Sekundärnutzung von Gesundheitsdaten

Europäischer Gesundheitsdatenraum und Gesundheitsdatennutzungsrecht auf dem Prüfstand

Stand 13.03.2025

Thilo Weichert
weichert@netzwerk-datenschutzexpertise.de
Waisenhofstraße 41, 24103 Kiel
www.netzwerk-datenschutzexpertise.de

Inhalt

Der am 25.03.2025 in Kraft tretende Europäische Gesundheitsdatenraum und diesen umsetzende nationale Regelungen haben einen Paradigmenwechsel hinsichtlich des Schutzes und der Nutzung von Gesundheitsdaten generell und von Patientengeheimnissen speziell zur Folge. Die Sekundärnutzung dieser Daten z. B. für Forschungszwecke wird erleichtert. Um zu gewährleisten, dass hierbei die Grundrechte der betroffenen Patienten gewahrt werden, sind normative und faktische Nachbesserungen nötig.

1 Einleitung

2024 haben sich die Gesetzgebungsorgane der Europäischen Union (EU) auf einen Europäischen Gesundheitsdatenraum (European Health Data Space – künftig abgekürzt als „EHDS“) verständigt, der am 05.03.2025 im Amtsblatt der Europäischen Union veröffentlicht wurde.[1] Parallel dazu beschloss der deutsche Bundesgesetzgeber das Gesundheitsdatennutzungsgesetz (GDNG) sowie Änderungen insbesondere im Sozialgesetzbuch (SGB) V. Damit wird die **Sekundärnutzung von Gesundheitsdaten** unter bestimmten Voraussetzungen erleichtert.

Diese rechtlichen Neuerungen stellen Gesundheitsfachkräfte sowie Patientinnen und Patienten vor völlig neue Herausforderungen: Ärzte und sonstige Personen und Institutionen im Gesundheitswesen müssen die von ihnen generierten Daten zur Verfügung stellen. Die Patienten müssen hinnehmen, dass ihre den Heilberuflern anvertrauten Informationen in pseudonymisierter Form von unbekannten Stellen weitergenutzt werden. Damit ist das Versprechen verbunden, dass die **medizinische Forschung** vorangebracht und die **Gesundheitsversorgung der Menschen** verbessert werden.

Damit einher gehen starke Veränderungen bei der Verarbeitung und Verwaltung der Gesundheitsdaten. Diese werden umfassend digitalisiert und sollen in einer noch zu schaffenden Infrastruktur ausgetauscht werden. Um dennoch die Vertraulichkeit zwischen Gesundheitsberuf und Patient zu wahren, sind im EHDS und in den nationalen Gesetzen Vorkehrungen vorgesehen. Diese werden im Folgenden nach Fragestellungen geordnet und zueinander in Beziehung gestellt. Dabei zeigt sich, dass mit den neuen Regeln ein kompliziertes, teilweise kaum durchsichtiges und inhaltlich unzureichendes Normengeflecht besteht. Dieses soll **verständlich gemacht und zugleich kritisch hinterfragt** werden.

Die neuen europäischen und nationalen Regelungen sind normative Vorgaben, die erst **sukzessive in die Realität umgesetzt** werden. Nicht alles, was erlaubt wird, wird schon gemacht. Der EHDS wird in Bezug auf die Sekundärnutzung von Daten weitgehend erst vier Jahre nach Inkrafttreten rechtlich verbindlich (Art. 105 S. 5 EHDS). Die nationalen

[1] Verordnung (EU) 2025/327 v. 11.02.2025 über den europäischen Gesundheitsdatenraum, ABl. EU v. 05.03.2025.

Umsetzungsregelungen sind teilweise erkennbar als vorläufige Vorgaben konzipiert, die durch weitere Normsetzungen modifiziert und weiterentwickelt werden können. Dies ändert nichts daran, dass die Regelungen den Anspruch auf Verbindlichkeit haben und eventuell schon heute zur praktischen Anwendung kommen.

Gesetzgeber, die Ärzteschaft, Angehörige der sonstigen Heilberufe sowie die Patientinnen und Patienten müssen sich schon jetzt darauf einstellen, was erlaubt, teilweise gemacht und künftig kommen wird. Daher ist es nötig, sich mit den neuen rechtlichen Vorgaben zur Sekundärnutzung von Gesundheitsdaten **intensiv zu befassen**.

Wegen der hohen Komplexität kann keine umfassende Darstellung erfolgen. Der Schwerpunkt wird vorliegend auf die innerstaatliche Umsetzung der Verarbeitung pseudonymisierter Gesundheitsdaten gesetzt. Nur am Rande erwähnt werden die primäre Nutzung von Gesundheitsdaten, die technische und organisatorische Umsetzung der Pseudonymisierung sowie die europaweite bzw. internationale Sekundärnutzung. Der Fokus der folgenden Darstellung liegt auf der **Wahrung des Datenschutzes auf nationaler Ebene**.

2 Normative Grundlagen

Die Regulierung der Nutzung von Gesundheitsdaten erfolgt insbesondere in zwei Rechtsgebieten: im **Medizinrecht und im Datenschutzrecht**.[2] Das Medizinrecht gewährleistet das Patientengeheimnis und erlaubt in engen Grenzen eine Datennutzung für Zwecke der Forschung. Das Datenschutzrecht schützt Gesundheitsdaten als besondere Kategorie von personenbezogenen Daten und regelt sehr umfassend Zweckänderungen. Es gilt bisher das Zweischranken-Prinzip, wonach bei jeder Verarbeitung sowohl das Medizinrecht wie auch die Datenschutz-Vorschriften zu beachten sind.[3] Neuerungen, die ihren Hintergrund insbesondere im europäischen Recht haben, verbinden die beiden Bereiche und vollziehen dabei eine Wendung weg vom Vorrang der Datengeheimhaltung hin zur Datennutzung.

