

DR. THILO WEICHERT, WAISENHOFSTR. 41, 24103 KIEL

An die Fraktionen des Deutschen Bundestags
und die Mitglieder des Gesundheitsausschusses
des Deutschen Bundestags

Platz der Republik 1

11011 Berlin

Kiel, den 11.05.2026

**Entwurf der Bundesregierung eines
Gesetzes zur Stärkung von Medizinregistern und zur Verbesserung der
Medizinregisterdatennutzung – BR-Drs. 176/26 v. 27.03.2026
(Medizinregistergesetz)**

Sehr geehrte Damen und Herren Abgeordnete,

das Bundeskabinett hat mit Datum vom 11.03.2026 dem im Betreff genannten Gesetzesentwurf zugestimmt.¹

Zu einem Referentenentwurf des Bundesgesundheitsministerium (BMG) vom 27.10.2025² hatte das Netzwerk Datenschutzexpertise mit Datum vom 04.12.2025 kritisch Stellung genommen.³ Datenschutzorganisationen, die regelmäßig zu datenschutzrelevanten Gesetzgebungsvorhaben Stellung beziehen, waren bei der Verbändeanhörung des BMG nicht zur Stellungnahme aufgefordert. Während das BMG die angeforderten, den Entwurf weitgehend positiv bewertenden Stellungnahmen von medizinischen Verbänden auf seiner Webseite veröffentlichte,⁴ weigerte sich das BMG, offiziell die Stellungnahme des Netzwerks Datenschutzexpertise zur Kenntnis zu nehmen und diese zu veröffentlichen.

Dessen ungeachtet ist die vom Netzwerk Datenschutzexpertise vorgetragene Kritik, dass die Rolle der Datenschutzaufsicht nicht abgebildet wurde, im Kabinettsentwurf teilweise berücksichtigt. Weitere Kritiken blieben aber leider ohne Berücksichtigung, so dass auch dem Kabinettsentwurf bescheinigt werden muss, dass er gegen Europarecht sowie nationales Verfassungsrecht verstößt.

¹ Abrufbar im Internet unter https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/M/Medizinregistergesetz_Kabinett.pdf.

² Abrufbar im Internet unter https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/M/Medizinregistergesetz_RefE.pdf

³ Abrufbar im Internet unter https://www.netzwerk-datenschutzexpertise.de/sites/default/files/ste_2025_medregg-refe.pdf.

⁴ Links werden aufgeführt unter <https://www.bundesgesundheitsministerium.de/service/gesetze-und-verordnungen/detail/medizinregistergesetz>.

Im Interesse der Behebung dieser Verstöße sowie im Interesse einer praktikablen Umsetzung der begrüßenswerten Intention, Medizinregisterdaten insbesondere für Forschungszwecke zur Verfügung zu stellen, nehmen wir erneut Stellung. Wir wären dem Bundestag dankbar, wenn unsere Erwägungen im weiteren Gesetzgebungsprozess Eingang finden würden:

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. Weitere Referentenentwürfe liegen vor, so zu einem Forschungsdatengesetz (FDG-E) des Bundesministeriums für Forschung, Technologie und Raumfahrt (Stand 22.12.2025) sowie ein im April 2026 geleakter Entwurf eines „Gesetzes für Daten und digitale Innovation im Gesundheitswesen“ (GeDigG-E).

Der Entwurf für ein Medizinregistergesetz (MRG-E) 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“.⁵

Die Koalitionsvereinbarung 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. 64). Diese anderen Zwecke müssen mit dem ursprünglichen Zweck „vereinbar“ sein, wobei insbesondere das Verhältnis „zwischen den betroffenen Personen

⁵ Koalitionsvertrag zwischen CDU, CSU und SPD, 21. Legislaturperiode, Verantwortung für Deutschland“, S. 111.

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 weiteren Regelungen Eingang gefunden hat. Die Geltung des Patientengeheimnisses wird in Art. 9 Abs. 3 DSGVO ausdrücklich anerkannt.

