

Stellungnahme zum Entwurf der Bundesregierung (BReg) „Entwurf eines Gesetzes für Daten und digitale Innovation im Gesundheitswesen“ (GeDIG) – BR-Drs. 448/26 v. 14.08.2026

insbesondere zum Gesundheitsdatennutzungsgesetz und zur geplanten
Forschungskennziffer

Stand: 17.09.2026

Inhalt

1	Allgemeines.....	2
2	Zu den konkreten Regelungsvorschlägen.....	3
2.1	Zu Änderungen in Art. 1 hinsichtlich des Forschungsdatenzentrums (FDZ).....	3
2.2	Zu den §§ 1 Abs. 4, 24 Vorrang vor dem Gendiagnostikgesetz (GenDG).....	4
2.3	Zu den §§ 3, 10 Abs. 1 u. 2, 11 Abs. 2 GDNG-E – Forschungskennziffer (FKZ).....	4
2.4	Zu §§ 6-8, 18, 19 – Zugangsstellen für Gesundheitsdaten.....	7
2.5	Zu §§ 10, Abs. 2, 11 Abs. 3, 14 – Technische Infrastruktur.....	10
2.6	Zu § 15 – Datenschutzrechtliche Informationspflichten.....	11
2.7	Zu § 17 – Betroffenenrechte-Register.....	11
2.8	Zu §§ 17, 25 – Datenschutzaufsicht.....	12
2.9	Zu § 26 – Verknüpfung von FDZ-Daten mit Daten aus Krebsregistern.....	13
2.10	Zu § 27 – Registrierungs- und Publikationspflichten bei Forschungsprojekten.....	13
2.11	Zu §§ 28, 29 – Geheimhaltungspflichten und Strafvorschrift.....	13
2.12	Zur unzureichenden Wahrung des Patientengeheimnisses.....	14
3	Ergebnis.....	15

Thilo Weichert

Waisenhofstraße 41, 24103 Kiel

0431 9719742

weichert@netzwerk-datenschutzexpertise.de

Karin Schuler

Kronprinzenstraße 76

53173 Bonn

0228 2024733

schuler@netzwerk-datenschutzexpertise.de

www.netzwerk-datenschutzexpertise.de

Am 15.07.2026 beschloss das Bundeskabinett den „Entwurf eines Gesetzes für Daten und digitale Innovation im Gesundheitswesen“ (GeDIG) und brachte diesen ins Gesetzgebungsverfahren ein (BR-Drs. 448/26).

Der Entwurf befasst sich mit einer Vielzahl von Themen im Zusammenhang mit der Digitalisierung des Gesundheitswesens. Ein wesentlicher Teil hat die Umsetzung des Europäischen Gesundheitsdatenraums (European Health Data Space – EHDS) zum Ziel. Hierbei geht es u. a. darum, unter Beachtung des Kapitels IV des EHDS nationale Regelungen für eine Sekundärnutzung von Gesundheitsdaten zu schaffen.

Hierfür sind grundlegende Änderungen des Gesundheitsdatennutzungsgesetzes (GDNG) vorgesehen (Art. 7 GeDIG) sowie weitere damit zusammenhängende Änderungen im Sozialgesetzbuch V (SGB V, insbes. Art. 1 GeDIG).

Das Netzwerk Datenschutzexpertise hat mit Datum vom 13.03.2025 ein umfangreiches Gutachten „Sekundärnutzung von Gesundheitsdaten“ erstellt, in dem eine Analyse der damals verabschiedeten Regelungen des GDNG im Hinblick auf europäisches Recht und insbesondere des EHDS erfolgt. Auf dieses Gutachten wird im Folgenden Bezug genommen:

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

Dem Kabinettsentwurf ging ein Referentenentwurf des Bundesgesundheitsministeriums voraus, der mit Stand 26.05.2026 im Netz veröffentlicht wurde:

https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/G/GeDIG_RefE.pdf

Gegenüber dem Referentenentwurf wurden teilweise wesentliche Änderungen vorgenommen, auf die Bezug genommen wird (GDNG-RefE). Soweit im folgenden Text Seitenangaben gemacht werden, beziehen sie sich auf den Regierungsentwurf in der Bundesratsdrucksache 448/26.

1 Allgemeines

Die Intention des Gesetzentwurfs, die Digitalisierung im Gesundheitswesen voranzutreiben und die nationalen Regelungen an die Vorgaben des Europäischen Gesundheitsraums (European Health Data Space – EHDS)¹ anzupassen, werden begrüßt.

Eine umfassende Stellungnahme zu dem Entwurf ist angesichts der vielen unterschiedlichen Themen hier nicht beabsichtigt. Die vorliegende Stellungnahme beschränkt sich auf die geplanten Änderungen des Gesundheitsdatennutzungsgesetzes (GDNG) und die damit in Verbindung stehenden Regelungen zur Sekundärnutzung von Gesundheitsdaten, für die in Kapitel IV des EHDS (Art. 53-81) verpflichtende Vorgaben bestehen und die Relevanz für den Datenschutz der betroffenen Patienten haben. Diese Vorgaben zielen darauf ab, dass „Daten für Zwecke des öffentlichen Interesses, der Unterstützung gesundheitspolitischer Maßnahmen und der wissenschaftlichen Forschung weiterverwendet werden (Sekundärnutzung)“ (S. 109).

¹ Verordnung (EU) 2025/327 v. 11.02.2025, ABl. EU v. 05.03.2025.

Dazu muss der „gesetzliche Rahmen für den Aufbau eines vernetzten, europäisch anschlussfähigen Gesundheitsdatenökosystems geschaffen“ werden (S. 4). Ein zentraler Bestandteil hierfür ist der Ausbau des Forschungsdatenzentrums Gesundheit (FDZ) (S. 6).

2 Zu den konkreten Regelungsvorschlägen

2.1 Zu Änderungen in Art. 1 hinsichtlich des Forschungsdatenzentrums (FDZ)

In § 303e Abs. 2 Nr. 11 SGB V-E ist – zusätzlich zu den bisherigen Sekundärnutzungszwecken – geplant, auf Antrag eines Leistungserbringers FDZ-Daten bereitzustellen „mit dem Ziel der Vernetzung von Leistungserbringern mit ähnlichen Fällen zum fachlichen Austausch oder zur Anbahnung eines **Konsils**“ (lit. a) und „auf Antrag eines **Sponsors** einer klinischen Prüfung oder einer Stelle, die eine klinische Prüfung durchführt, mit dem Ziel geeignete Prüfungsteilnehmer für diese klinische Prüfung zu ermitteln“ (lit. b). Gemäß § 303e Abs. 5 Satz 4 SGB V-E soll für diese Zwecke das Pseudonym von Leistungserbringern aufgelöst und die betreffende Person durch die Vertrauensstelle identifiziert werden können.

In den beiden Fällen geht es darum, patientenbeziehbare Nutzungen zu ermöglichen. Dies mag zur Durchführung eines fachlich qualifizierten Konsils im Rahmen der primären Leistungserbringung (ärztlichen Versorgung) im Interesse einer Verbesserung der medizinischen Versorgung gerechtfertigt sein. Die Bereitstellung von personenbezogenen Patientendaten an den Sponsor einer klinischen Prüfung lässt sich dagegen auch nicht im Entferntesten mit dem Gemeinwohl rechtfertigen. Das Auffinden geeigneter Prüfungsteilnehmer muss und kann durch die **klinische Prüfung durchführende Stelle** erfolgen.

Gemäß § 303e Abs. 4 S. 4 u. 5 SGB V-E ist geplant, dass die berechtigten Empfänger durch das FDZ nach dem **Verpflichtungsgesetz** – auch per Videoschalte – verpflichtet werden. Dies dient einer unbürokratischen Unterwerfung der Empfänger unter die Regelungen des § 203 Abs. 2 StGB. Dies ist im Interesse der Vertraulichkeit der Datennutzung zu begrüßen, genügt aber – auch angesichts rechtlich begründeter Vollzugsdefizite bei der Durchsetzung der Geheimhaltungsverpflichtung – nicht (dazu s. u. zu § 29 GDNG-E).