2.1 Das Patientengeheimnis

Das Patientengeheimnis geht als ärztliche Schweigepflicht auf den Eid des Hippokrates (ca. 460 bis 370 vor Christus) zurück. Die Vertraulichkeit zwischen dem **medizinischen Helfenden** und dem Patienten wird geschützt. Der Patient soll sich einer Hilfsperson umfassend anvertrauen können, ohne hierdurch Nachteile befürchten zu müssen. Dadurch soll die Hilfsperson adäquat – individuell, kompetent, situationsbezogen und ausreichend informiert – Hilfe leisten zu können.[4] Das Patientengeheimnis findet in Deutschland seit 1871

[2] Dochow, S. 910 n. w. N.
[3] Weichert in Kühling/Buchner, Art. 9 Rn. 146; Dochow, S. 915, Pöttgen, Medizinische Forschung, 217 ff ; Niggemeier in Augsberg/Düwell/Müller, S. 276 f.
[4] BVerfG 08.03.1972 – 2 BvR 28/71, NJW 1972, 1124; Weichert, Rahmenbedingungen, S. 74; Dochow, S. 798.

strafrechtlichen Schutz (§ 300 RStGB); Verstöße dagegen stehen heute u. a. gemäß § 203 StGB unter Strafe.

Gemäß § 203 Abs. 1 Nr. 1 StGB macht sich strafbar, wer unbefugt ein fremdes Geheimnis offenbart, „das ihm als Arzt, Zahnarzt, … Apotheker oder Angehörigen eines anderen Heilberufs … anvertraut worden oder sonst bekannt geworden ist“. Gemäß § 203 Abs. 3 u. 4 StGB werden Gehilfen der den Heilberuf ausübenden Personen sowie an deren Tätigkeit „mitwirkende Personen“ als Geheimnisträger in die **berufliche Schweigepflicht** einbezogen und können im Fall einer unbefugten Offenbarung strafrechtlich zur Verantwortung gezogen werden.[5]

Das Patientengeheimnis hat eine Vielzahl weiterer normativer Konkretisierungen erfahren. Für Ärzte gelten die **ärztlichen Berufsordnungen**, die sich an der Muster-Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (MBOÄ) orientieren. § 9 MBOÄ regelt die ärztliche Schweigepflicht.

Sekundärnutzungen der aus der Behandlung stammenden Informationen durch Dritte waren im Medizinrecht zunächst nicht vorgesehen. Dem behandelnden Arzt wird aber erlaubt, seine Erfahrungen wissenschaftlich zu nutzen. Die Nutzung von ärztlichen Erkenntnissen für die **Forschung** ist in der Deklaration von Helsinki, die weltweit ethische Grundsätze für Ärzte standesrechtlich festlegt,[6] sowie in § 15 MBOÄ für die deutsche Ärzteschaft einschränkend geregelt.

Mit der Ermöglichung der Sekundärnutzung von Gesundheitsdaten werden der Kreis der Zugangsberechtigten und der Umfang der Nutzung stark erweitert. Erklärtes Ziel bleibt dabei, die berufliche Geheimhaltung generell bzw. die ärztliche Schweigepflicht speziell zu wahren (ErwGr 55 S. 5, 93 S. 2 EHDS). Dessen ungeachtet geht mit dem EHDS und dem entsprechenden nationalen Recht ein **Paradigmenwechsel** einher: Waren Gesundheitsdaten im Interesse der Betroffenen geheim zu halten, was durch das Datenschutzrecht noch verstärkt wurde (s.u. 2.2), so tritt nun die „Sozialpflichtigkeit“ der Daten in den Vordergrund. Die Daten sollen im Interesse der Gesellschaft genutzt werden.[7]

2.2 Der Schutz von Gesundheitsdaten

Das Datenschutzrecht verfolgt primär den Zweck, individuelle Grundrechte und insbesondere das Grundrecht auf Datenschutz (Recht auf informationelle Selbstbestimmung) angesichts einer zunehmenden Digitalisierung zu wahren (s. u. 2.3). Damit soll zugleich das auf Handlungs- und Mitwirkungsfähigkeit der Bürger basierende freiheitlich-demokratische

[5] Ausführlich hierzu Weichert, Rahmenbedingungen, S. 73-91.
[6] Dazu ausführlich Weichert ZfME 2025, 70 ff.
[7] Bernhardt/Ruhmann/Weichert, DANA 1/2023, 21; Weichert GuP 2023, 184; Weichert ZfME 2025, 83.

Gemeinwesen gestärkt werden.[8] Seit der Etablierung des Datenschutzrechts erfolgt eine differenzierte Behandlung von personenbezogenen Daten generell und von besonders schutzwürdigen Daten speziell, zu denen die Gesundheitsdaten gehören. Die Verarbeitung dieser „besonderen Kategorie personenbezogener Daten“ (sog. sensible oder **sensitive Daten**) unterliegt gemäß Art. 9 Abs. 1 Datenschutz-Grundverordnung (DSGVO) zusätzlichen Anforderungen.