Die durch die DSGVO gemachten Vorgaben, deren zentrale Funktion darin besteht, dem **Grundrecht auf Datenschutz** (Art. 8 Europäische Grundrechte-Charta – GRCh) bzw. dem Recht auf informationell Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz – GG) zu genügen, 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 direkt personenbezogener oder 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 zunächst zu Recht vor allem von der medizinischen Forschung reklamiert, dass die Rechtsgrundlagen für ihre Tätigkeit unzureichend sind. Der MRG-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 (vgl. S. 24, 28 f.).

In vergangenen Jahren wurde von Datenschützern und von Forschenden kritisiert, dass trotz der Beschränkungen des Datenzugangs für die Forschung der **Schutz der sensitiven Gesundheitsdaten** mangelhaft ist.⁶ 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. 42). Ohne eine Befristung und eine Evaluierung werden die bestehenden Defizite des geplanten Gesetzes u.U. langfristig festgeschrieben.

Die **Gesetzgebungskompetenz** für den Erlass eines MRG des Bundes wird mit einer Vielzahl von Vorschriften des Grundgesetzes (Art. 73 Nr. 11, 74 Nr. 1, 12, 13, 19, 26:GG: Statistik, Strafrecht, bürgerliches Recht, Sozialversicherung, Förderung wissenschaftliche Forschung, gemeingefährliche oder übertragbare Krankheiten, Untersuchung von Erbinformationen, Transplantation) begründet (S. 21 f. des Entwurfs), was jedoch nicht den gesamten Regelungsbereich des MRG-E abdeckt. Es ist im Interesse der Transparenz und Einheitlichkeit der Regulierung des Gesundheitswesens dringend geboten, eine konkurrierende Gesetzgebungskompetenz des Bundes für das Gesundheitswesen vorzusehen, um Normkonflikte mit dem Recht der Bundesländer zu vermeiden. Der vorliegende Entwurf sollte Anlass sein, diese GG-Änderung vorzunehmen.

Es ist nicht erkennbar, dass der MRG-E mit dem geplanten **Forschungsdatengesetz** (FDG) des Bundesministeriums für Forschung, Technologie und Raumfahrt (BMFTR, Stand 22.12.2025) abgestimmt ist, der auch die Nutzung von Medizinregistern regeln soll (siehe dort die Anlage 1 mit Verweis auf u. a. auf das Versichertenverzeichnis der Kranken- und der Pflegekassen oder die klinischen Krebsregister der Länder, Anlage 2 mit Verweis u. a. auf das Leibniz-Institut für Psychologie oder das Robert-Koch-Institut). Diese Diskrepanz führt zwangsläufig zu Rechtsunsicherheit.

Irritierend ist, 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 und für den nationalen Gesetzgeber verbindlich. Datenaltruismus ist die freiwillige gemeinsame 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

⁶ 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.

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 Stellungnahme Angaben zu Paragraphen oder Seiten ohne weitere Kennzeichnung gemacht, so beziehen diese sich auf den Kabinettsentwurf.

III. Zu einzelnen Regelungen

Zu § 1 Anwendungsbereich

Der Verweis, dass der **Schwerpunkt der geregelten Register** in den unter Abs. 1 Nr. 1-4 aufgeführten Bereiche liegen muss, ist ausschließlich mit der insofern zu begründenden Gesetzgebungszuständigkeit des Bundes zu begründen (s. o. II). Tatsächlich liegt ein Schwerpunkt der relevanten Medizinregister im Bereich von Krankenhäusern, für die die Gesetzgebungszuständigkeit bei den Bundesländern liegt. Dadurch entsteht eine große Rechtsunsicherheit bei der Anwendung.

Der **Begriff der wissenschaftlichen Forschung** (Abs. 1 Nr. 3) ist bisher nicht nationalgesetzlich definiert. Zur Vermeidung einer extensiven Auslegung des Begriffs ist eine Definition geboten, so wie sie in dem Entwurf eines FDG des Bundesforschungsministeriums (BMFTR, dort § 2 Nr. 2) vorgesehen ist.