In § 303e Abs. 6 S. 2 SGB V-E soll der **Ausschluss von Datennutzenden** von der FDZ-Nutzung für zwei Jahre im Fall eines Datenschutzverstoßes nicht nur durch die Datenschutzaufsicht, sondern auch eigenständig durch das FDZ festgestellt werden können. Dies ist im Interesse der zeitnahen Verhinderung von Datenmissbräuchen zu begrüßen. Dies genügt aber nicht, um die Vertrauenswürdigkeit der Datennutzenden sicherzustellen. Diese muss vor Gewährung des Datenzugangs geprüft und positiv festgestellt werden. Derartiges ist im Gesetzentwurf nicht vorgesehen und muss gesetzlich geregelt werden.²

² Weichert, Sekundärnutzung von Gesundheitsdaten, 13.05.2025, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2025_03_sekundaerntzg_gesdat.pdf, Kap. 9 (S. 40 ff.).

Zu Art. 7 Änderung des Gesundheitsdatennutzungsgesetzes (GDNG-E)

2.2 Zu den §§ 1 Abs. 4, 24 GDNG-E – Vorrang vor dem Gendiagnostikgesetz (GenDG)

Die geplante Regelung sieht vor, dass die neuen GDNG-Normen nicht nur den SGB V (gesetzliche Krankenversicherung – GKV) und SGB XI (gesetzliche Pflegeversicherung – GPV) vorgehen, sondern auch dem Gendiagnostikgesetz (GenDG), „soweit sie den gleichen Sachverhalt regeln“. Es wird klargestellt, dass in Deutschland die **Verarbeitung von Gendaten** (Art. 4 Nr. 13 DSGVO) nur nach **Einwilligung** der jeweils Betroffenen zulässig sein soll, auch soweit es um die Sekundärnutzung gemäß dem EHDS geht. Dies wird in Art. 51 Abs. 1 lit. f, g i u. q, Abs. 4 EHDS erlaubt und ist in § 24 GDNG-E so vorgesehen.

In Art. 10 des Entwurfs ist eine Änderung des GenDG vorgesehen. Danach muss sich die **Aufklärung** vor Einholung der Einwilligung auch auf die Sekundärnutzung von Gendaten gemäß dem EHDS erstrecken (§ 9 Abs. 2 Nr. 7 GenDG-E).

Zur Forschungsnutzung von Gendaten enthält das GenDG keine Festlegungen.³ Da im GDNG und im EHDS Sekundärnutzungen nicht nur für Forschungszwecke, sondern auch für weitere Zwecke erlaubt werden, so dass es zu einer Überschneidung mit dem GenDG kommen kann, wird der Vorrang des GDNG bestimmt. Es ist zu begrüßen, dass von der durch den EHDS eingeräumten Möglichkeit Gebrauch gemacht wird, „strengere Anforderungen“ für die Verarbeitung von Gendaten vorzusehen (S. 247). Es ist jedoch nicht erkennbar, weshalb Gendaten für **andere als wissenschaftliche Sekundärzwecke** genutzt werden sollen. Für solche sonstigen Sekundärzwecke (z. B. Politikgestaltung od. Bildungs- und Lehrtätigkeit, vgl. Art. 53 Abs. 1 EHDS) sind personenbeziehbare Gendaten ungeeignet. Derartige Sekundärnutzungen müssen gesetzlich ausdrücklich ausgeschlossen werden..

Mit dem Vorrang des GDNG vor dem GenDG wird bewirkt, dass das wissenschaftlich begründete „**Trainieren, Testen und Bewerten von Algorithmen** auch in Medizinprodukten, In-Vitro-Diagnostika, KI-Systemen und digitalen Gesundheitsanwendungen“ (Art. 53 Abs. 1 lit. e ii EHDS) per Einwilligung erlaubt werden kann. Es ist zumindest fraglich, ob dabei den hohen Anforderungen an die Wirksamkeit einer informierten Einwilligung sowie an den Schutz von Gendaten in der Praxis genügt werden wird. Es bedarf zumindest zusätzlicher Sicherungen, dass bei der Sekundärnutzung von Gendaten den Anforderungen an die Wissenschaftlichkeit der Forschung⁴ und an das Gemeinwohl (§ 1 Abs. 2 GDNG)⁵ genügt wird.

2.3 Zu den §§ 3, 10 Abs. 1 u. 2, 11 Abs. 2 GDNG-E – Forschungskennziffer (FKZ)

Gemäß § 3 Abs. 1 GDNG-E soll „eine eindeutige, pseudonyme Kennziffer für natürliche Personen (Forschungskennziffer) eingeführt werden“ für „die **Verknüpfung von Gesundheitsdaten** verschiedener Gesundheitsdateninhaber zur Weiternutzung“ und für die Durchsetzung des Widerspruchsrechts nach Abs. 71 Abs. 1 EHDS. Diese soll durch ein von der koordinierenden Zugangsstelle für Gesundheitsdaten festgelegtes technisches Verfahren erzeugt werden. Koordinierende Zugangsstelle soll nach § 7 Abs. 1 das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) sein (§ 7 Abs. 1 GDNG-E). Die Forschungskennziffer (FKZ) soll aus dem unveränderbaren Teil der Krankenversicherungsnummer (KVNr) mithilfe einer unumkehrbaren Berechnung erzeugt

³ § 2 Abs. 2 Nr. 1 GenDG, BR-Drs. 633/08 v. 29.08.2008, 35; dazu Weichert VuR 2025, 285.

⁴ Weichert, Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung, 2022, S. 18 ff.

⁵ Weichert, Datenschutz und Datensicherheit (DuD) 2026, 33 ff.

werden, wobei aus der FKZ kein Rückschluss auf die KVNr möglich sein soll.⁶ Das technische Verfahren soll im Benehmen mit dem Bundesamt für die Sicherheit in der Informationstechnik (BSI) und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) festgelegt werden. Dieses technische Verfahren soll dann „kostenfrei für die Nutzung durch Gesundheitsdateninhaber und weitere Akteure“ bereitgestellt werden (§ 3 Abs. 2 GDNG-E).

Die Gesundheitsdateninhaber müssen in Erfüllung ihrer Pflicht nach Art. 60 Abs. 1 EHDS die von ihnen gehaltenen Datensätze mit der KVNr durch Aufruf einer Anwendung des vom BfArM bereitgestellten Verfahrens eine Kopie erzeugen, die statt der KVNr mit der FKZ versehen ist. Diese Kopie müssen sie getrennt weiterverarbeiten und der anfordernden Zugangsstelle zur Verfügung stellen.

Im Referentenentwurf war vorgesehen, dass zusätzlich zur KVNr und weitere „**unmittelbar identifizierende Daten**“ betroffener Personen ... vor der Zurverfügungstellung zu entfernen“ sind (§ 11 Abs. 2 GDNG-RefE, siehe dort die Begründung auf S. 185). Weshalb diese Regelung gestrichen wurde, ist unklar. Tatsächlich kann über Merkmalsdaten trotz der Pseudonymisierung eines Datensatzes mit Hilfe der FKZ regelmäßig eine Identifizierung vorgenommen werden. Angesichts der allgegenwärtigen Nutzung (und Speicherung in medizinischen Verwaltungssystemen) vieler identifizierender Daten (Namen, Geburtsdatum, Adresse, Telefonnummer, E-Mail-Adresse) bei Gesundheitsdateninhabern (Ärzten, Krankenhäusern usw.) gibt es vielfältige Ansatzpunkte für eine Reidentifizierung von Personen anhand eines solchen Datensatzes.. Dies gilt besonders, wenn Art der Erkrankung, Behandlungsdatum und Behandlungsort bekannt sind. Der Entwurf sieht weder ein für Gesundheitsdateninhaber verbindliches Anonymisierungsverfahren vor noch insgesamt ein Verfahren, das Reidentifizierungen wirksam ausschließt.