Art. 4 Nr. 15 DSGVO definiert „**Gesundheitsdaten**“ als „personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“. Als sensitive Daten sind gemäß Art. 9 Abs. 1 DSGVO u. a. auch genetische Daten sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person geschützt. Auch diese besonderen Datenkategorien können einen Gesundheitsbezug haben (s. u. 5.5 u. 5.7).[9]

Art. 9 Abs. 2 DSGVO **erlaubt die Verarbeitung** von sensitiven Daten, u. a. wenn die betroffene Person ausdrücklich eingewilligt hat (lit. a). Zulässig ist auch die Verarbeitung, wenn sie „auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines **erheblichen öffentlichen Interesses** erforderlich“ ist (lit. g).

Gestattet wird die Verarbeitung zudem „für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die **Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich** auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien“ (Art. 9 Abs 2 lit. h DSGVO). Durch den Verweis auf Art. 9 Abs. 3 DSGVO wird bei dieser Alternative zusätzlich gefordert, dass die befassten Personen einem Berufsgeheimnis unterliegen. Es erfolgt also eine Bezugnahme auf das Patientengeheimnis (s. o. 2.1).

Art. 9 Abs. 2 lit i DSGVO regelt eine weitere Verarbeitungserlaubnis: „Die Verarbeitung ist aus Gründen des **öffentlichen Interesses im Bereich der öffentlichen Gesundheit**, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei

[8] BVerfG 15.12.1983 – 1 BvR 209 u.a., NJW 1984, 422; ausführlich dazu Zimmermann, Datenschutz und Demokratie, 2021.
[9] Zum Gesundheitsbezug genetischer Daten Weichert in Kühling/Buchner, Art. 4 Nr. 134 ff.

Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich".

Schließlich kann auch **Forschung** eine Verarbeitung sensitiver Daten legitimieren: „Die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 erforderlich" (Art. 9 Abs. 2 lit. j DSGVO).

Auch ohne ausdrückliche Einwilligung besteht also eine Verarbeitungserlaubnis „auf der **Grundlage des Unionsrechts oder des Rechts eines Mitgliedsstaats**" in den Fällen der lit. g bis j des Art. 9 Abs. 2 DSGVO.[10] Solche Grundlagen werden nun durch den EHDS, das GDNG und das SGB V geschaffen.

2.3 Grundrecht auf Datenschutz

Der primäre Zweck der DSGVO ist es, „die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten" zu schützen (Art. 1 Abs. 2 DSGVO). Im Vordergrund steht damit das Grundrecht auf Datenschutz nach **Art. 8 GRCh**:

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Das Grundrecht auf Datenschutz gemäß Art. 8 DSGVO ist identisch mit dem 1983 vom BVerfG aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) abgeleiteten „**Recht auf informationelle Selbstbestimmung**".[11]

Die **berufliche Schweigepflicht** (Patientengeheimnis) hat auch eine Grundlage im Schutz der individuellen Privatsphäre[12] bzw. dem Grundrecht auf Datenschutz. Sie findet in Art. 339 AEUV eine normative Konkretisierung für EU-Institutionen. Das Patientengeheimnis dient

[10] Böning/Riechert in Augsberg/Düwell/Müller, S. 233 f.
[11] BVerfG 15.12.1983 – 1 BvR 209/83 u. a., NJW 1984, 419; zum Verhältnis des deutschen zum europäischen Grundrechtsschutzes beim Datenschutz Bretthauer/Spiecker gen. Döhmann JZ 2020, 995.
[12] BVerfG 08.03.1972 – 2 BvR 28/71, NJW 1972, 1124.

zudem dem Schutz der körperlichen und seelischen Unversehrtheit (Art. 2 Abs. 1 GG, Art. 3 GRCh), dem Schutz der Berufsausübung des medizinischen Helfers (Art. 12 GG, Art. 15 GRCh) sowie der Verwirklichung des Sozialstaatsprinzips.[13]

Mit der Bereitstellung von Gesundheitsdaten für Sekundärzwecke erfolgen **Grundrechtseingriffe**. Für die Annahme eines solchen informationellen Eingriffs bedarf es nicht einer aktiven (menschlichen) Kenntnisnahme der Daten und auch nicht, dass ein Personenbezug direkt hergestellt wird oder ein Missbrauch erfolgt. Es genügt, dass personenbeziehbare Daten für einen spezifischen Zweck verarbeitet werden.[14]

2.4 Sonstige digitale Betroffenen-Grundrechte

Bei der Sekundärnutzung von Gesundheitsdaten können weitere Grundrechte tangiert sein. Hierzu gehört das „**Recht auf körperliche und geistige Unversehrtheit**“ (Art. 2 Abs. 2 S. 1 GG, Art. 3 Abs. 1 GRCh).[15] Gemäß Art. 3 Abs. 2 lit. a GRCh muss im Rahmen der Medizin und der Biologie insbesondere „die freie Einwilligung des Betroffenen nach vorheriger Aufklärung entsprechend den gesetzlich festgelegten Modalitäten“ beachtet werden. Relevant sein können weiterhin „das Recht auf Achtung des Privat- und Familienlebens, seiner Wohnung sowie seiner Kommunikation“ (Art. 7 GRCh, Art. 6, 10, 13 GG) sowie das Recht auf Gleichbehandlung (Art. 3 GG, Art. 20 GRCh) sowie die Diskriminierungsverbote u. a. wegen der genetischen Merkmale, einer Behinderung, des Alters oder der sexuellen Ausrichtung (Art. 21 Abs. 2 GRCh, vgl. Art. 23-26 GRCh). Art. 35 GRCh spricht jedem Menschen ein Recht auf Zugang zur Gesundheitsversorgung und auf ärztliche Versorgung zu.[16]

