf den erörterten Referentenentwurf.

[1] Statt vieler Krawczak/Weichert, Vorschlag einer modernen Dateninfrastruktur für die medizinische Forschung in Deutschland, September 2017, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_twmk_vorschlag_dinfmedforsch_v1.9_170927.pdf.

III. Zu einzelnen Regelungen

Zu § 2 Begriffsbestimmungen

Die Definition von „**Medizinregister**“ ist zu weit, da jede Form der Sammlung von strukturierten Gesundheitsdaten erfasst wird. Als notwendiges zusätzliche Merkmal ist aufzunehmen, dass die Daten von verschiedenen meldenden Gesundheitseinrichtungen stammen.

Zu den §§ 3 u. 4 Zentrum für Medizinregister (ZMR)

Das im Rahmen des BfArM einzurichtende ZMR ist nur **eines von mehreren** dort einzurichtenden bzw. eingerichteten Organisationseinheiten, die mit der Sekundärnutzung von Gesundheitsdaten befasst sind bzw. sein sollen. Weitere sind die Datenzugangs- und Koordinierungsstelle nach § 3 GDNG, das Forschungsdatenzentrum Gesundheit (FDZ) gemäß §§ 303d f. SGB V sowie die zentrale Plattform für genetische Modellprojekte gemäß § 64e Abs. 9-9b SGB V.

Das BfArM ist eine nachgeordnete Behörde des Bundesgesundheitsministeriums (BMG) und als solche **weisungsabhängig**. Ein zentraler Zweck der sekundären Datenverarbeitung ist die Förderung der unabhängigen Medizinforschung. Eine Aufgabe bei der Sekundärnutzung von Gesundheitsdaten besteht darin, einen diskriminierungsfreien Datenzugang und einen Schutz der Daten zu gewährleisten.[2] Dies ist nicht gewährleistet, solange keine wirksame Datenschutzaufsicht über die Sekundärdatenverarbeitung in Medizinregistern erfolgt. Die bisherigen Normen wie auch die geplante Regelung gewährleisten nicht die gebotene Unabhängigkeit der zuständigen Organisationseinheiten bei der Aufgabenwahrnehmung.[3]

Es ist geplant, das BfArM zur **nationalen Zugangsstelle für Gesundheitsdaten** (Art. 57-59 EHDS) zu machen. Es ist aber nicht erkennbar, wie die gesetzlich etablierten Funktionseinheiten des BfArM zueinander heute im Verhältnis stehen bzw. künftig stehen sollen, insbesondere soweit es Überschneidungen und gegenseitige Abhängigkeiten gibt (z.B. bei der Verknüpfung von FDZ- oder Krebsregisterdaten mit sonstigen Registerdaten). Der Verweis auf Ergänzungen in künftigen Gesetzgebungsverfahren (S. 44) ist insofern wenig hilfreich.

Die wichtigste Aufgabe des ZMR besteht darin, die Qualifizierung von Medizinregistern vorzunehmen (Abs. 1 Nr. 3). An diese Qualifizierung werden sehr weit gehende datenschutzrechtliche Eingriffsbefugnisse geknüpft. Wegen der hohen datenschutzrechtlichen Relevanz muss beim ZMR insofern Expertise vorhanden sein (vgl. § 6 Abs. 1 Nr. 1 lit. c u. d). Insofern verblüfft, dass das ZMR nicht verpflichtet wird, bei der Erfüllung seiner Aufgaben die zuständigen Datenschutzaufsichtsbehörden zu beteiligen, obwohl es genau deren europarechtlich vorgesehene Aufgabe ist, sich an derartigen relevanten Prozessen einzubringen (Art. 57 f. DSGVO). Der **Verzicht auf die Einbindung der Datenschutzaufsicht** ist nicht unbürokratisch, sondern provoziert Doppelprüfungen, die mit dem Gesetz gerade vermieden werden sollen (S. 50).

[2] Vgl. Art. 8 Abs. 3 GRCh, EuGH 03.09.2010 – C-518/07, Rn. 24 24 f.; Weichert in Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG, 3. Aufl. 2024, Art. 52 m.w.N.
[3] Weichert, Sekundärnutzung von Gesundheitsdaten, 13.03.2025, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2025_03_sekundaerntzg_gesdat.pdf, Kap. 10.2 (S. 43 ff.).

Zu § 5 Medizinregisterverzeichnis

Das vom ZMR zu führende Verzeichnis dient ausschließlich der Information von Datennutzenden (S. 46) und bringt **keinen Transparenzgewinn für die Betroffenen**. Das Verzeichnis könnte dazu genutzt werden, die insofern bestehenden bisherigen Defizite zu beheben, indem in das Verzeichnis auch die Angaben zu geplanten, in jedem Fall aber zu den erlaubten Zweckänderungen, Zusammenführungen und Übermittlungen aufgenommen werden (s.u. zu § 13).