Unter Einsatz der FKZ darf die Zugangsstelle dann die Datensätze zwecks Verknüpfung mit anderen für die Sekundärnutzung zugelassenen Daten an weitere berechnigte Stellen zur Datennutzung weitergeben (§ 3 Abs. 4 GDNG-E). Die Nutzung der FKZ wird erlaubt, wenn dies für die Datensatz-Verknüpfung **für Sekundärzwecke erforderlich** ist. Dies soll auch der Fall sein, wenn die Verknüpfung per Einwilligung legitimiert wird (S. 229). Derartige Einwilligungen können wegen ihrer Unbestimmtheit (sog. broad consent) nicht ansatzweise den Anforderungen an Einwilligungen in den Art. 4 Nr. 11, Art. 7 DSGVO genügen. Es bedarf daher verbindlicher zusätzlicher Schutzvorkehrungen, um die Betroffeneninteressen zu wahren. Die Details des Verfahrens soll das Bundesministerium für Gesundheit (BMG) in einer Rechtsverordnung konkretisieren (§ 3 Abs. 5 GDNG-E). Es ist fraglich, ob hierüber ein wirksamer Betroffenenenschutz bewirkt werden kann.

Die **Krankenversicherungsnummer** (§ 290 SGB V) bzw. deren unveränderbarer Teil (KVNr) liegt bei GKV-Leistungserbringern und u. a. bei der Renten- und der Unfallversicherung vor, ist aber bisher nicht allen Gesundheitsdateninhabern bekannt. Um deren Daten einer Sekundärnutzung über die FKZ zuführen zu können, benötigen sie wegen des (oben beschriebenen) vorgesehenen Verfahrens zukünftig in jedem Fall die KVNr. § 3 Abs. 3 GDNG-E erlaubt ihnen daher eine solche Datenerhebung und -speicherung. Allerdings macht das Gesetz die Erlaubnis entgegen dem Erforderlichkeitsgrundsatz nicht davon abhängig, dass die Daten tatsächlich für Sekundärzwecke genutzt werden sollen.⁷ Die Verarbeitung der KVNr durch solche Stellen stellt daher einen Verstoß gegen das Datenminimierungsgebot nach Art.

⁶ Einen ähnlichen Regelungsvorschlag enthält § 20 Abs. 1 MRG-E, BT-Drs. 21/5922 v. 13.05.2026.

5 Abs. 1 lit. c DSGVO dar. Die Speicherung der KVNr und die dadurch bewirkte weite Verbreitung der KVNr in vielen nicht erforderlichen Fällen begünstigt deren Missbrauch. Ebenso wie die FKZ (s. u.) ist die KVNr eine nationale Kennziffer, deren Missbrauch durch Garantien verhindert werden muss.⁸ Die in § 290 Abs. 4 SGB V geregelte Zweckbeschränkung ist insofern ungenügend.

Die Gesetzesbegründung geht zu Recht davon aus, dass es sich bei der FKZ als „unique identifier“ um eine **nationale Kennziffer** i. S. v. Art. 87 DSGVO handelt (S. 4). Art. 87 DSGVO erlaubt solche Kennziffern „nur unter Wahrung geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person“ gemäß der DSGVO. Die Gesetzesbegründung im Referentenentwurf behauptete, dass die Anforderungen des geplanten § 3 GDNG diesen Anforderungen genüge (S. 172). Der Regierungsentwurf schweigt zu dieser zentralen europarechtlichen Frage. Tatsächlich wird den europarechtlichen Anforderungen nicht genügt, da konkrete Festlegungen für die Garantien in einer Rechtsverordnung und nicht in einem Gesetz vorgenommen werden sollen.⁹ Während die KVNr ausschließlich zur eindeutigen Identifizierung genutzt werden darf, dient die FKZ der Verknüpfung von – möglicherweise vielen und großen – Datensätzen. Daher besteht bei der FKZ eine gesteigerte Gefahr, dass mit ihr umfassende Persönlichkeitsprofile erstellt werden. Vorkehrungen hiergegen werden nicht geregelt. Die geplante Regelung verstößt daher gegen höherrangiges Europarecht.

Das nach § 3 Abs. 2 S. 1 GDNG-E nötige „**Benehmen**“ mit dem BSI und dem BfDI bei der Festlegung des Verfahrens zur Generierung der FKZ stellt keine Garantie i. S. v. Art. 87 DSGVO dar.¹⁰ Benehmen ist eine Form der Mitwirkung bei einem Rechtsakt. Während „Einvernehmen“ bedeutet, dass vor einem Rechtsakt das Einverständnis einer anderen Stelle vorliegen muss, muss bei einer Entscheidung, die nur im Benehmen mit einer anderen Stelle zu treffen ist, nicht das Einverständnis der anderen Stelle vorliegen. Vielmehr kann von der Äußerung der beteiligten Stelle abgewichen werden. Im Rahmen der Benehmensherstellung muss zwar eine gesteigerte materielle Berücksichtigung erfolgen, die sich in einer ernsthaften Bemühung um die Herstellung des Einvernehmens äußert. Doch hier besteht ein Behördenermessen bzw. ein nicht überprüfbarer Beurteilungsspielraum.¹¹

Unabhängig davon, ob das BSI und der BfDI der Art der Generierung der FKZ zugestimmt haben, handelt es sich bei dem geplanten Verfahren um eine relativ **einfach angreifbare Form einer Pseudonymgenerierung**. Die Zahl der berechtigten Nutzenden des FKZ-Verfahrens ist nicht eingegrenzt, so dass die Nutzung des Algorithmus durch diese oder durch weitere nicht berechnete Personen oder Stellen nicht im Ansatz kontrolliert werden kann. Um den Missbrauch einer FKZ zu vermeiden, dürfte eine regelmäßige Anpassung des generierenden Algorithmus nötig sein.

Gemäß § 11 Abs. 1 GDNG-E darf zur Erfüllung des Anspruchs auf Datenzugang sowohl zur Vorbereitung als auch zur Umsetzung des Datenzugangs die **Verknüpfung von Datensätzen**

⁷ So enthält z. B. das Nationale Obduktionsregister (NAREG) keine KVNr, <https://naton.network/nareg/informationen/register/>.

⁸ Weichert in Kühling/Buchner, DS-GVO BDSG, 4. Aufl. 2024, Art. 87 Rn. 22.

⁹ Ebenso die Stellungnahme der unabhängigen Datenschutzbehörden der Länder v. 18.05.2026, S. 4 f.

¹⁰ Kritisch ebenso Stellungnahme der unabhängigen Datenschutzbehörden der Länder v. 18.05.2026, S. 5.