2.5 Forschungsfreiheit

Art. 5 Abs. 3 GG und Art. 13 S. 1 GRCh garantieren die Forschungsfreiheit. Diese Freiheit umfasst auch die medizinische Forschung. Der **Begriff der Forschung** ist bisher nicht gesetzlich definiert, wird aber in vielen Regelungen vorausgesetzt. Gemäß der höchstrichterlichen Rechtsprechung in Deutschland ist Forschung die „geistige Tätigkeit mit dem Ziel, in **methodischer, systematischer und nachprüfbarer Weise neue Erkenntnisse zu gewinnen**“.[17] Dem entsprechen singulär gebliebene Regelungen im Aufenthaltsrecht, wonach Forschung die „systematisch betriebene, schöpferische Arbeit mit dem Zweck der Erweiterung des Wissensstands, einschließlich der Erkenntnisse über den Menschen, die Kultur und die

[13] EuGH 08.04.2014 – C-293/12 u. C-594/12, Rn. 58, NJW 2014, 712; MVVerfG 18.05.2000 – LVerfG 5/98, NVwZ 2000, 1038; SächsVerfGH 14.05.1996 – Vf. 44-II/94, NJW 1996, 1954; BVerfG 19.07.1972 – 2 BvL 7/71, NJW 1972, 2214 (Sozialarbeiter); zur anwaltlichen Schweigepflicht BVerfG 12.04.2005 – 2 BvR 1027/02, NJW 2005, 1919; BVerfG 20.04.2016 – 1 BvR 966/09 u. 1 BvR 1140/09 Rn. 257, DVBl 2016, 779.
[14] Dazu ausführlich Bretthauer/Spiecker gen. Döhmann JZ 2020, 993 f., 996.
[15] Bieresborn, Gesundheitsrecht.blog Nr. 33, 2023, 4.
[16] Bernhardt/Ruhmann/Weichert, DANA 1/2023, 21.
[17] BVerfG 25.09.2023 – 1 BvR 2219/20 - BVerwG 27.06.2024 – 2 C 5.23, Rn. 11, NVwZ 2024, 1575; BVerfG 29.05.1973 – 1 BvR 424/71 u. 325/72, NJW 1973, 1176.

Gesellschaft, sowie der Einsatz dieses Wissens mit dem Ziel, neue Anwendungsmöglichkeiten zu finden“ ist.[18]

Vom Forschungsbegriff erfasst ist sowohl die Grundlagenforschung wie auch die anwendungsbezogene Forschung.[19] Voraussetzung ist, dass bei der wissenschaftlichen Tätigkeit genügend **Unabhängigkeit und Selbständigkeit** verbleiben.[20]

Gemäß der ganz herrschenden Meinung kann aus der Forschungsfreiheit kein Anspruch auf Datenzugang abgeleitet werden. Dies bedeutet jedoch nicht, dass sie bei der Gewährung von Datenzugängen keine Rolle spielt. Vielmehr muss der Stellenwert des Grundrechts beachtet werden, über Fragen eines Datenzugangs muss „sachgerecht, also frei von Willkür und unter angemessener Berücksichtigung des Anliegens entschieden“ werden.[21]

In Umsetzung der Forschungsfreiheit enthält Art. 5 Abs. 1 lit. b DSGVO eine **Privilegierung** bei der Sekundärnutzung von personenbezogenen Daten: Diese Nutzung ist „nicht unvereinbar mit den ursprünglichen Zwecken“, wenn den Anforderungen des Art. 89 Abs. 1 DSGVO genügt wird. Diese Regelung verpflichtet zu „geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person“ gemäß der DSGVO: „Mit diesen Garantien wird sichergestellt, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird. Zu diesen Maßnahmen gehört die Pseudonymisierung, sofern es möglich ist, die Forschungszwecke auf diese Weise zu erfüllen. (Art. 89 Abs. 1 S. 2-4 DSGVO). Die DSGVO sieht weitere Privilegierungen für die Verarbeitung für Forschungszwecke vor, und zwar in Bezug auf die Betroffenenrechte (Art. 89 Abs. 2 DSGVO, s. u. 12.1)[22] sowie bei der Datenlöschung (Art. 17 Abs. 3 lit. d DSGVO, dazu s. u. 5.7)[23].

Die Forschungsfreiheit geht nicht so weit, dass der Forschende selbst bestimmen kann, welche auf gesetzlicher Grundlage beschafften Daten für sein Projekt erforderlich sind. Zumindest bedarf es einer Plausibilität dafür, dass die personenbeziehbaren Daten für die Behandlung der Forschungsfrage geeignet sein können.[24] Werden dagegen Daten auf Vorrat für eine Vielzahl von Forschungsprojekten erhoben und gespeichert, so wie dies bei medizinischen Registern und z. B. auch beim in Deutschland etablierten Forschungsdatenzentrum (FDZ, s. u. 3.1 u. 6.2) der Fall ist, so ist eine **Erforderlichkeitsprüfung**