Zu §§ 6, 7 Qualifizierung von Medizinregistern

Es ist grundsätzlich zu begrüßen, dass über die Qualifizierung versucht wird, bei dem bisher bestehenden Wildwuchs von Medizinregistern[4] Strukturen zu schaffen und **Qualitätsanforderungen** zu verwirklichen. Zu begrüßen ist auch, dass qualifizierte Register einen Datenmanagementplan, ein Datenschutzkonzept und eine Datenschutzfolgenabschätzung mit technisch-organisatorischen Maßnahmen vorlegen müssen.

Unklar ist, wie das ZMR verfährt, wenn die vorzulegenden Antragsunterlagen nicht den gesetzlichen Anforderungen entsprechen. Das BfArM hat sich bisher nicht durch spezifische **Datenschutzkompetenz** profiliert. Es ist nicht gewährleistet, dass die Unterlagen von einer unabhängigen, fachlich qualifizierten Stelle begutachtet und bewertet werden.

Für „qualifizierte Medizinregister mit Widerspruchslösung“ soll (nur) ein Ethik-Votum der landesrechtlich zuständigen **Ethik-Kommission** vorgelegt werden müssen (S. 52). Die Regulierung und erst Recht die Praxis der Ethik-Kommission in den Ländern ist sehr unterschiedlich und teilweise intransparent. Ethik-Kommissionen haben regelmäßig medizinisch-fachliche Kompetenzen. Bei komplexen technischen und vor allem schwierigen datenschutzrechtlichen Fragen besteht dagegen zumeist nur eine geringere Fähigkeit zur Beurteilung.

Im Vordergrund steht bei der sekundären Datennutzung und bei Widersprüchen hiergegen das allgemeine Persönlichkeitsrecht und der Datenschutz. Da bei der Qualifizierung materiell-rechtliche Fragen von zentraler Bedeutung sind, ist eine Einbindung der unabhängigen, transparenten und regulierten Datenschutzaufsicht dringend geboten (s.o. zu §§ 3 u. 4). Die Begründung für die **Nichtbefassung der Datenschutzaufsicht** – die Vermeidung von Aufwand (S. 29) – signalisiert, dass die Berücksichtigung datenschutzrechtlicher Expertise unerwünscht ist. Angesicht der hohen datenschutzrechtlichen Relevanz der Qualifizierung genügt die (informelle) Einbindung des internen Datenschutzbeauftragten gemäß Art. 38 DSGVO (S. 50) nicht.

Eine **unqualifizierte Qualifizierung** von Medizinregistern läuft Gefahr, dass derzeit offensichtlich rechtswidrige Medizindatensammlungen ein amtliches Gütesiegel verpasst bekommen und die damit verbundenen – zumeist verdeckten – Geschäftsmodelle ausweiten können. So wurden z.B. das bundesweite Praxisregister Schmerz oder die Krankenhausfall-Datensammlung von Bindoc öffentlich wegen massiver Datenschutzverstöße kritisiert, ohne dass daraus von staatlichen Behörden Schlussfolgerungen gezogen wurden.[5]

[4] BQS/TMF, Gutachten zur Weiterentwicklung medizinischer Register, Oktober 2021, https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Gesundheit/Abschlussberichte/REG-GUT-2021_Registergutachten_BQS-TMF-Gutachtenteam_2021-10-29.pdf.
[5] Nähere Informationen hierzu unter https://www.netzwerk-datenschutzexpertise.de/dokument/datenschutz-im-gesundheitsbereich.

Welche **Begehrlichkeiten** an den in den Registern gespeicherten Daten bestehen, zeigt die zustimmende Stellungnahme des BITKOM zu dem vorliegenden MRG-E, in der aber vorgeschlagen wird, dass keine externe Prüfung der Qualifizierung erfolgen solle, sondern ein Selbst-Deklaration der „Qualitätsstandards" genügen solle und in der der weitgehend kontrollfreie Antrags- und Datennutzungsprozess nach § 17 noch als zu hinderlich und zeitintensiv kritisiert wird.[6]

Ohne dies explizit zu machen, muss die Qualifizierung von Medizinregistern als eine Umsetzung des Art. 72 EHDS verstanden werden, der für **vertrauenswürdige Gesundheitsdateninhaber** ein vereinfachtes Zugangsverfahren auf nationalgesetzlicher Ebene erlaubt. Die europäische Regelung verlangt jedoch, dass der Zugang über eine „sichere Verarbeitungsumgebung" erfolgt (Abs. 2 lit. a), die erlaubende Stelle für die Antragsbehandlung „über das erforderliche Fachwissen" verfügt (Abs. 2 lit. b), zusätzliche Garantien bestehen (Abs. 2 lit. c) und eine regelmäßige Prüfung der Qualifikation erfolgt (Abs. 2 S. 3). Diesen Vorgaben entsprechen die Anforderungen des MRG-E nicht.