Zu § 3 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.⁷ 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.⁸

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). Die unverbindliche Zusammenarbeitsregelung in § 4 Abs. 3 ist insofern wenig hilfreich.

⁷ 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.

⁸ Weichert, Sekundärnutzung von Gesundheitsdaten, 13.03.2025, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2025_03_sekundaermtzg_gesdat.pdf, Kap. 10.2 (S. 43 ff.).

Zu § 4 Aufgaben des ZMR

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, Abs. 2). Es ist fraglich, ob insofern die Beteiligung der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) neben vielen weiteren Institutionen (Abs. 2) und die geplante Ausstattung des ZMR mit 4 Mitarbeitenden (S. 23) genügt.

Zu § 5 Medizinregisterverzeichnis

Das vom ZMR zu führende Verzeichnis dient ausschließlich der Information von Datennutzenden (S. 47) und bringt **keinen Transparenzgewinn für die Betroffenen**. Das Verzeichnis könnte dazu genutzt werden, die bisher geplanten Transparenzdefizite zu beheben, indem in das Verzeichnis auch die Angaben zu geplanten, in jedem Fall zu den erlaubten Zweckänderungen, Zusammenführungen und Übermittlungen aufgenommen werden (s. u. zu § 13).

Ungeregelt bleibt nach dem Entwurf die Anforderungen des **Data Governance Acts** (DGA). Nach Art. 17 DGA muss durch die zuständige Behörde ein öffentliches Register der anerkannten altruistischen Organisationen geführt werden, das in Art. 18 DGA aufgeführte Anforderungen erfüllen muss (s. u. zu § 6).

Zu § 6 Qualifizierung von Medizinregistern

Es ist grundsätzlich zu begrüßen, dass über die Qualifizierung versucht wird, bei dem bisher bestehenden Wildwuchs von Medizinregistern⁹ 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 die Qualifizierung der Medizinregister soll ein Ethik-Votum der landesrechtlich zuständigen **Ethik-Kommission** vorgelegt werden müssen (Abs. 1 S. 2 Nr. 2). Die Regulierung und erst Recht die Praxis der Ethik-Kommission in den Ländern ist sehr unterschiedlich und teilweise intransparent. Ethik-Kommissionen haben vorrangig medizinisch-fachliche Kompetenzen. Bei komplexen technischen und vor allem schwierigen datenschutzrechtlichen Fragen, die sich bei der Anwendung des MRG ergeben, besteht dagegen zumeist nur eine geringere Fähigkeit zur Beurteilung.

Im Vordergrund steht bei der sekundären Datennutzung und bei Widersprüchen der Betroffenen das allgemeine Persönlichkeitsrecht und der Datenschutz. Dies wird nun – anders als noch im Referentenentwurf – in Abs. 2 ausdrücklich bestätigt. Die Bewertung soll durch das in das BfArM integrierte ZMR erfolgen. Da bei der Qualifizierung materiell-

⁹ 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.

rechtliche Fragen von zentraler Bedeutung sind, ist eine Einbindung der unabhängigen, transparenten und regulierten Datenschutzaufsicht 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. Angesichts der hohen datenschutzrechtlichen Relevanz der Qualifizierung genügt die (informelle) Einbindung des internen Datenschutzbeauftragten gemäß Art. 38 DSGVO (S. 56) nicht.

Art. 19 Abs. 2 DGA nennt Voraussetzungen an **datenaltruistische Organisationen**, die in § 8 entweder anders benannt werden oder überhaupt nicht aufgeführt sind. Letztgenanntes gilt insbesondere für die Einnahmequellen des Registers (lit. d). Gemäß Art. 18 lit. a und c DGA wird eine rechtliche Unabhängigkeit und eine funktionelle und strukturelle Trennung von sonstigen Tätigkeiten der verantwortlichen Stelle gefordert.