[18] So Art. 3 Nr. 9 Richtlinie EU) 2016/801 v. 11.05.2016 (REST-RL), ABl. EU v. 21.05.2016, L 132/21; zuvor Art. 2 lit. b Richtlinie 2005/71/EG v. 12.10.2005 (Forscher-RL), ABl. EU v. 03.11.2005, L 289/15; dem folgend § 38a Abs. 1 S. 2 AufenthV.
[19] BVerwG 27.06.2024. 2 C 5.23, Rn. 20, NVwZ 2024, 1576; BVerfG 20.10.1982 – 1 BvR 1467/80, BVerfGE 61, 246, 251 f. = NVwZ 1983, 542 (LS); BAG 21.06.1989 – 7 ABR 58/87, NZA 1990, 402, 404.
[20] BVerwG 27.06.2024. 2 C 5.23, Rn. 20, NVwZ 2024, 1576; ausführlich Weichert, Rahmenbedingungen, S. 20 f. m. w. N.; Weichert ZD 2020, 19 f.
[21] BVerfG 30.01.1986 – 1 BvR 1352/85; Pöttgen, Medizinische Forschung, S. 28 ff. m. w. N.; Bieresborn, Gesundheitsrecht.blog Nr. 33, 2023, 4 f.
[22] Weichert, Rahmenbedingungen, S. 139 ff.
[23] Weichert, Rahmenbedingungen, S. 163 ff.
[24] Kühling/Schildbach NZS 2020, 47.

kaum möglich, da die wissenschaftlichen Fragestellungen sich in einem breiten Spektrum bewegen können. Im FDZ erfolgt insofern eine Datenspeicherung für noch ungewisse Zwecke (Vorratsdatenspeicherung, s. u 5.8).[25] Damit steht das Datenminimierungsgebot des Datenschutzes (Art. 5 Abs. 1 lit. c DSGVO) im Konflikt mit der Wahrheitssuche durch Forschung, da der Umfang der für eine wissenschaftliche Frage herangezogenen Daten regelmäßig ein Qualitätsfaktor für das Forschungsergebnis ist.[26]

2.6 Weitere verfassungsrechtliche Aspekte im Interesse einer sekundären Datennutzung

Für eine verfassungsrechtliche Legitimation der Sekundärnutzung von Gesundheitsdaten können weitere Aspekte relevant sein: Art. 12 GG und Art. 15 GRCh gewähren das Recht, einen frei gewählten oder angenommenen Beruf auszuüben. Hieraus ergibt sich zwar kein Anspruch auf einen Zugang zu fremden Daten. Begründet wird dadurch aber die Befugnis, verfügbare Daten beruflich zu nutzen. Entsprechendes kann aus dem Eigentumsrecht (Art. 14 Abs. 1 GG, Art. 17 GRCh) abgeleitet werden, das aber umfassend einem **Gesetzvorbehalt** und einer Sozialpflichtigkeit unterliegt (Art: 14 Abs. 2 GG, Art. 17 Abs. 1 S. 2 GRCh). Das Recht auf unternehmerische Freiheit hat in der deutschen Verfassung seine Grundlage in der allgemeinen Handlungsfreiheit (Art. 2 Abs. 1 GG) und ist in der GRCh in Art. 16 ausdrücklich normiert.

Inwieweit aus der **Informationsfreiheit** (Art. 5 Abs. 1 S. 1 GG, Art. 11 Abs. 1 S. 2 GRCh) ein Anspruch auf Informationszugang abzuleiten ist, ist umstritten.[27] Sämtliche Grundrechte unterliegen einem Gemeinwohlvorbehalt im Sinne **sozialer Sicherheit** (Art. 20 Abs. 1 GG, Art. 34 GRCh), des Verbraucherschutzes (Art. 38 GRC) und des Umweltschutzes (Art. 37 GRCh).

Die Auswertung von Gesundheitsdaten insbesondere durch die medizinische Forschung dient dem **Gesundheitsschutz** (Art. 35 GRCh) und schafft die Voraussetzung dafür, dass staatliche wie private Einrichtungen ihrem Auftrag zur Wahrung der körperlichen und seelischen Gesundheit nachkommen können (Art. 2 Abs. 2 GG, Art. 3 GRCh).

Die Gewährleistung einer **effektiven, wirtschaftlichen und einfachen Verwaltung** ist zudem ein gewichtiger öffentlicher Belang (Art. 20 Abs. 3 GG).[28] Damit kann angesichts begrenzter Ressourcen eine in Art. 3 GG geforderte Gleichbehandlung ermöglicht werden.

3 Die Regelung der Sekundärnutzung von Gesundheitsdaten

Die Sekundärnutzung von Gesundheitsdaten war über viele Jahre hinweg kein öffentlich erörtertes Thema. Das Patientengeheimnis schloss eine Nutzung für andere als therapeutische

[25] Zur Rechtsprechung hierzu Schiedermair in Simitis/Hornung/Spiecker, Einleitung Rn. 177 ff.
[26] Zur Datenminimierung bei Big Data Bieresborn, Gesundheitsrecht.blog Nr. 33, 2023, 9.
[27] Dazu ausführlich Wegener, Der geheime Staat, 2006, S. 475 ff.
[28] BFH 14.03.2012 – XI R 33/09, Rn. 30 ff.