Zu §§ 8 ff. Meldungen durch Gesundheitseinrichtungen

Die Regelungen sehen einen formalisierten Prozess vor, mit dem sich Gesundheitseinrichtungen zur Meldung gegenüber qualifizierten Medizinregistern verpflichten. Damit soll eine **gesetzliche Datenerhebungs- und Übermittlungsbefugnis** an das Register verbunden sein, soweit der Betroffene dem nicht nach entsprechender Information widersprochen hat.

Die Erhebungsbefugnis der Gesundheitseinrichtungen nach § 9 Abs. 1 S. 1, mit der eine Übermittlungsbefugnis nach § 10 und eine Übermittlungspflicht nach § 8 Abs. 1 S. 1 an die Register verknüpft sein sollen, animiert Gesundheitseinrichtungen, Daten über das für eine Behandlung erforderliche Maß zu erheben (und zu speichern), um diese Daten an ein Register weiterzuübermitteln. Dadurch wird das **Datenminimierungsgebot** des Art. 5 Abs. 1 lit. c DSGVO ausgehebelt (S. 52 f.).

Als Widerspruchsmöglichkeit ist für Betroffene nur ein **Generalwiderspruch** nach einer vorab erfolgenden Generalinformation (vor der Erstmeldung, vgl. § 9 Abs. 1) vorgesehen. So besteht für die Patienten das Risiko, dass ohne deren Willen sensitive Daten an ein Register übermittelt werden, wogegen sie bei der Möglichkeit einer Einzelfallentscheidung widersetzt hätten. Die Regelung zielt darauf ab, die Verfügungsmacht über Daten von Betroffenen vollständig auf den Arzt zu übertragen und diesen dazu zu veranlassen, möglichst umfassend Daten den Registern und letztlich Dritten für eine Vielzahl unüberschaubarer Zwecke zur Verfügung zu stellen. Eine Ausnahme hiervon ist nur hinsichtlich Ergebnissen aus genetischen Untersuchungen vorgesehen (§ 9 Abs. 6 i.V.m. § 11 GenDG).

Zu § 11 Datenkranz

Die scheinbar einschränkende Regelung („darf nur") ist angesichts des **umfassenden Katalogs** erlaubter Gesundheitsmerkmale ohne wirkliche Begrenzung. Die Regelung geht davon aus, dass qualifizierte Medizinregister im Regelfall mit vielen Identifizierungsdaten direkt personenbezogen geführt werden und das Ziel der Datenminimierung (z.B. bzgl. des Registerzwecks) aus dem Blick gerät. Diese Tendenz wird dadurch verstärkt, dass das BMG ermächtigt wird, verbindliche interoperable, strukturierte und standardisierte Datenformate per Rechtsverordnung vorzugeben (§ 11 Abs. 2 i.V.m. § 385 Abs. 1 S. 1, Abs. 2 S 1 Nr. 1 SGB V).

[6] BITKOM, Stellungnahme November 2025, https://www.bitkom.org/sites/main/files/2025-11/bitkom-stellungnahme-medizinregistergesetz-mrg.pdf, S. 4 u. 5.

In Registern gespeichert werden können sollen **soziodemographische Angaben** (Abs. 1 Nr. 1 lit. g) . Darunter fallen gemäß der Gesetzesbegründung z.B. Angaben zu einem Migrationshintergrund oder einer ethnischen Zugehörigkeit, der Familienstand oder die Haushaltsgröße (S. 56). Dadurch wird der Inhalt von Medizinregistern in unverhältnismäßiger Weise ausgeweitet. Eine Erforderlichkeit dürfte hierfür kaum begründbar sein.

Entsprechendes gilt für Angaben zu **Lebensumständen und Gewohnheiten** (Abs. 1 Nr. 2), die in ein Medizinregister aufgenommen werden können. Die Begründung nennt als Merkmale: „familiäre Situation, wie zum Beispiel eine mögliche Versorgung eines Patienten zu Hause und Angaben zur beruflichen Situation, worunter zum Beispiel eine bestehende Arbeitsfähigkeit oder Arbeitsunfähigkeit zu fassen ist“, „Ernährung und Ernährungsstil“, z.B. „zur veganen oder vegetarischen Ernährung oder auch religiös bedingte Speisevorschriften“ sowie „Konsum legaler und illegaler Drogen“, z.B. „Raucherstatus, der-Alkoholkonsum, eingenommene Medikamente, die Applikationsform oder Angaben zu Dauer und Dosis“ (S. 56 f.).