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 schon vor langer Zeit öffentlich wegen massiver Datenschutzverstöße kritisiert, ohne dass daraus von staatlichen Behörden Schlussfolgerungen gezogen wurden.¹⁰

Welche **Begehrlichkeiten** an den in den Registern gespeicherten Daten bestehen, zeigt die zustimmende Stellungnahme des BITKOM zum Referentenentwurf eines MRG, in der vorgeschlagen wird, dass keine externe Prüfung der Qualifizierung erfolgen, 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.¹¹

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, 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 § 7 Qualifizierung zum Medizinregister mit Widerspruchslösung

Das Verhältnis zwischen § 6 und § 7 ist unklar. Erst aus der Begründung (S. 54) geht indirekt hervor, dass es Medizinregister ohne und mit Widerspruchslösung geben soll. Die Entscheidung hierüber soll letztlich beim Register selbst liegen, wobei diese durch eine Ethik-Kommission bewertet wird. Die Frage, ob Betroffenen ein Widerspruchsrecht zugestanden wird, ist zentral für die Wahrung von deren Grundrecht auf Datenschutz. Das **Betroffenenrecht auf Widerspruch** soll dann nicht zugestanden werden, wenn das Register eine „vollzählige Datenbasis“ anstrebt.

¹⁰ Nähere Informationen hierzu unter <https://www.netzwerk-datenschutzexpertise.de/dokument/datenschutz-im-gesundheitsbereich>.

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

Zu § 8 Meldepflicht meldender Gesundheitseinrichtungen

Die Regelungen in den §§ 8 ff. sehen einen formalisierten Prozess vor, mit dem sich Gesundheitseinrichtungen zur Meldung gegenüber qualifizierten Medizinregistern verpflichten. Damit wird nicht nur eine Befugnis, sondern eine **gesetzliche Datenerhebungs- und Übermittlungspflicht** an das Register begründet, soweit der Betroffene eine pauschalierte Datenfreigabe erklärt hat. Diese „Alles-oder Nichts-Lösung“ zielt auf eine möglichst umfassende Datenverarbeitung ab, ohne spezifische Besonderheiten des Einzelfalls zu berücksichtigen. So wie dies bei der Eintragung in der elektronischen Patientenakte möglich ist, muss es der Gesundheitseinrichtung und dem Patienten möglich sein, eine Meldung im Einzelfall zu unterlassen. Der Verweis in der Begründung, alternativ könne die Gesundheitseinrichtung die Registermeldung auf einer Einwilligung begründen (S. 55), erhöht für diese den Meldeaufwand und schränkt dadurch das Wahlrecht des insofern betroffenen Patienten, der nur bei der Freigabe (§ 9) einbezogen wird, ein.

Zu 9 Datenfreigabe durch die Betroffenen

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.

Die Datenfreigabe entspricht dem bisher praktizierten **Broad Consent**, jedoch mit dem Unterschied, dass die Zustimmung zur Datenverarbeitung nicht mehr für Zwecke differenziert oder eingeschränkt erteilt werden kann, sondern nur pauschal für alle in § 12 genannten Zwecke.

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 sich 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 § 10 Verarbeitung bei Registern mit Widerspruchslösung

Anders als in § 9 vorgesehen, soll offenbar bei Registern mit Widerspruchslösung auch im Einzelfall für den Betroffenen ein Widerspruch möglich sein. Da aber hierauf **nur bei der erstmaligen Meldung** hingewiesen werden muss (§ 13), werden auch in diesen Fällen das Datenminimierungs-Gebot und die Betroffenenrechte ausgehöhlt.

Zu § 12 Zwecke der qualifizierten Medizinregister

Die Regelung repliziert weitgehend 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 identifizierenden 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). Gemäß der Begründung (S. 60) wird dadurch den Anforderungen der Art. 6 Abs. 3 und 4 DSGVO genügt, ohne dass die dort aufgeführten Anforderungen (Zweckvereinbarkeit im Einzelfall, kein Risiko für die Betroffenen, geeignete Garantien wie z. B. Pseudonymisierung) geprüft werden müssen.