Zwecke weitestgehend aus, da sie von einer Patienteneinwilligung in Form einer Schweigepflichtentbindung abhängig war. Im Rahmen der gesetzlichen Krankenversicherung wurden durch Änderungen im Sozialgesetzbuch (SGB) V zwar zunehmend Formen der Datenauswertung eingeführt. Deren Ziele stehen jeweils in einem engen Zusammenhang mit der **konkreten Gesundheitsversorgung** und haben insbesondere die Verbesserung der Wirtschaftlichkeit und die Qualitätssicherung im Blick.[29]

3.1 Kleine Geschichte der Sekundärnutzung von Gesundheitsdaten

In den 90er Jahren waren es insbesondere Medizinforschende, die einen verbesserten Zugang zu den primär für Behandlungszwecke erstellten Gesundheitsdaten einforderten. Dieser Forderung stand das Datenschutz- und das Medizinrecht entgegen, das für die Forschungsnutzung der Daten weitgehend die Einwilligung der betroffenen Patienten forderte und nur unter engen Voraussetzungen eine **wissenschaftliche Auswertung** ohne solche Einwilligungen erlaubte. Die sich daraus ergebenden Konflikte wurden ausschließlich zwischen Medizinforschenden und Datenschützern ausgetragen und spielten im öffentlichen Diskurs keine wesentliche Rolle.[30]

Im Interesse einer verstärkten Kontrolle der Gesundheitsausgaben suchte die rot-grüne Bundesregierung 1999 eine verbesserte Datengrundlage. Auf Anraten von Datenschützern wurde im Rahmen der GKV-Gesundheitsreform 2000[31] vorgesehen, dass für Zwecke des Risikostrukturausgleichs (§§ 266 f. SGB V) die **GKV-Abrechnungsdaten** pseudonymisiert gespeichert und ausgewertet werden dürfen.[32] Von Datenschützern wurde dies damals als „echter Durchbruch“ von „Privacy-Enhancing-Technologies“ gefeiert.[33]

Patientengeheimnis und Patientenautonomie sowie das **Datenschutzrecht** machten es – gesetzlich normiert – Medizinforschenden zunehmend schwer, ihre vom technischen Fortschritt und der medizinischen Erkenntnis getriebenen Forschungskonzepte mit den bestehenden normativen Vorgaben in Einklang zu bringen. Die nötigen Einwilligungen und die Zweckfestlegungen bezogen sich jeweils auf konkrete Forschungsprojekte und verhinderten wissenschaftliche Weiternutzungen. Das Datenminimierungsgebot wurde als Hindernis wahrgenommen. Der Internationalisierung von Forschung, deren Langzeitorientierung und dem multifunktionalen Datennutzungsbedarf konnte mit dem rechtlichen Rahmen immer

[29] Weichert DANA 4/1999, 21 f.
[30] Pöttgen, Medizinische Forschung, S. 19 m. w. N., s. a. einerseits Bochnik MedR 1994, 398 u. MedR 1996, 262; andererseits Weichert MedR 1996, 258 ff.; zur Entwicklung auch Weichert ZfME 2025, 75-78.
[31] GKV-Gesundheitsreformgesetz 2000 v. 22.12.1999, BGBl. I S. 2626.
[32] Kühling/Schildbach NZA 2020, 42.
[33] Weichert DANA 4/1999, 23 f.; DSB-Konferenz v. 07./08.10.1999, Patientenschutz durch Pseudonymisierung, vgl. Weichert MedR 2020, 539 f.

schwerer genügt werden. Soweit spezialgesetzliche Regelungen zur Sekundärnutzung bestanden, bezogen sie sich jeweils auf eng begrenzte Anwendungsbereiche.[34]

Der Diskurs zwischen Datenschützern und Medizinforschenden förderte zwar ein zunehmendes gegenseitiges Verständnis für **Persönlichkeitsschutz und Forschungsbedarf**.[35] Die Öffentlichkeit und die Politik zeigten hierfür aber kaum Interesse. Zu einer Anpassung der Rechtsgrundlagen kam es nicht. Die Datenschutzkonferenz, der Zusammenschluss der deutschen Datenschutzaufsichtsbehörden, akzeptierte 2020 den „Broad Consent" als Verarbeitungslegitimation für die Medizin-Informatikinitiative und stellte damit zentrale datenschutzrechtliche Anforderungen an die Einwilligung im Interesse der Forschung zurück: die Bestimmtheit der Einwilligung, die Betroffenentransparenz und die Zweckbindung.[36]

Die Diskussion über die Digitalisierung des Gesundheitswesens führte zu neuen Initiativen auch im Hinblick auf die Sekundärdatennutzung. Ende 2019 trat das von der schwarz-roten Regierung und Gesundheitsminister Jens Spahn auf den Weg gebrachte „Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation" (Digitale-Versorgung-Gesetz - DVG) in Kraft, wodurch die für Zwecke des Risikostrukturausgleichs pseudonym zentral gespeicherten Daten in ein **Forschungsdatenzentrum Gesundheit** (FDZ) überführt und vom Umfang ausgeweitet werden sollten. Eine Vielzahl sekundärer Nutzungszwecke, u. a. auch die Forschung, war vorgesehen (§§ 303a ff. SGB V).[37]

Die praktische Umsetzung des DVG kam nur langsam voran. Dessen ungeachtet führte das neue Gesetz zu einer intensiven **öffentlichen Debatte**.[38] Ein gegen die zentrale Speicherung im FDZ und die geplante Sekundärdatennutzung gerichteter Antrag auf Erlass einer einstweiligen Anordnung gegen das DVG wurde vom BVerfG abgelehnt, wobei das Gericht zugestand, dass der Antragsteller „gewichtige Bedenken gegen die streitgegenständlichen Vorschriften" vorgetragen habe.[39]

In die Diskussion kam rechtstatsächlich wie normativ Bewegung durch die zum Jahreswechsel 2019(/2020 ausgebrochene **Corona-Pandemie**. Der Politik wie der Öffentlichkeit in Deutschland und anderen EU-Mitgliedstaaten wurde schlagartig bewusst, dass die Erfassung von Gesundheitsdaten – anders wie etwa in Israel oder in Großbritannien – unzuverlässig, verstreut, inaktuell und vom Umfang ungenügend ist, um das Pandemiegeschehen erfassen und verstehen zu können. Dies löste geradezu hektische Gesetzgebungsaktivitäten sowohl auf