Die weiteren Kategorien des zulässigen Datenkranzes gegen bis ins Detail des individuellen Lebens, der Krankheiten und des Umfeldes und erfassen teilweise auch **Daten Dritter** (z.B. „Familienanamnese“, Abs. 1 Nr. 5).

Abs. 2 sieht vor, dass die Datenübermittlung strukturiert, standardisiert und interoperabel erfolgen soll. Die Begründung geht davon aus, dass dies **automatisiert** durch „Ausleitung der Daten aus den Praxisverwaltungs- und Krankenhausinformationssystemen erfolgen soll“. Eine solche Vorgehensweise würde dazu führen, dass eine persönliche Abwägung durch den Arzt mit möglicherweise entgegenstehenden Schutzinteresse des Betroffenen nicht mehr erfolgen würde.

Als europarechtliche Rechtsgrundlage für sämtliche im MRG-E zugelassenen Formen der Datenverarbeitung wird Art. 6 Abs. 1 lit. c u. e i.V.m. Art. 6 Abs. 3 lit. b DSGVO genannt (u.a. S. 59). Danach ist, im Umsetzung von Art. 52 Abs. 2 S. 2 GRCh, eine **Angemessenheitsprüfung** im Einzelfall erforderlich. Auch in den in Anspruch genommenen Alternativen des Art. 9 Abs. 2 DSGVO ist vorgesehen, dass im Interesse der Angemessenheit Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ vorgesehen werden müssen (so z.B. lit. j). Da solche wirksamen Garantien im MRG-E nicht vorgesehen sind, verstoßen die Regeln gegen Europarecht.

Zu § 12 Abs. 1 u. 2 Zwecke der qualifizierten Medizinregister

Die Regelung repliziert den umfassenden Zweckekanon, der in den Art. 53 Abs. 1 EHDS, § 4 Abs. 2 GDNG, § 303e Abs. 2 SGB V vorgegeben ist. Erfasst wird aber nicht nur, wie in den anderen Regelungen vorgesehen ist, die Verarbeitung pseudonymisierter Daten, sondern auch die **Verarbeitung von identifizierten Gesundheitsdaten**.

Die in Abs. 1 aufgeführten **Zwecke** umfassen den gesamten Gesundheitsbereich mit der Tendenz, darüber hinauszugehen: Qualitätssicherung (Nr. 1), Unterstützung politischer Entscheidungsprozesse (Nr. 2), Aufgabenwahrnehmung im Bereich der öffentlichen Gesundheit (Nr. 3), Gesundheitsberichterstattung (Nr. 4), Entwicklung und Überwachung von Produkten und Methoden einschließlich dem Einsatz von Künstlicher Intelligenz (Nr. 5), Nutzenbewertungen (Nr. 6), Forschung (Nr. 7). So heißt es z.B. in der Begründung (S. 61): „Auch für das Testen und Trainieren von Systemen der künstlichen Intelligenz sind die hochstrukturierten und kuratierten Daten aus Medizinregistern eine wertvolle Datenquelle, um die Validität der KI-Anwendung zu gewährleisten, z.B. für KI-gestützte Therapieempfehlungen. Die Regelung ermöglicht den umfassenden Einsatz von Medizinregistern für diese Zwecke.“

Mit diesem Zwecke-Katalog erfolgt eine massive **Ausweitung der Registerzwecke**, die sich bisher zumeist darauf beschränkten, die individuelle Behandlung zu unterstützen oder eine Qualitätssicherung dieser Behandlung (gemäß SGB V) zu gewährleisten.

Von den aufgeführten Zwecken ist nur die wissenschaftliche Forschung grundrechtliche **privilegiert** (Art. 5 Abs. 3 GG, Art. 13 S. 1GRCh) und steht insofern gleichrangig neben dem Grundrechtsschutz der Betroffenen. Die Gesundheitsberichterstattung, der ein aufwändiges Aggregierungsverfahren zugrunde liegen muss[7], ist von der DSGVO privilegiert (Art. 5 Abs. 1 lit. b DSGVO: Statistik).