¹¹ Ramsauer in Kopp/Ramsauer, VwVfG, 25. Aufl. § 9 Rn. 82; Henneke/Berger in Knack/Henneke, VerwVfG, 11. Aufl. 2020, § 35 Rn. 88.

durch die zuständige Zugangsstelle mit der FKZ vorgenommen werden. Die Bereitstellung der Daten soll in einer sicheren Verarbeitungsumgebung erfolgen. Dabei wird den Gesundheitsdatennutzern die FKZ nicht offengelegt (§ 11 Abs. 2 GDNG-E).¹²

Die Bereitstellung in der sicheren Verarbeitungsumgebung, ohne dass den Datennutzern die FKZ offengelegt wird, soll gemäß der Gesetzesbegründung dadurch ermöglicht werden, dass die Datensätze bei der Bereitstellung an die Datennutzern nochmals **projektbezogen pseudonymisiert** werden. Diese Zuordnungen der FKZ mit dem Projektpseudonym müssen von den Zugangsstellen aufbewahrt werden, damit bei wesentlichen Befunden nachträglich eine Zuordnung zur FKZ und letztlich zum Betroffenen möglich ist (S. 239), so wie dies in Art. 58 Abs. 3 EHDS geregelt ist. Wenn der Datennutzer – wie die in § 14 Abs. 3 GDNG-RefE noch ausdrücklich vorgesehen war und in der Praxis wohl ein weit verbreiteter Fall – eigene Daten in die Auswertung einbringt, so ist unklar, wie hierbei zu verfahren ist. Aus der Begründung ergibt sich, dass der Datennutzende seine eigenen Forschungsdaten der Zugangsstelle zur Verfügung stellen soll, damit dort eine Projektpseudonymisierung erfolgen kann. Weiter heißt es dort, es sei sicherzustellen, „dass durch die Verknüpfung kein erhöhtes Identifikationsrisiko für die betroffenen Personen besteht“ (S. 240). Dies ist in der Praxis kaum zu erreichen, wenn die von Datennutzenden selbst eingeführten Daten für diesen einen Personenbezug haben. Dies wird regelmäßig der Fall sein.

2.4 Zu §§ 6-8, 18, 19 – Zugangsstellen für Gesundheitsdaten

In § 6 GDNG-E werden die Stellen beschrieben, die nach nationalem Recht die Genehmigung für den **Zugang zu Gesundheitsdaten** erteilen und diesen Zugang technisch gewähren, deren weitere Nutzung kontrollieren und die hierzu vorgesehene Kommunikation vornehmen (Art. 57 EHDS).

Festgelegt wird als „**koordinierende Zugangsstelle**“ in erster Linie das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM), welches die Aufgaben der nationalen Kontaktstelle für die Sekundärnutzung im EU-Rahmen wahrnimmt und die Tätigkeit der nachgeordneten domänenspezifischen Zugangsstellen (§ 9 GDNG-E) koordiniert (§ 7 GDNG-E). Die koordinierende Zugangsstelle ist auch zur Durchsetzung der nach Art. 63, 64 EHDS vorgesehenen Maßnahmen befugt (§ 18 GDNG-E). Sie soll Beschwerden entgegennehmen und bearbeiten (§ 19 GDNG-E).

Art. 55 Abs. 3 EHDS verpflichtet zur **unabhängigen Aufgabenwahrnehmung**: „Die Mitgliedstaaten stellen sicher, dass jegliche Interessenkonflikte zwischen den organisatorischen Teilen von Zugangsstellen für Gesundheitsdaten, die die verschiedenen Aufgaben dieser Stellen wahrnehmen, vermieden werden, beispielsweise durch organisatorische Schutzmaßnahmen wie die Trennung zwischen den verschiedenen Aufgaben der Zugangsstellen für Gesundheitsdaten, einschließlich der Bewertung von Anträgen, des Empfangs und der Aufbereitung von Datensätzen.“ Interessenkonflikte sind mit den einschlägigen Interessenträgern zu vermeiden (Art. 55 Abs. 4 EHDS). „Zugangsstellen für Gesundheitsdaten sollten ihre Entscheidungen über den Zugang zu elektronischen Daten für die Sekundärnutzung unbeeinflusst treffen und jegliche Interessenkonflikte vermeiden. Daher

¹² Im Entwurf eines Forschungsdatengesetzes (FDG) des Bundesforschungsministeriums (BMFTR, Stand 22.12.2025) wird in einem § 9 ebenfalls die „Zusammenführung von Daten zu Forschungszwecken“ vorgesehen, was über ein zu schaffendes „Deutsches Zentrum für Mikrodaten“ erfolgen soll auf Grundlage der Steuer-ID (§ 139b AO) oder anderer Kennnummern.

sollten die Mitglieder der Governance- und Entscheidungsstellen jeder Zugangsstelle für Gesundheitsdaten und deren Personal von jeder nicht mit ihren Aufgaben zu vereinbarenden Handlung absehen und keine **nicht vereinbare Tätigkeit** ausüben“ (ErwGr 54 S. 7, 8 EHDS).

Die Unabhängigkeit der Zugangsstelle, insbesondere im Rahmen des **Zugangsgenehmigungs-Verfahrens**, wird durch den Entwurf nicht gewährleistet. Zwar überlässt der EHDS es den Mitgliedstaaten, die Organisation der Zugangsstellen zu regeln. Hierbei müssen aber Interessenkonflikte ausgeschlossen werden. Insofern bieten sich Anleihen an die Datenschutzaufsichtsbehörden an, deren Unabhängigkeit klar geregelt ist (Art. 52 DSGVO) und wozu es schon hinreichend Rechtsprechung gibt.¹³ Zugangsstellen wie Datenschutzbehörden haben hinsichtlich des Grundrechtsschutzes vergleichbare Aufgaben. Von zentraler Bedeutung ist die Unabhängigkeit von der politischen Administration, zumal es sich um einen zentralen Bedarfsträger für Sekundärnutzungen handelt. Die Rechtsaufsicht durch das BMG, die Einbindung in das vom BMG weisungsabhängige BfArM und die Befugnis des BMG, durch Verordnung Vorgaben zu machen, widersprechen dem Erfordernis der Unabhängigkeit.¹⁴

Die **Unabhängigkeit des BfArM** wird schon dadurch beeinträchtigt, dass dieser Stelle im Rahmen der Sekundärnutzung von Gesundheitsdaten weitere gesetzliche Aufgaben zugewiesen sind oder werden sollen. So ist das BfArM der Betreiber der FDZ (§ 303d SGB V). Das BfArM ist als Zentrum für Medizinregister vorgesehen (§ 3 MRG-E).¹⁵ Inwieweit insofern Rollen- und Interessenkonflikte entstehen können, wird vom Entwurf nicht thematisiert, geschweige denn einer Klärung zugeführt.

Die Problematik der Unabhängigkeit besteht insbesondere für die Zugangsgewährung zu Daten für die Forschung (Art. 53 Abs. 1 lit. e EHDS), wo regelmäßig nicht mit anonymisierten Daten gearbeitet werden kann. Im Interesse der **Unabhängigkeit wissenschaftlicher Forschung** müssen Anträge auf Datenzugang ausschließlich nach fachlichen Kriterien beschieden werden. Politische oder auch kommerzielle Interessen haben zurückzustehen. Um dies zu gewährleisten ist es nötig, dass Entscheidungen nicht den Weisungen einer interessierten Stelle unterliegen. Beim BMG handelt es sich jedoch um eine Stelle, bei der in hohem Maße Interessen an Themen und Ergebnissen von Forschungsvorhaben bestehen können.¹⁶

Bei der koordinierenden Zugangsstelle wird ein „**Arbeitskreis zur Gesundheitsdatennutzung**“ eingerichtet. Darin vertreten sein sollen Vertreter von Patientenorganisationen, Leistungserbringer, die Gesundheitsforschung sowie „weiterer betroffener Gruppen und Institutionen“: „Der Arbeitskreis wirkt beratend an der Ausgestaltung, Weiterentwicklung und Evaluation der Aufgabenwahrnehmung der koordinierenden Zugangsstelle für Gesundheitsdaten mit“ (§ 8 Abs. 3 GDNG-E). Es ist unerklärlich, weshalb der BfDI als zentrale Datenschutzeinrichtung des Bundes bei der Besetzung des Arbeitskreises nicht ausdrücklich erwähnt wird. Ohne eine Vertretung der Datenschutzaufsicht und deren Expertise wird der Arbeitskreis nicht in der Lage sein, seine Beratungsaufgaben,

¹³ EuGH 09.03.2010, C-518/07, NJW 2010, 1265, EuGH 16.10.2012, C-614/10, ZD 2012, 563; EuGH 08.04.2014, C-288/12, ZD 2014, 301.