[34] Dazu ausführlich Schneider, Sekundärnutzung, S. 53 ff.
[35] Krawczak/Weichert, DatenschutzNachrichten (DANA) 4/2017, 193-200 = https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_twmk_vorschlag_dinfmedforsch_v1.9_170927.pdf
[36] Datenschutzkonferenz, 15.04.2020, Beschluss zu den Einwilligungsdokumenten der Medizininformatik-Initiative.
[37] Digitale-Versorgung-Gesetz v. 09.12.2019, BGBl. I S. 2562.
[38] Affirmativ Kühling/Schildbach NZS 2020, 42 ff.; kritisch Weichert MedR 2020, 539 ff.
[39] BVerfG 19.03.2020, 1 BvQ 1/20, JZ 2020, 1012 f. Rn. 8; kritisch dazu Bretthauer/Spiecker gen. Döhmann JZ 2020, 990 ff.

europäischer wie auf nationaler Ebene aus. Diese mündeten in der EU im EHDS[40], auf nationaler Ebene im „Gesetz zur verbesserten Nutzung von Gesundheitsdaten“ (Gesundheitsdatennutzungsgesetz – GDNG).[41] Das GDNG wurde zeitgleich mit einem „Digital-Gesetz“ für den Gesundheitsbereich am 14.12.2023 und am 02.02.2024 vom Bundesrat beschlossen und trat am 31.03.2024 in Kraft.

3.2 Europäischer Gesundheitsdatenraum

Beim Europäischen Gesundheitsdatenraum (European Health Data Space – EHDS) handelt es sich um eine europäische Verordnung, also um supranationales **direkt anwendbares Recht der Europäischen Union** (EU). Es muss bei der Rechtssetzung der EU-Mitgliedstaaten und bei der dortigen Rechtsanwendung zwingend beachtet werden (Art. .288 AEUV). Der EHDS ist Bestandteil der 2020 vorgestellten europäischen Datenstrategie, in der bereichsspezifische Datenräume vorgeschlagen werden, die für bestimmte Lebensbereiche einen Datenaustausch regeln und effektivieren und so zu einer Stärkung im globalen Wettbewerb führen sollen.[42] Die EU hatte sich bis zur Corona-Pandemie wenig um die Gesundheitspolitik in der Gemeinschaft gekümmert. Die Pandemie führte nun dazu, dass der Gesundheitsraum mit Priorität vorangetrieben wurde.[43] Der EHDS soll einen Governance-Rahmen schaffen, „um den Zugang zu elektronischen Gesundheitsdaten für die Zwecke der Primärnutzung von Gesundheitsdaten sowie der Sekundärnutzung dieser Daten zu erleichtern“ (Art. 1 Abs. 1 EHDS). Der EHDS nimmt eine Vorreiterrolle für die Einführung weiterer EU-Datenräume ein und ist insofern eine Blaupause für die Sekundärnutzung anderer Datenkategorien.[44]

Die Europäische Kommission hatte mit Datum vom 03.05.2022 einen Vorschlag für eine „Verordnung über den europäischen Raum für Gesundheitsdaten“ vorgelegt.[45] Am 07.12.2023 gaben der EU-Rat[46] und am 13.12.2023 das Europäische Parlament[47] jeweils eine Stellungnahme ab. Im Frühjahr 2024 haben das Parlament und der Rat im Trilog eine politische Einigung über den Vorschlag der Kommission zum EHDS erzielt. Diese wurde am 24.04.2024 vom Parlament und erst am 21.01.2025 vom Rat angenommen. Die Verordnung wurde am 05.03.2025 **im Amtsblatt der EU** veröffentlicht.[48] Sie trat 20 Tage danach in Kraft und wird später, teilweise erst nach zehn Jahren direkt wirksam (Art. 105 EHDS, ErwGr 115 S.

[40] ErwGr 2f.; 75, 111 EHDS
[41] Weichert GuP 2023, 183 f.
[42] Europäische Kommission, Europäische Datenstrategie (2020). https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de.
[43] Bernhardt/Ruhmann/Weichert, DANA 1/2023, 17 f. mit Hinweisen zu den EU-Kompetenzen.
[44] DSK, EHDS-Stellungnahme v. 27.03.2023, 2.
[45] COM(2022) 197 final 2022/0140 (COD).
[46] Rat der Europäischen Union, 16048/1/23 v. 07.12.2023, 2022/0140(COD).
[47] European Parliament, P9_TA(2023)0462_Amendments adopted by the European Parliament on 13 December 2023 on the proposal for a regulation of the European Parliament and of the Council on the European Health Data Space (COM(2022)0197 – C9-0167/2022 – 2022/0140(COD).
[48] Verordnung (EU) 2025/327 v. 11.02.2025 über den europäischen Gesundheitsdatenraum, ABl. EU v. 05.03.2025.

1 EHDS). Die Regelungen zur Sekundärnutzung (Kapitel IV EHDS) werden weitgehend vier Jahre nach Veröffentlichung wirksam (Art. 105 S. 5 EHDS).

Der EHDS regelt die Verarbeitung von Gesundheitsdaten in elektronischen Gesundheitsaufzeichnungen (Electronic Health Records – EHR) im Rahmen der Gesundheitsversorgung (**primäre Datennutzung**, Art. 2 Abs. 2 lit. j EHDS).