Alle weiteren Zwecke haben einen direkten operativen Bezug zu Politik, Wirtschaftlichkeit, Planung und Organisation. Diese operativen Zwecke – jenseits von Forschung und Qualitätssicherung – werden in der Begründung überhaupt nicht angesprochen (S. 20). Die personenbeziehbare Nutzung für diese Zwecke stellt eine große Gefahr für das Persönlichkeitsrecht der Betroffenen dar, selbst wenn diese pseudonymisiert erfolgen sollte. Erlaubt wird in Abs. 2 aber sogar die personenbezogene Datenverarbeitung. Einzige „Grenze“ ist die Erforderlichkeit, ohne dass irgendwelche Vorkehrungen oder Garantien vorgesehen sind. Eine derartig weitgehende Verarbeitungsbefugnis ist **unverhältnismäßig** und daher unzweifelhaft verfassungswidrig.[8]

Ein generelles Problem bei der Weitergabe von Gesundheitsdaten besteht darin, dass bei den Datenempfängern die Daten regelmäßig nicht mehr der Schweigepflicht nach § 203 StGB unterliegen. Ob § 203 StGB auf Medizinregister anwendbar ist, ist bisher nicht geklärt. Es besteht ein rechtliches Graufeld, auch wenn die Datenempfänger einer ärztlichen Leitung unterliegen, da fraglich ist, ob auf Grund gesetzlicher Übermittlungen eine Offenbarung nach § 203 StGB erfolgt. Daher ist es folgerichtig, dass in den §§ 18 f. eigenständige Geheimhaltungsvorschriften bestehen, die sich aber systematisch wie auch begrifflich („Datennutzende“) nicht auf die Register beziehen. Unstreitig dürfte sein, dass die in den Registern gespeicherten Daten nicht dem **Beschlagnahme- und Zeugnisverweigerungsschutz** gemäß den §§ 53 Nr. 3, 53a, 97 Abs. 2 StPO unterliegen. Dies ist bei Registern besonders problematisch, da die Daten hier zumeist zentral mit identifizierenden Daten für Strafverfolgungszwecke genutzt werden können.[9] Ein Rückgriff auf eine Verhältnismäßigkeitsprüfung[10] zum Schutz vor Einbezug in Strafverfahren ist unzureichend und nicht rechtssicher.

Zu § 12 Abs. 3 u. 4 Rückmeldung an Gesundheitseinrichtung

Die Rückmeldung an den Arzt oder die Gesundheitseinrichtung „zum Zweck der Behandlung der betroffenen Person, zur Verbesserung der Versorgungsqualität, der Patientensicherheit oder zur Qualitätssicherung“ ist auch in Art. 58 Abs. 3 EHDS vorgesehen. Zur Wahrung der Patientenvertraulichkeit ist es aber unabdingbar, dass die aus dem Register stammenden **Daten anderer Patienten** so anonymisiert bzw. aggregiert sind, dass deren Identifizierung ausgeschlossen ist. Hierfür macht die Regelung keine Vorgaben. Eine dies nahelegende Formulierung in der Begründung (S. 61) ist nicht ausreichend.

Zu §§ 13, 14 Abs. 2, 16 S. S. 3 Informationspflichten qualifizierter Medizinregister

In den Art. 13 und 14 DSGVO ist vorgesehen, dass Betroffene hinsichtlich jeder neuen sie betreffenden Datenverarbeitung informiert werden u.a. über Verantwortliche, Zwecke, Rechtsgrundlagen, Empfänger, Speicherdauer und Betroffenenrechte. § 13 reduziert diese

[7] BVerfG 15.12.1983 – 1 BvR 209/83 u.a., NJW 1984, 419 ff, Rn. 104 ff. (423 f.).
[8] Weichert, Sekundärnutzung von Gesundheitsdaten (Fn. 3), Kap. 7.5 (S. 37 f.).
[9] Vgl. Weichert, Sekundärnutzung von Gesundheitsdaten (Fn. 3), Kap, 8.1 (S. 39 f.).
[10] Vgl. BVerfG 25.09.2023 – 1 BvR 2219/20 Rn. 13-15, NVwZ 2024, 416.

Informationspflicht auf die einmalige Information „über die Zwecke“. Notwendig wäre aber eine Information, die **über die Zwecke hinaus** in jedem Fall die Art und den Umfang der Daten, die konkreten Empfänger und die Rechtsgrundlage benennt.

Zwar erlaubt Art. 14 Abs. 5 lit. c DSGVO die Regulierung der Informationspflicht in einer Rechtsvorschrift des Mitgliedsstaats. Doch müssen diese Regeln „geeignete **Maßnahmen zum Schutz der berechtigten Interessen** der betroffenen Person“ ausdrücklich vorsehen. Derartige kompensatorische Maßnahmen enthält der MRG-E nicht. Der Verweis auf das Auskunftsrecht nach Art. 15 DSGVO genügt nicht (S. 63). Der Hinweis läuft zudem leer, da die Betroffenen nicht erfahren, wer Empfänger ihrer Daten sind. Die Betroffenen haben keine reale Möglichkeit, über die bisherigen Rechtsgrundlagen (zumeist Einwilligung) hinausgehende Zweckänderungen und Übermittlungen zu Kenntnis zu nehmen, zu hinterfragen und, bei Bedarf, rechtlich anzugreifen. Daher sind die vorgesehenen Transparenzregelungen des MRG-E europarechtswidrig.