¹⁴ Weichert; Sekundärnutzung (Fn. 2), Kap. 10.2 (S. 44).

¹⁵ BT-Drs. 21/5922 v. 13.05.2026 = BR-Drs. 176/26 v. 27.03.2026.

¹⁶ Bernhardt/Ruhmann/Weichert DANA 1/2023, 23.

bei denen es immer auch um die Wahrung des Datenschutzes und des Patientengeheimnisses geht, adäquat wahrzunehmen.

Um Einzelinteressen etwas entgegensetzen zu können, bedarf es neben der Weisungsfreiheit der Zugangsstellen einer hohen Qualifikation der Entscheidenden sowie der prozeduralen **Einbindung pluraler Interessen**. Eine unverbindliche Einbindung von Interessenträgern sichert keine Unabhängigkeit. Es bedarf einer Verselbständigung der Zugangsstelle, einer Sicherstellung der Weisungsfreiheit der Zugangsstelle sowie einer Einbindung qualifizierter Gemeinwohlinteressen. Ein solches Gemeinwohlinteresse ist der Datenschutz, dessen Vertretung im Arbeitskreis nicht vorgesehen ist. Den europarechtlichen Anforderungen genügen die geplanten Regelungen nicht.

Daneben sind **domänenspezifische Zugangsstellen** vorgesehen, „zur Sicherstellung des erforderlichen Fachwissens“ (§ 9 Abs. 1 GDNG-E), die alleine oder überwiegend in bestimmten Bereichen den Zugang genehmigen und ermöglichen (§ 9 Abs. 2 GDNG-E). Dabei kann es sich auch um teilrechtsfähige Vereinigungen und juristische Personen des Privatrechts als Beliehene handeln. Im Referentenentwurf war vorgesehen, dass deren Bestimmung durch das BMG erfolgt und das im Einvernehmen mit dem Wirtschaftsministerium (BMWE) bei Einbezug von Gesundheitsdateninhabern „aus der industriellen Gesundheitswirtschaft“, mit dem Arbeits- und Sozialministerium (BMAS) bei Dateninhabern „der Renten- und Unfallversicherung“, mit dem Forschungsministerium (BMFTR) bei Dateninhabern der Forschung und mit dem Ministerium des Innern (BMI) bei Statistikämtern (§ 8 Abs. 3 GDNG-RefE). Der Regierungsentwurf enthält keine entsprechenden Konkretisierungen, sondern verweist generell auf das GDNG und das Landesrecht (§ 9 Abs. 1 GDNG-E). Die Gesetzesbegründung nennt das FDZ (§ 303d SGB V) und das geplante Zentrum für Medizinregister (ZMR, § 3 MRG-E)¹⁷ als geborene domänenspezifische Zugangsstellen. Für den universitätsmedizinischen Bereich soll diese Funktion von einem Akteur aus dem Netzwerk Universitätsmedizin übernommen werden (S. 237).

Die domänenspezifischen Zugangsstellen müssen den Anforderungen des Art. 55 Abs. 2 S. 1 EHDS genügen. Aus der Begründung ergibt sich, dass die Zugangsstelle nicht für Zugangsanträge einer eigenen Organisationseinheit zuständig sein kann (S. 238). Dies genügt aber nicht den Anforderungen des EHDS, der „jegliche Interessenkonflikte“ ausschließen will (Art. 55 Abs. 3 EHDS). Die unklare Benennung der Zugangsstellen sowie die in der Gesetzesbegründung angegebenen potenziellen Beispiele für domänenspezifische Zugangsstellen zeigen, dass der Gesetzgeber kein Interesse daran hat, dass die Genehmigung von Datenzugängen von einer tatsächlich **unabhängigen Stelle** erfolgt.

Interessenkonflikte sind auch nicht ausgeschlossen, wenn das BfArM eine Sekundärnutzung vornehmen möchte und in diesen Fällen für die Antragsgenehmigung die vorgesetzte Behörde, das BMG zuständig ist (§ 10 Abs. 3 GDNG-E).

2.5 Zu §§ 10, Abs. 2, 11 Abs. 3, 14 – Technische Infrastruktur

Die **Gesundheitsdateninhaber** sollen, soweit möglich und geeignet, bei der Bereitstellung der mit der FKZ versehenen Datensätze für die Zugangsstellen die Telematik-Infrastruktur (TI) nutzen (§ 12 Abs. 3 GDNG-E).

¹⁷ BT-Drs. 21/5922 v. 13.05.2026 = BR-Drs. 176/26 v. 27.03.2026.

Die pseudonymisierte Bereitstellung durch die Zugangsstellen für die Datennutzer soll in einer **sicheren Verarbeitungsumgebung** erfolgen (§ 13 Abs. 1 S. 2 GDNG-E). Die Notwendigkeit der Verarbeitung in der sicheren Verarbeitungsumgebung gilt für die nationalen Zugangsstellen und für vertrauenswürdige Gesundheitsdateninhaber (Art. 87 Abs. 1 EHDS). Diese sind für die Sicherheit der Verarbeitungsumgebung verantwortlich (Art. 73 EHDS). Über sie erfolgt die Übermittlung an die Datennutzer (Art. 68 Abs. 11 EHDS, ErwGr 77 EHDS). Damit soll eine Konkretisierung der Datensicherungsmaßnahmen, wie sie in Art. 32 DSGVO zur Pflicht gemacht werden, erfolgen (S. 240). Die sichere Verarbeitungsumgebung kann schon vom Dateninhaber zur Verfügung gestellt werden (§ 13 Abs. 2 S. 2 GDNG-E). Die beantragenden Datennutzer können darum bitten, die Daten in einer bestimmten sicheren Verarbeitungsumgebung bereitgestellt zu bekommen (§ 13 Abs. 1 GDNG-E). Die Gesetzesbegründung erklärt, dass eine technische Verbindung der sicheren Verarbeitungsumgebung mit der TI sinnvoll sein kann (S. 239 f.).

Zur technischen Umsetzung können sich die Zugangsstellen Dritter bedienen, wenn diese die Anforderungen des Art. 73 EHDS einhalten. Hierbei handelt es sich um eine **Auftragsverarbeitung** i. S. v. Art. 28 DSGVO. Insofern können auch die Dateninhaber selbst mit der Bereitstellung beauftragt werden (so ausdrücklich § 14 Abs. 2 GDNG-RefE).

Art. 1 Nr. 20 Data Governance Act (DGA) **definiert** die sichere Verarbeitungsumgebung als „die physische oder virtuelle Umgebung und die organisatorischen Mittel, mit denen die Einhaltung der Anforderungen des Unionsrechts, wie der Verordnung (EU) 2016/679, insbesondere im Hinblick auf die Rechte der betroffenen Personen, der Rechte des geistigen Eigentums und der geschäftlichen und statistischen Vertraulichkeit, der Integrität und der Verfügbarkeit, sowie des geltenden Unionsrechts und des nationalen Rechts gewährleistet wird und die es der Einrichtung, die die sichere Verarbeitungsumgebung bereitstellt, ermöglichen, alle Datenverarbeitungsvorgänge zu bestimmen und zu beaufsichtigen, darunter auch das Anzeigen, Speichern, Herunterladen und Exportieren von Daten und das Berechnen abgeleiteter Daten mithilfe von Rechenalgorithmen“.

Folgende **Vorkehrungen** sind für die sichere Verarbeitungsumgebung vorgesehen (Art. 73 Abs. 1 EHDS): Zugriffsbeschränkung auf jeweils projektbezogene zugelassene Nutzende (lit. a, c), technisch-organisatorische Maßnahmen (lit. b), mindestens einjährige Verarbeitungsprotokollierung (lit. e), Überwachung der Sicherheitsmaßnahmen (lit. f). Zudem sind regelmäßige Audits vorgesehen (Art. 73 Abs. 3 EHDS). Die EU-Kommission legt in einem Durchführungsrechtsakt die konkreten Maßnahmen fest (Art. 73 Abs. 5 EHDS).