Problematisch ist, dass all die genannten Zwecke auch durch den Einsatz sog. **künstlicher Intelligenz** verfolgt werden dürfen und insofern nicht einmal eine Pseudonymisierung identifizierender Daten verpflichtend ist (Abs. 1 Nr. 8). Die Regelung ermöglicht damit den weitgehend uneingeschränkten Einsatz von Medizinregisterdaten für das Testen und Trainieren von KI-Systemen. Der Verweis in der Begründung (S. 62) auf europarechtliche Regelungen, u. a. die KI-Verordnung, ist keine wirksame Begrenzung.

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. Voraussetzung ist lediglich, dass ein irgendwie geartetes „öffentliches Interesse“ bejaht wird. Der Umstand, dass Register zuvor ein Qualifizierungsverfahren haben, ist keine Garantie für das Vorliegen eines öffentlichen Interesses im Einzelfall (das suggeriert aber die Begründung, S. 67).

Von den aufgeführten Zwecken ist nur die **wissenschaftliche Forschung** grundrechtlich privilegiert (Art. 5 Abs. 3 GG, Art. 13 S. 1 GRCh). Nur diese steht insofern gleichrangig neben dem Grundrechtsschutz der Betroffenen. Die Gesundheitsberichterstattung, der ein aufwändiges Aggregierungsverfahren zugrunde liegen muss¹², 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 – bleiben äußerst unbestimmt. Die personenbeziehbare Nutzung für diese Zwecke stellt eine große Gefahr für das Persönlichkeitsrecht der Betroffenen dar, zumal diese Zwecke auch direkt personenbezogen verfolgt werden können. Einzige „Grenze“ ist die Erforderlichkeit, ohne dass irgendwelche Vorkehrungen oder Garantien vorgesehen sind. Eine derartig weitgehende Verarbeitungsbefugnis ist **unverhältnismäßig** und daher verfassungswidrig.¹³

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 §§ 17 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 Zeugnisverweigerungschutz** 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.¹⁴ Ein Rückgriff

¹² BVerfG 15.12.1983 – 1 BvR 209/83 u.a., NJW 1984, 419 ff, Rn. 104 ff. (423 f.).

¹³ Weichert, Sekundärnutzung von Gesundheitsdaten (Fn. 8), Kap. 7.5 (S. 37 f.).

¹⁴ Vgl. Weichert, Sekundärnutzung von Gesundheitsdaten (Fn. 8), Kap. 8.1 (S. 39 f.).

auf eine Verhältnismäßigkeitsprüfung¹⁵ zum Schutz vor Einbezug in Strafverfahren ist unzureichend und nicht rechtssicher.

Zu § 12 Abs. 4 u. 5 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.

Zu § 13 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 Informationspflicht auf die einmalige Information „über die Zwecke“. Die Anwendbarkeit der Art. 13, 14 DSGVO wird vollständig suspendiert. Notwendig wäre eine Information, die **über die Zwecke hinaus** in jedem Fall die Art und den Umfang der Daten, die konkreten Empfänger und die Rechtsgrundlage benennt.

Die Information erfolgt **gegenüber der Öffentlichkeit**. Die Betroffenen werden nur über diesen Weg informiert. Weshalb dies im „öffentlichen Interesse“ notwendig sein soll, um die „Flexibilität“ der Datennutzung zu gewährleisten (S. 65), ist nicht ersichtlich.

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 (S. 65) genügt nicht. Der Hinweis läuft zudem leer, da die Betroffenen nicht erfahren, wer die 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 – ohne die Flexibilität der Regelung zu beeinträchtigen – in der Form hergestellt werden, dass dem ZMR alle Übermittlungen, Zusammenführungen oder Zweckänderungen angezeigt werden und das ZMR diese allgemein z. B. über das **Internet-Verzeichnis** bekannt macht (s. o. zu § 5).