Transparenz könnte in der Form hergestellt werden, dass dem ZMR alle Übermittlungen, Zusammenführungen oder Zweckänderungen angezeigt werden und das ZMR diese in einem allgemein z.B. über das **Internet-Verzeichnis** bekannt macht (s.o. zu § 5).

Zu § 14 Abs. 1 Datenzusammenführung in Qualifizierten Registern

Die Regelung erlaubt die Zusammenführung von Meldungen der Gesundheitseinrichtungen mit den „Bestandsdaten des Medizinregisters“. Zweck ist die Zusammenführung der zu einer Person gemeldeten Daten. Dies ist grds. sinnvoll. Es bestehen jedoch Unsicherheiten, wie weit der Begriff „Bestandsdaten“, der gesetzlich nicht definiert ist, verstanden wird und wie der Zweck der Zusammenführung bei Abweichungen zwischen gemeldeten und Bestandsdaten erreicht wird, ohne das Datenminimierungsgebot zu verletzen. Rückfragen und Klärungen können zur Übermittlung sensitiver Daten von anderen Betroffenen führen (vgl. das Verfahren der **Zuordnungssicherung** in § 8a AZRG).

Zu §15 Verarbeitung bei einwilligungsbasierten Medizinregistern

Die Regelung erlaubt bei einwilligungsbasierten Medizinregistern, die qualifiziert wurden, ohne Berufung auf die gesetzlichen Übermittlungsregelungen der §§ 9, 10 die Anwendung der Verarbeitungsbefugnisse in den §§ 16-21. Dies hat zur Folge, dass Datenübermittlungen erlaubt werden, die über die Erlaubnis in der Einwilligungserklärung der Betroffenen hinausgehen. Dies führt zwangsläufig dazu, dass die Betroffenen eine **falsche Vorstellung** von der durch ihre Erklärung erlaubten Datenverarbeitung haben und der datenschutzrechtlich geforderten Transparenz nicht genügt wird.

Zu § 16 Registerkooperationen

Die Regelung erlaubt die Zusammenführung der Daten qualifizierter Register auf der Grundlage einer **Kooperationsvereinbarung**, die dem ZMR angezeigt werden muss. Erlaubte Zwecke hierfür sind sämtliche in § 12 Abs. 1 genannten. Einzige Schutzvorkehrung ist die Pflicht zur Pseudonymisierung bzw. zur Anonymisierung, „sobald dies … möglich ist“.

Die Regelung zielt auf eine Zusammenführung der bisherigen Register für vielfältige Zwecke vor, ohne dass datenschutzrechtliche Vorkehrungen bestehen. Die Regelung, dass die Kooperationsvereinbarung den Zweck und technisch-organisatorische Maßnahmen benennen muss, ist keine solche wirksame Vorkehrung, da **keine Prüfung und Genehmigung der Vereinbarung** durch eine unabhängige fachkundige Stelle gewährleistet ist. Selbst die minimalste Maßnahme, die Pflicht zur Veröffentlichung der Kooperationsvereinbarung, ist nicht vorgesehen. Vielmehr wird in S. 3 pauschal auf den unzureichenden § 13 verwiesen.

Zu § 17 Übermittlung von Registerdaten an Datennutzende

Die Regelung erlaubt die Übermittlung von Registerdaten zu sämtlichen in § 12 Abs. 1 genannten Zwecken auf Antrag und nach Genehmigung durch das qualifizierte Register in pseudonymisierter Form, wenn das Register den Eindruck hat, dass „schutzwürdige Interessen der betroffenen Person nicht beeinträchtigt werden oder das **öffentliche Interesse** an der Datenverarbeitung die schutzwürdigen Interessen der betroffenen Personen überwiegt". Zudem wird eine Bewertung des Reidentifizierungsrisikos durch das Register gefordert (Abs. 3). Die Regelung erweckt den unzutreffenden Eindruck („oder"), dass selbst bei fehlendem öffentlichen Interesse an der Übermittlung diese zulässig sein kann. Dies ist aber nicht der Fall (vgl. § § 1 Abs. 2 u. 3 GDNG).

Die Anträge sind dem ZMR zu melden, das diese veröffentlicht (Abs. 6). Nicht veröffentlicht wird, dass und unter welchen Bedingungen den Anträgen stattgegeben wurde. Der **Umfang der Veröffentlichung** wird nicht festgelegt (s.o. zu §§ 13 ff.). Damit kann die Öffentlichkeit nicht und können die Betroffenen nicht erkennen, inwieweit ihre Datenschutzbelange beeinträchtigt sein können.