Zur Gewährleistung der Sicherheit der Verarbeitungsumgebung ist die Durchführung einer Datenschutz-Folgenabschätzung nötig (Art. 35 DSGVO). Zusätzlich ist es geboten, die Pflicht zur Durchführung einer **Zertifizierung** nach den Anforderungen des Art. 42 DSGVO vorzusehen.

Die Datennutzer können **eigene Daten** in die sichere Verarbeitungsumgebung einbringen, wobei diese Datensätze zuvor von der Zugangsstelle projektbezogen pseudonymisiert werden müssen (§ 13 Abs. 3 GDNG-E, S. 240).

2.6 Zu § 15 – Datenschutzrechtliche Informationspflichten

Im Rahmen ihrer **Informationspflicht** nach Art. 13 DSGVO werden Dateninhaber verpflichtet, die von der Verarbeitung Betroffenen darüber zu informieren, „dass die erhobenen Daten

nach Kapitel IV (der EHDS-Verordnung) an Gesundheitsdatennutzer zur Verfügung gestellt werden können“ (§ 15 Abs. 1 S. 1 GDNG-E). Die Gesundheitsdatennutzer sollen gegenüber den Betroffenen keine Informationspflicht gemäß den Art. 13, 14 DSGVO haben. Die vage Ankündigung durch die Gesundheitsdateninhaber, dass die hochsensiblen Gesundheitsdaten künftig möglicherweise für sekundäre Zwecke genutzt werden, ohne dass erkennbar ist, welche Stellen für konkret welche Zwecke dies sein werden, genügt den grundrechtlichen Transparenzanforderungen nicht. Informationelle Selbstbestimmung wird so unmöglich gemacht. Die Nutzung entspricht nicht Treu und Glauben (Art. 8 Abs. 2 S. 1 GRCh).

Überhaupt **keine Informationspflicht** soll bestehen, wenn die Daten zum Zeitpunkt des Inkrafttretens des GeDiG schon erhoben worden sind, selbst wenn die Erhebung auf der Grundlage einer Einwilligung erfolgt ist (§ 15 Abs. 2 GDNG-E). Als Kompensation dieses Verzichts auf die Betroffeneninformation sieht nicht das Gesetz, sondern die Begründung vor, die Transparenz- und Informationspflichten zu diesen „Altdatenbeständen“ könnten durch die koordinierende Zugangsstelle erfolgen, die hierfür „öffentliche Informationskampagnen“ durchführen solle (S. 242). Dies genügt nicht den Transparenzanforderungen der DSGVO (Art. 5 Abs. 1 lit. a, Art. 14 DSGVO).

Es bedarf einer gesetzlichen Regelung, die den Wesensgehalt des Grundrechts auf Datenschutz unter Wahrung der Verhältnismäßigkeit achtet (Art. 52 Abs. 1 GRCh). Es ist nachvollziehbar, dass den Betroffenen von Neuerhebungen oder von Altbeständen von Gesundheitsdaten noch nicht mitgeteilt werden kann, welchen Sekundärnutzungen ihre Daten künftig zugeführt werden. Daher ist es nötig, dann eine **öffentliche Transparenz** herzustellen, wenn die Genehmigung der Sekundärnutzung beantragt und wenn diese erteilt wird. Dies ist über ein Internetportal ohne übermäßigen Aufwand realisierbar.

Art. 58 Abs. 1 u. 2 EHDS sieht Transparenzpflichten vor. Diese sollen „dazu beitragen, eine faire und transparente Verarbeitung gemäß Artikel 14 Absatz 2 der Verordnung (EU) 2016/679 sicherzustellen, indem zum Beispiel Informationen über den Zweck der Verarbeitung und die verarbeiteten Datenkategorien bereitgestellt werden, sodass natürliche Personen verstehen können, ob ihre Daten gemäß **Datengenehmigungen für die Sekundärnutzung** bereitgestellt werden“ (ErwGr 66 S. 4 EHDS).¹⁸ Die geplante Regelung missachtet diese europarechtlich verbindliche Vorgabe.

2.7 Zu § 17 – Betroffenenrechte-Register

Das BMG soll gemäß § 16 GDNG-E eine „geeignete Einrichtung“ mit dem Führen eines „Registers zur Durchführung der Rechte betroffener Personen nach der EHDS-Verordnung“ beauftragen. Dort sollen Betroffene zu jeder Zeit ihren **Widerspruch** nach Art. 71 EHDS erklären können. Ihnen soll zudem ermöglicht werden, hierüber ihr **„Recht auf Nichtwissen“** über wesentliche Befunde“ nach Art 58 Abs. 3 S. 3 EHDS wahrzunehmen. Die Kommunikation zwischen den Betroffenen und dem Register soll entweder über ein elektronisches Endgerät im Rahmen des Kontos zur elektronischen Patientenakte (ePA, § 334 Abs. 1 Nr. 1 SGB V) erfolgen oder über die Ombudsstelle der Krankenkasse (§ 332a SGB V).

Der Widerspruch kann gemäß § 16 Abs. 2 GDNG-E entweder generell erfolgen oder sich auf **„bestimmte Zwecke“** nach Art. 53 Abs. 1 EHDS beschränken. Eine über diese Granularität hinausgehende Widerspruchsmöglichkeit wird mit dem Argument zurückgewiesen, dies würde

¹⁸ Weichert, Sekundärnutzung (Fn. 2), Kap. 12.2 (S. 56 f.).

das Funktionieren des Sekundärnutzungsverfahrens beeinträchtigen (S. 243). Die Widersprüche sollen bei der Gewährung des Datenzugangs berücksichtigt werden, selbst wenn der Antrag über die Zwecke hinausgeht, die der Widerspruch nennt.

Die Registerstelle für die Betroffenenrechte darf die Widerspruchserklärung selbst, die KVNr, die FKZ sowie weitere **erforderliche Daten** verarbeiten (§ 16 Abs. 5 GDNG-E). Die Kommunikation der Betroffenen bzw. der Ombudsstelle soll automatisiert erfolgen, wobei das Verfahren im Benehmen mit dem BSI und dem BfDI festgelegt werden soll (§ 16 Abs. 6 GDNG-E).

Das in § 16 GDNG-E vorgesehen Register genügt nicht den bestehenden Transparenzanforderungen (dazu zu § 15). Es beschränkt sich auf eine pauschale Umsetzung der Rechte auf Widerspruch und auf Nichtwissen. Die verfassungsrechtlich und in der DSGVO vorgesehenen Rechte, etwa auf **Auskunft und Berichtigung** (Art. 8 Abs. 2 S. 2 GRCh, Art. 15 ff. DSGVO) werden vom Gesetzentwurf völlig ignoriert. Diese Rechte sollen vorenthalten werden, obwohl es technisch möglich ist, diesen Rechten Geltung zu verschaffen. Es ist nicht begründbar, dass eine unbestimmte Zahl von Datenempfänger pseudonymisierte Betroffenen Daten erlangen dürfen und diese Daten personenbeziehbar zusammengeführt werden dürfen, dass aber kein Verfahren vorgesehen wird, mit dem diese ihre Betroffenenrechte, insbesondere das auf Auskunft wahrnehmen können.¹⁹ Hierin liegt eine offensichtliche Missachtung des höherrangigen Europa- und Verfassungsrechts.