Zu § 14 Personenbezogene 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 kann grds. sinnvoll sein. 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 sensibler Daten von anderen Betroffenen führen (vgl. das Verfahren der Zuordnungssicherung in § 8a AZRG).

¹⁵ Vgl. BVerfG 25.09.2023 – 1 BvR 2219/20 Rn. 13-15, NVwZ 2024, 416.

Selbst für diese hochriskante Form der Datenverarbeitung ist keine individuelle, sondern nur eine **öffentliche Information** vorgesehen (Abs. 2). Diese öffentliche Information soll durch die Register erfolgen und nicht durch das ZMR. So ist angesichts der Vielzahl von möglichen Kooperationen für Betroffene nicht im Ansatz nachvollziehbar, was mit ihren Daten passiert. Auf die Ausführungen zu § 13 wird verwiesen.

Zu §15 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“ (Abs. 3).

Die Regelung zielt auf eine Zusammenführung der bisherigen Register für vielfältige Zwecke ohne wirksame datenschutzrechtliche Vorkehrungen. 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, etwa durch die Datenschutzaufsicht oder auch durch eine Ethik-Kommission, 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 § 16 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 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 (Abs. 5 u. 6) sind ungenügend: Die Register entscheiden über die Nutzungsanträge, ohne dass sie hierfür qualifiziert und unabhängig genug sind. Für die Betroffenen ist die Weiternutzung ihrer Daten über die Veröffentlichung durch das ZMR nur ansatzweise erkenn- und überprüfbar. Eine Veröffentlichungspflicht der Ergebnisse der Datennutzung, wie sie in Art. 61 Abs. 4 EHDS vorgesehen ist, ist nicht vorgesehen. So ist auch kaum eine nachträgliche Überprüfung der erfolgten Datennutzung möglich. Die Regelung ist in der vorliegenden Form unverhältnismäßig.¹⁶

Zu §§ 17 f. Sanktionsbewehrte Geheimhaltungspflichten

Die Regelungen sehen sanktionsbewehrte Zweckbindungs- und Geheimhaltungspflichten für die Datennutzenden vor. Diese Nutzenden genießen jedoch kein strafprozessuales

¹⁶ Zu den rechtlichen Anforderungen ausführlich Weichert, Sekundärnutzung von Gesundheitsdaten (Fn. 8), Kap. 10 (S. 42 ff.).

Zeugnisverweigerungsrecht; deren Daten unterliegen keinem Beschlagnahmeverbot (s. o. zu § 12). Noch problematischer ist, dass die strafrechtliche Sanktionsmöglichkeit gemäß § 18 Abs. 3 von einem Strafantrag insbesondere der Betroffenen abhängig gemacht wird. Betroffene erhalten aber regelmäßig keine Kenntnis von Verstößen gegen § 17, 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.¹⁷

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.

Zu § 19 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. 5 vorgesehene **Speicherdauer** von 100 Jahren, die dem § 303d Abs. 4 SGB V in Bezug auf das FDZ entspricht, wird mit Forschungsinteressen begründet (S. 72). Derartige Forschungsinteressen können aber nicht in Bezug auf sämtliche in Medizinregistern gespeicherten 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.¹⁸

Zu § 20 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. 2 Vorblatt, 20). Dem kann von den Betroffenen widersprochen werden (Abs. 3). 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.

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, die künftig auch für die Umsetzung des EHDS genutzt werden soll (S. 20). 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.

¹⁷ Vgl. Weichert, Sekundärnutzung von Gesundheitsdaten (Fn. 8), Kap. 14.1 (S. 64 f.)

¹⁸ Vgl. Weichert, Sekundärnutzung von Gesundheitsdaten (Fn. 8), Kap. 5.8 (S. 29).