Die vorgesehenen **Sicherungen und Garantien** bei der Datenübermittlung sind ungenügend: Es gibt keine Anforderung hinsichtlich der Vertrauenswürdigkeit und Fachkunde der antragstellenden potenziellen Datennutzenden. Es werden keine Vorgaben gemacht, welchen konkreten Anforderungen ein Antrag genügen muss und wie diese glaubhaft gemacht werden müssen. Die Register entscheiden über die Nutzungsanträge, ohne dass sie hierfür qualifiziert und unabhängig genug sind. Für die Betroffenen ist die Weiternutzung ihrer Daten nicht im Ansatz erkenn-, geschweige denn überprüfbar. Eine nachträgliche Überprüfung der erfolgten Datennutzung ist nicht vorgesehen. Die Regelung ist in der vorliegenden Form offensichtlich unverhältnismäßig.[11]

Zu § 18 f. Sanktionsbewehrte Geheimhaltungspflichten

Die Regelungen sehen sanktionsbewehrte Zweckbindungs- und Geheimhaltungspflichten für die Datennutzenden vor. Diese Nutzer genießen jedoch kein strafprozessuales Zeugnisverweigerungsrecht; deren Daten unterliegen keinem Beschlagnahmeverbot (s.o. zu § 12 Abs. 1, 2). Noch problematischer ist, dass die strafrechtliche Sanktionsmöglichkeit gemäß § 19 Abs. 3 von einem Strafantrag insbesondere der Betroffenen abhängig gemacht wird. Betroffene erhalten aber regelmäßig keine Kenntnis von Verstößen gegen § 18, so dass schon aus diesem Grund voraussichtlich die **Strafvorschrift leerlaufen** würde. Hinzu kommt, dass Verstöße gegen die Vertraulichkeit von Gesundheitsdaten von den Strafverfolgungsbehörden und den Gerichten in den Praxis als wenig relevant angesehen werden, was dazu führt, dass in der Praxis bisher solche Sanktionen kaum erfolgen, wenngleich ein großes Dunkelfeld besteht.[12]

Angesichts dessen zeugt der schwarz-rote Koalitionsvertrag (s.o. unter I.) von geringen Problembewusstsein, in dem ohne Realitätsbezug als einzige Schutzvorkehrung vor einem Missbrauch der Gesundheitsdaten auf die „**konsequente Ahndung von Verstößen**" verwiesen wird.

[11] Zu den rechtlichen Anforderungen ausführlich Weichert, Sekundärnutzung von Gesundheitsdaten (Fn. 3), Kap. 10 (S. 42 ff.).
[12] Vgl. Weichert, Sekundärnutzung von Gesundheitsdaten (Fn. 3), Kap. 14.1 (S. 64 f.)

Zu § 20 Technisch-organisatorische Maßnahmen

Die Regelung hat weitgehend keinen eigenen **Regelungsinhalt**, da sie auf ohnehin geltende Regelungen verweist (§ 22 Abs. 2 BDSG, Art. 5 Abs. 1 lit. c, 25, 32 DSGVO). Die Regelung zur Notwendigkeit eines Rechte- und Rollenkonzeptes und der Protokollierung in Abs. 3 ist als Konkretisierung zu begrüßen.

Die in Abs. 4 vorgesehene **Speicherdauer** von 100 Jahren, die dem § 303d Abs. 4 SGB V in Bezug auf das FDZ entspricht, wird mit Forschungsinteressen begründet (S. 68). Derartige Forschungsinteressen können aber nicht in Bezug auf sämtliche in § 11 genannten Daten für diese lange Zeit für angemessen angesehen werden. Angesichts der ungenügenden Schutzvorkehrungen hinsichtlich der zumeist mit Klarnamen arbeitenden Register wird mit der Speicherdauer ein lebenslanges unverhältnismäßiges Risiko für die Betroffenen begründet.[13]

Zu § 21 Nutzung der Krankenversichertennummer

Die Regelung erlaubt die Nutzung (des unveränderbaren Teils) der Krankenversichertennummer zur Erstellung von Pseudonymen, mit denen eine stellenübergreifende Datensatzzuordnung ermöglicht wird (S. 20). Dem kann von den Betroffenen widersprochen werden (Abs. 1 S. 2). Eine tatsächliche **Information über das Widerspruchsrecht** ist jedoch nicht gewährleistet, da diese gemäß Abs. 2 nicht individuell erfolgt, sondern lediglich „öffentlich und allgemein". Da sich die Widerspruchsmöglichkeit auf die Abwehr einer eher abstrakten Gefahr eines Datenmissbrauchs in äußerst komplexen Verarbeitungszusammenhängen bezieht, ist es für die Betroffenen kaum möglich, insofern eine rationale Entscheidung zu treffen (s.o. zu §§ 8 ff.).