2.8 Zu §§ 17, 25 – Datenschutzaufsicht

Abweichend von § 40 Abs. 1 Bundesdatenschutzgesetz (BDSG) wird der **Bundesbeauftragte für den Datenschutz und die Informationsfreiheit** (BfDI) in § 17 GDNG-E für zuständig erklärt für die Umsetzung der Widerspruchsrechte nach Art. 71 EHDS wie für jede sonstige Datenverarbeitung gemäß dem Kapitel IV EHDS, also den Regeln zur Sekundärnutzung von Gesundheitsdaten, selbst wenn diese durch nicht-öffentliche Stellen erfolgt. Diese Zuständigkeitskonzentration wird mit Art. 87 Abs. 3 S. 1 GG gerechtfertigt (S. 245). Die Datenschutzaufsicht soll mit den Zugangsstellen zusammenarbeiten (Art. 65 EHDS).

§ 25 GDNG-E sieht vor, dass die zuständige Datenschutzaufsichtsbehörde ein zeitlich und inhaltlich begrenztes **Forschungsprojekt genehmigen** kann, auch wenn die Betroffenen hierzu nicht ihre Einwilligung in die Verarbeitung der Gesundheitsdaten erteilt haben. Die Genehmigung ist eine Ermessensentscheidung. Sie setzt voraus, dass die Forschungsinteressen die Betroffeneninteressen überwiegen, was von Nebenbestimmungen abhängig gemacht werden kann (S. 251).

Eine Nutzung von auf Einwilligungsbasis erhobenen Daten für Forschungsprojekte hat zur Folge, dass eine Verarbeitung entgegen der erteilten Einwilligung erfolgt. In jedem Fall können die Betroffenen nicht erkennen, wer für welche Zwecke ihre Daten verarbeitet. Damit wird die in Art. 5 Abs. 1 lit. a DSGVO geregelte **Transparenzpflicht** verletzt. Den Anforderungen des Art. 14 DSGVO wird nicht genügt, wonach Garantien und geeignete Maßnahmen zur Wahrung der Betroffeneninteressen gefordert sind (Art. 14 Abs. 5 lit. b, c DSGVO; s. o. zu § 15).²⁰ Dadurch, dass von Aufsichtsbehörden erwartet wird, Forschungsprojekte auf Basis einer

¹⁹ Weichert ZD 2025, 255 ff.

²⁰ Stellungnahme der unabhängigen Datenschutzbehörden der Länder v. 18.05.2026, S. 8 f.

datenschutzwidrigen Regelung zu genehmigen, würden diese gesetzlich veranlasst, entgegen ihrem verfassungsrechtlichen Auftrag tätig zu werden.

2.9 Zu § 26 – Verknüpfung von FDZ-Daten mit Daten aus Krebsregistern

Die bisherige Regelung des § 4 GDNG soll zu § 26 GDNG-E werden, wonach die pseudonymisierten Daten des Forschungsdatenzentrums Gesundheit (FDZ) mit Daten der klinischen **Landeskrebsregister** verknüpft werden dürfen. Die Genehmigung erfolgt durch die koordinierende Zugangsstelle.

2.10 Zu § 27 – Registrierungs- und Publikationspflichten bei Forschungsprojekten

Die bisherige Regelung des § 8 GDNG wird zu § 27 GDNG-E und wird dadurch erweitert, dass auch Forschungsprojekte nach den §§ 303a ff. SGB V einer Registrier- und Publikationspflicht unterworfen werden (so Referentenentwurf S. 197). Die Regelung entspricht Art. 61 Abs. 4 EHDS.

Es gibt keinen Grund, Vorhaben, die auf einer **Patienteneinwilligung** basieren, von der (ohnehin beschränkten) Transparenzpflicht auszunehmen, so wie dies in § 27 Abs. 1 GDNG-E vorgesehen ist. Dies gilt besonders, solange bei den betroffenen Projekten auf den sog. „broad consent“ gesetzt wird, der den Anforderungen des Art. 7 DSGVO nicht genügt, die Betroffenen weitestgehend im Unklaren über die weitere Nutzung lässt und der derzeit als Königsweg für die medizinische Forschung genutzt wird.²¹

Der Transparenz abträglich ist in § 27 Abs. 2 GDNG-E zudem die Regelung, dass eine Publikationspflicht nicht bestehen soll, wenn das Forschungsvorhaben auf Grundlage eines Gesetzes bereits **an anderer Stelle registriert** wurde. Betroffene können so nicht erkennen, ob ihre Daten von einem Vorhaben betroffen sein können. Es muss sichergestellt werden, dass den Transparenzpflichten bei der Sekundärnutzung von Gesundheitsdaten an einer zentralen, für die Öffentlichkeit erkennbaren Stelle genügt wird. Nur durch die Möglichkeit, auch im Nachhinein die Sekundärnutzung zu überprüfen, besteht eine informationelle Grundlage, eine Aussage über die Berechtigung der Bereitstellung, über die Beachtung des Gemeinwohls und über die Beachtung des Datenschutzes vorzunehmen.

2.11 Zu §§ 28, 29 – Geheimhaltungspflichten und Strafvorschrift

Der bisherige § 7 GDNG zu **Geheimhaltungspflichten** soll zu § 28 GDNG-E werden, wobei nicht nur Datennutzende, sondern alle beteiligten natürlichen oder juristischen Personen verpflichtet werden, nicht nur Forschende, sondern alle, die gemäß den nach dem GDNG erlaubten Zwecken Daten verarbeiten.

Die bisherige Strafvorschrift des § 9 GDNG wird zu § 29 GDNG-E. Nach § 29 Abs. 1 GDNG-E wird mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft, wer gegen das Zweckänderungs- und Weitergabe- oder das Reidentifizierungsverbot des § 28 Abs. 1 u. 2 GDNG-E verstößt. Eine Strafverschärfung (Freiheitsstrafe bis zu drei Jahren) ist vorgesehen, wenn der Täter „gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen“ (§ 29 Abs. 2 GDNG-E). Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind neben den Betroffenen auch der Verantwortliche sowie die zuständige Aufsichtsbehörde (§ 29 Abs. 3 GDNG-E). Diese Norm entspricht der datenschutzrechtlichen Strafnorm in § 42 BDSG, wobei jedoch der Strafraum in § 29 Abs. 1

²¹ Weichert, Rahmenbedingungen (Fn. 4), S. 99 f.

GDNG-E gegenüber § 42 BDSG im Grundtatbestand geringer ist. Da insofern regelmäßig beide Straftatbestände vorliegen und § 42 BDSG und § 29 GDNG-E sich gegenseitig konsumieren können, kommt jeweils die Norm mit dem höheren Strafmaß zur Anwendung. Einen Verweis auf § 203 Abs. 1 StGB (berufliche Schweigepflicht, Patientengeheimnis) enthält das GDNG nicht.

Bei jedem Strafantrag muss die Antragsfrist von 3 Monaten nach Kenntniserlangung von der Straftat gewahrt werden (§ 77b StGB). Die Gesetzesbegründung zum ursprünglichen GDNG verweist auf das große Schadenspotenzial durch die Tatbegehung des bisherigen § 9 GDNG (jetzt § 29 GDNG-E).²² Angesichts dessen ist das durchgängig (BDSG, GDNG, StGB) vorgesehene **Antragserfordernis** zu restriktiv. Dies gilt insbesondere hinsichtlich der Betroffenen. Bei diesen handelt es sich regelmäßig um Menschen, die von einem Datenschutzverstoß in starkem Maße beeinträchtigt sind, die aber in vielen Fällen von einem Verstoß keine Kenntnis erlangen. Dass ein Verantwortlicher einen Antrag stellt, ist ungewiss, zumal es sich bei dem Täter regelmäßig um ihn selbst oder um dessen Mitarbeiter handelt. Auch die Aufsichtsbehörden können Gründe haben, auf einen Strafantrag zu verzichten. Die Vertraulichkeitsregelungen bei der Nutzung von Gesundheitsdaten – gerade im Fall einer Sekundärnutzung – bestehen im öffentlichen Interesse. Daher sollte auch die Strafverfolgung bei einem Verstoß generell im öffentlichen Interesse liegen. Dies spricht dafür, die anwendbaren Strafnormen als Officialdelikte auszugestalten.