Mit der generellen Verfügbarkeit der Krankenversicherthenummer 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.¹⁹ 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.

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 hierbei ein wirksamer Datenschutz vorgesehen:

- Das für die Administration des Gesetzes vorgesehene Zentrum für Medizinregister (ZMR) ist nicht unabhängig genug und wird ungenügend ausgestattet.
- Die Information der Betroffenen erfolgt nicht konkret im Einzelfall, sondern nur allgemein, so dass den Transparenzfordernissen des Art. 14 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. Hierin liegt ein Verstoß gegen die Art. 6 Abs. 3 u. 4 DSGVO sowie gegen Art. 9 Abs. 2, 89 Abs. 2 DSGVO).
- Die undifferenzierte Speicherfrist von 100 Jahren verstößt gegen das Datenminimierungsgebot von Art. 5 Abs. 1 lit. c DSGVO.
- 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 fehlt an Schutzvorkehrungen bei der Nutzung der Krankenversicherthenummer.
- Es fehlt an einer Regelung zur Evaluierung und Befristung des Gesetzes.
- Die Vorgaben des Data Governance Acts hinsichtlich der Transparenz und Unabhängigkeit der datenaltruistischen Organisationen werden vollständig ignoriert.

Eine Auseinandersetzung mit dem Datenschutz findet in dem Entwurf nur ungenügend 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. 26). Tatsächlich verstößt der Entwurf in vieler Hinsicht gegen die Datenschutz-Grundverordnung sowie grundsätzlich gegen das europarechtlich und verfassungsrechtlich garantierte Grundrecht auf Datenschutz.

Der Entwurf muss daher überarbeitet werden. Dabei sind folgende Regelungen aufzunehmen:

- Das Register in § 5 ist umfassend zu einem Register auszubauen, das den Anforderungen des Art. 17-19 DGA wie auch den Informationspflichten des Art. 14

¹⁹ Weichert in Kühling/Buchner, DS-GVO BDSG, 4. Aufl. 2024, Art. 87 Rn. 11.

DSGVO für die Betroffenen entspricht. Hierbei aufzunehmen sind die wesentlichen in § 6 aufgeführten Angaben, sowie Angaben über Einnahmequellen, Unabhängigkeit, Datenempfänger und Umsetzung der Betroffenenrechte.

- Anstelle der Maximalspeicherfrist von 100 Jahren sind zweckgebundene differenzierte Speicher- und Pseudonymisierungsfristen aufzunehmen.
- Statt der pauschalen Freigabe sind auch differenzierte Freigabemöglichkeiten für die Betroffenen vorzusehen.
- Die Zulassung der Datennutzungen durch die Register bedarf in jedem Einzelfall (§§ 15, 16) einer unabhängigen Kontrollmöglichkeit. Hierzu ist neben der Transparenz für die Betroffenen zumindest eine Anzeige gegenüber der zuständigen Datenschutzaufsicht geboten.
- Hinsichtlich der Sekundärnutzungszwecke ist zu differenzieren zwischen Forschung, bei der auch mit pseudonymisierten Einzelfalldatensätzen gearbeitet werden darf, und nicht-privilegierten Nutzungen, bei denen eine darüber hinausgehende Aggregation der Datensätze nötig ist.
- Die Daten der Register müssen gesetzlich von einem der Strafprozessordnung entsprechenden Zeugnisverweigerungsrecht und Beschlagnahmeverbot erfasst werden.
- Taten gemäß der Strafvorschrift des § 18 sind als Officialdelikt auszugestalten, die ohne Antragserfordernis verfolgt werden können.
- Eine Evaluierungsklausel ist aufzunehmen, um nach zwei Jahren Praxis zu prüfen, inwieweit die vorgesehenen Schutzvorkehrungen genügen oder ob ergänzende Schutzregelungen angezeigt sind

Für Erläuterungen stehen wir gerne zur Verfügung.

Mit freundlichen Grüßen
Dr. Thilo Weichert