Auf der Grundlage eines aus der Krankenversicherungsnummer gebildeten Pseudonyms soll die **Verknüpfung von Daten** von Medizinregistern mit Daten anderer Medizinregister und Daten weiterer Datenquellen erleichtert werden. Perspektivisch soll damit ein direktes Datenlinkage mit Hilfe einer anlassbezogenen Forschungskennziffer ermöglicht werden (S. 40). Zwar dürfen Medizinregister und meldende Gesundheitseinrichtungen den unveränderbaren Teil der Krankenversichertennummer nach § 290 SGB V nur zur Erzeugung eines Pseudonyms für die Verknüpfung mit anderen Datenquellen erheben und verarbeiten. Mit der generellen Verfügbarkeit der Krankenversichertennummer in einer Vielzahl von Registern sowie im Rahmen des primären Zwecks der gesetzlichen Krankenversicherung wird das Risiko der Reidentifizierung bei derart pseudonymisierten Datensätzen massiv erhöht. Die Nummer droht so, zu einem „Kennzeichen von allgemeiner Bedeutung" für den Gesundheitsbereich zu werden.[14] Gemäß Art. 87 S. 2 DSGVO muss in solchen Fällen durch geeignete „**Garantien** für die Rechte und Freiheiten der betroffenen Person" der Persönlichkeitsschutz gewahrt werden. Der Entwurf sieht keine Vorkehrungen vor, um dieses Risiko zu bewerten und einzugrenzen.

[13] Vgl. Weichert, Sekundärnutzung von Gesundheitsdaten (Fn. 3), Kap. 5.8 (S. 29).
[14] Weichert in Kühling/Buchner, DS-GVO BDSG, 4. Aufl. 2024, Art. 87 Rn. 11.

IV. Ergebnis

So sehr es zu begrüßen ist, dass sich der deutsche Gesetzgeber anschickt, die Datenverarbeitung in Medizinregistern generell gesetzlich zu regeln, so wenig ist es hierbei gelungen, einen – auch nur in Ansätzen – wirksamen Datenschutz vorzugesehen:

- Das für die Administration des Gesetzes vorgesehene Zentrum für Medizinregister (ZMR) ist nicht unabhängig genug und steht in einem ungeklärten Verhältnis zu anderen im BfArM angesiedelten Organisationseinheiten.
- Die Information der Betroffenen erfolgt nicht konkret im Einzelfall, sondern nur allgemein, so dass den Transparenzerfordernissen der DSGVO nicht genügt wird.
- Die erlaubten Zwecke der Datennutzung gehen weit über die Forschungsnutzung hinaus und erstrecken sich (selbst mit identifizierenden Daten) auf operative Zwecke mit einem hohen Missbrauchsrisiko, ohne dass hinreichende Sicherungsvorkehrungen vorgesehen sind.
- Der Datenaustausch zwischen Registern wird umfassend erlaubt, ohne dass Schutzvorkehrungen vorgesehen sind.
- Die Nutzungsgestattung für Datennutzende erfolgt durch die Register selbst und ist intransparent und kontrollfrei.
- Das Patientengeheimnis wird durch die Weiternutzung aufgehoben, was u.a. dazu führt, dass für die Daten kein Schutz vor der Nutzung durch Strafverfolgungsbehörden besteht.
- Die Sanktionsregelungen ist so restriktiv, dass eine wirksame Ermittlung, Verfolgung und Ahndung von Datenschutzverstößen unwahrscheinlich ist.
- Es ist unerfindlich, weshalb angesichts der geregelten hochsensiblen Datenverarbeitung keine Einbindung der hierfür vorgesehenen Datenschutzaufsichtsbehörden vorgesehen ist.
- Es fehlt an Schutzvorkehrungen bei der Nutzung der Krankenversicherungsnummer.
- Es fehlt an einer Regelung zur Evaluierung und Befristung des Gesetzes.
- Die Vorgaben des Data Governance Acts werden vollständig ignoriert.

Eine Auseinandersetzung mit dem Datenschutz findet in dem Entwurf nicht statt. Vielmehr heißt es lapidar und ohne weitere Begründung: „Dieser Gesetzesentwurf ist mit dem Recht der Europäischen Union und mit den völkerrechtlichen Verträgen, die die Bundesrepublik Deutschland geschlossen hat, vereinbar“ (S. 22). Tatsächlich verstößt der Entwurf in vieler Hinsicht gegen die Datenschutz-Grundverordnung sowie grundsätzlicher gegen das europarechtlich und verfassungsrechtlich garantierte Grundrecht auf Datenschutz.

Der Entwurf muss daher grundlegend überarbeitet werden. Der Autor der vorliegenden Stellungnahme steht hierbei gerne unterstützend zur Verfügung.

Mit freundlichen Grüßen
Dr. Thilo Weichert