2.12 Zur unzureichenden Wahrung des Patientengeheimnisses

Das GeDIG sieht lediglich Änderungen der Sozialgesetzbücher und des GDNG vor, betrachtet aber nicht, dass sich durch diese Änderungen weitere rechtliche Probleme ergeben, die im Rahmen der vorliegenden Gesetzgebung gelöst werden müssen.

Die Weitergabe von Gesundheitsdaten für Sekundärzwecke führt dazu, dass bei den Datenempfängern die Daten regelmäßig nicht mehr der **Schweigepflicht nach § 203 Abs. 1 StGB** unterliegen. Die Empfänger von Patientengeheimnissen im Rahmen der Regelungen des EHDS bzw. des GDNG sind in vielen Fällen keine Angehörigen von den in § 203 StGB genannten Heil- oder sonstigen Hilfsberufen. Offensichtlich ist, dass ihnen die über die Sekundärnutzung erlangten Patientengeheimnisse nicht offenbart wurden. Daher ist es folgerichtig, dass in den § 29 GDNG-E (bisher § 9 GDNG) eine eigenständige Strafvorschrift enthält.

Eine Konsequenz der Datenweitergabe im Rahmen der Sekundärnutzung ist, dass die betroffenen Daten nicht mehr dem **Beschlagnahme- und Zeugnisverweigerungsschutz** gemäß den §§ 53 Nr. 3, 53a, 97 Abs. 2 StPO unterliegen. Gemäß § 53 Abs. 1 Nr. 3 StPO genießen nur solche Personen ein Zeugnisverweigerungsrecht, denen in ihrer Eigenschaft als Heilberufler Daten „anvertraut oder bekanntgeworden“ sind. Gesundheitsdatennutzer kann nach Art. 2 Abs. 2 lit. u EHDS jede natürliche oder juristische Person sein. Anträge auf Zugang zu Gesundheitsdaten können nach Art. 67 Abs. 1 EHDS alle natürlichen oder juristischen Personen stellen. Der Umstand, dass sekundär genutzte Gesundheitsdaten pseudonymisiert sind, ist kein großes praktisches Hindernis für Strafverfolgungsorgane, da sie mit ihren rechtlichen Befugnissen die Möglichkeit haben, Reidentifizierungen vorzunehmen. Der strafprozessuale Zugriff auf solche Daten wird dadurch erleichtert, dass diese regelmäßig in

²² BT-Drs. 20/9046 (= BR-Drs. 434/23), 58.

digitaler und gut aufbereiteter Form vorliegen.²³ Ein Rückgriff auf eine Verhältnismäßigkeitsprüfung²⁴ zum Schutz vor Einbezug in Strafverfahren ist nicht rechtssicher und unzureichend. Auf die Problematik wurde schon im Rahmen der Sachverständigenanhörung im Bundestag zum Medizinregistergesetz hingewiesen.²⁵

Angesichts des mit dem GeDIG erfolgenden Paradigmenwechsels²⁶ hinsichtlich des Umgangs mit dem Patientengeheimnis ist es dringend erforderlich, eine **Evaluation** der Umsetzung des Gesetzes vorzusehen und so auf Grund der erlangten Erkenntnisse Anpassungen der Regelungen und der Praxis der Sekundärnutzung von Gesundheitsdaten zu ermöglichen. Gemäß § 23 Abs. 1 GDNG-E ist eine Evaluierung der Aufgabenwahrnehmung durch die koordinierende Zugangsstelle erst ab dem 26.03.2029 vorgesehen. Das Datum ist das, ab dem der EHDS direkt anwendbar ist (Art. 105 Abs. 4 EHDS). Damit bleibt der entscheidende Zeitraum des Aufbaus der Infrastruktur zur Sekundärnutzung von Gesundheitsdaten in Deutschland ohne begleitende Kontrolle, was angesichts des hohen Grundrechtsbezugs unverantwortlich ist.

3 Ergebnis

Die geplanten Regelungen in einem GeDIG zur Sekundärnutzung von Gesundheitsdaten widersprechen in folgenden Punkten übergeordnetem Europa- und Verfassungsrecht:

- Die Reidentifizierung pseudonymisierter für Sekundärzwecke genutzter Gesundheitsdaten wird weder technisch noch normativ und damit nicht wirksam ausgeschlossen.
- Die Regelungen zur Forschungskennziffer (FKZ) führen dazu, dass deren Kenntnis und der Zugang zu ihrer Erzeugung weit verbreitet sein werden, eine Kompromittierung der FKZ leicht möglich sein wird und dadurch der Schutz der derart pseudonymisierten Datensätze nicht hinreichend gewährleistet ist.
- Für die als nationale Kennziffer ausgestaltete FKZ sind – entgegen den Vorgaben der DSGVO – keine wirksamen Schutzmaßnahmen geregelt.
- Die Unabhängigkeit der Zugangsstellen, die für die Entscheidung über die Bereitstellung der Gesundheitsdaten sowie für die Bereitstellung selbst zuständig sind, ist nicht gewährleistet.
- Die Information der Betroffenen über die Bereitstellung und Nutzung ihrer leicht reidentifizierbaren Daten ist ungenügend.
- Die Wahrnehmung der Betroffenenrechte ist nicht hinreichend gewährleistet.
- Die Kontrolle von Sekundärnutzungen und die Sanktionierung dabei erfolgender Datenschutzverstöße ist unzureichend geregelt.
- Es fehlt an einem Schutz vor Beschlagnahme und vor einer Zeugnispflicht in Strafverfahren.

Daher sind folgende Änderungen erforderlich:

²³ Ausführlich dazu mit weiteren Nachweisen Weichert, Sekundärnutzung (Fn. 2), Kap. 8.1, 8.2 (S. 39 f.).

²⁴ Vgl. BVerfG 25.09.2023 – 1 BvR 2219/20 Rn. 13-15, NVwZ 2024, 416.

²⁵ Stellungnahme vom 01.06.2026, Deutscher Bundestag, Ausschuss für Gesundheit, Ausschussdrucksache 21(14)89(1), S. 10 f.

²⁶ Bernhardt/Ruhmann/Weichert, DANA 1/2023, 21; Weichert MedR 2025, 500; ders. DANA 2/2024, 66.

- Die Nutzung der Forschungskennziffer bedarf einer präzisen gesetzlichen Regelung mit hinreichenden Garantien zur Verhinderung der Reidentifizierung.
- Die Zugangsstellen sind aus der Hierarchie des BMG herauszulösen. Es ist zu gewährleisten, dass sie ihre Aufgaben qualifiziert und unabhängig wahrnehmen können.
- Zur Gewährleistung einer hinreichenden Sicherheit ist vorzusehen, dass die sicheren Verarbeitungsumgebungen zur Datennutzung entsprechend Art. 42 DSGVO zu zertifizieren sind.
- Das in § 16 GDNG-E vorgesehene Portal zur Wahrung der Betroffenenrechte muss dahingehend ausgeweitet werden, dass die Betroffenen erkennen können, welche Datennutzungen erfolgen bzw. erfolgt sind und dass sie ihr Recht auf Auskunft wahrnehmen können.
- Verstöße gegen die Vertraulichkeitsverpflichtung des GDNG sind als Officialdelikte auszugestalten. Eine wirksame Kontrolle und Sanktionierung muss gewährleistet werden.
- In die Strafprozessordnung sind Regelungen aufzunehmen, die sicherstellen, dass bzgl. der Sekundärdaten keine Zeugnispflicht besteht und keine Beschlagnahme erfolgt.

Die Autoren der vorliegenden Stellungnahme stehen gerne für weitere Erläuterungen und im Rahmen von Beratungen unterstützend zur Verfügung.

Karin Schuler

Dr. Thilo Weichert