Mit dem EHDS wird zudem das Ziel verfolgt, ein kohärentes, vertrauenswürdiges und effizientes Umfeld für Forschung, Innovation, Politikgestaltung und Regulierungstätigkeiten durch eine **Sekundärdatennutzung** in der gesamten EU zu schaffen.[49] Sekundärnutzung ist die Verarbeitung der Gesundheitsdaten für einen anderen als den ursprünglichen bei der Erhebung verfolgten Zweck (Art. 2 Abs. 2 lit. e EHDS).

Der EHDS stellt gleich zu Beginn fest, dass er die Geltung der allgemeinen EU-Regelungen zum Datenschutz, insbesondere der **DSGVO, unberührt** lasse (Art. 1 Abs. 3 EHDS). Diese Formel findet sich in vielen europäischen Rechtsakten. Die DSGVO enthält eine Vielzahl von Öffnungs- bzw. Spezifizierungsklauseln, die nicht nur den Mitgliedstaaten, sondern auch der EU die Möglichkeit einer Konkretisierung der DSGVO-Vorgaben eröffnet. Beim EHDS handelt es somit um eine bereichsspezifische Regelung zur Verarbeitung von Gesundheitsdaten, der eigenständige Rechtsgrundlagen zur Verarbeitung von personenbezogenen Daten enthält. Die allgemeinen Vorgaben der DSGVO behalten aber bei der Anwendung des EHDS volle Gültigkeit. Der EHDS beschränkt sich darauf, die DSGVO zu präzisieren und zu ergänzen (Art. 1 Abs. 2 lit. a EHDS).[50]

Die vom EHDS mit einer umfassenden Digitalisierung des Gesundheitswesens in der EU verfolgten Ziele lassen sich **nur schrittweise** realisieren (ErwGr 115 S. 2 EHDS). Er soll aber jetzt schon die nötigen Rechtsgrundlagen schaffen. Für die Umsetzung sind weitere nationale Normsetzungen nötig. Eine solche ist für Deutschland das GDNG.

Der EHDS schafft keine Rechtsgrundlagen für die erstmalige Erfassung elektronischer Gesundheitsdaten. Die Kompetenz hierfür bleibt bei den Mitgliedstaaten. Der EHDS definiert aber rechtliche Rahmenbedingungen für die Ersterfassung, um die Weiternutzung der Daten zu erleichtern. Für die Sekundärnutzung der Gesundheitsdaten schafft der EHDS dagegen **materielle Rechtsgrundlagen**, wie sie in Art. 6 Abs. 1 i. V. m. Art. 9 Abs. 2 DSGVO gefordert werden.[51] Insofern bleibt für die nationalen Gesetzgeber kein Regelungsspielraum. Die nationalen Regelungsmöglichkeiten beschränken sich darauf, die teilweise allgemeinen EHDS-Vorgaben zu konkretisieren und umzusetzen (ErwGr 52 S. 5 EHDS). Bzgl. der Sekundärnutzung

[49] ErwGr 6 EHDS.
[50] Kritisch Böning/Riechert in Augsberg/Düwell/Müller, S. 216.
[51] Art. 6 Abs. 1 lit. a, c, e u. f i. V. m. Art. 9 Abs. 2 lit. g-j DSGVO, ErwGr 52 EHDS; Bernhardt/Ruhmann/Weichert, DANA 1/2023, 19.

von Gesundheitsdaten wird damit auch Art. 9 Abs. 4 DSGVO, der es den Mitgliedstaaten freistellt, Bedingungen für die Verarbeitung von Gesundheitsdaten zu regeln, eingeschränkt.

Der EHDS beruft sich bei seiner DSGVO-Bezugnahme auf die Rechtsgrundlagen in **Art. 6 Abs. 1 lit. a, c, e u. f DSGVO** (ErwGr 53 S. 3 EHDS). Da die Sekundärnutzung gemäß dem EHDS nicht von einer Einwilligung (lit. a) abhängig gemacht wird,[52] kommen insofern nur die Buchstaben c (Erfüllung einer rechtlichen Verpflichtung) und e (Wahrnehmung einer Aufgabe im öffentlichen Interesse) in Betracht. Eine Berufung auf Buchstabe f, der eine Abwägung zwischen berechtigten Interessen privater Stellen mit den Schutzinteressen der Betroffeneninteressen vorsieht, kommt für die Sekundärnutzung nicht in Frage: Ein individuelles privates Interesse kann den mit der Sekundärnutzung verbundenen Grundrechtseingriff nicht legitimieren. Allenfalls in Ergänzung zu einem ohnehin bestehenden überwiegenden öffentlichen Interesse können berechtigte private Belange bei einer Sekundärnutzung gemäß dem Kapitel V des EHDS eine Rolle spielen.[53]

3.3 Data Governance Act

Der EHDS ist im Zusammenhang mit dem Data Governance Act (DGA) zu sehen, der seit dem 24.09.2023 Gültigkeit hat.[54] Gemäß Art. 1 Abs. 1 DGA regelt diese Verordnung u. a. „Bedingungen für die **Weiterverwendung von Daten** bestimmter Datenkategorien, die im Besitz öffentlicher Stellen sind, innerhalb der Union“ (lit. a) sowie einen Rahmen für die freiwillige Eintragung von Einrichtungen, die für altruistische Zwecke zur Verfügung gestellte Daten erheben und verarbeiten (lit. c). Der DGA schafft keine eigenen Rechtsgrundlagen für die Sekundärnutzung von Daten, sondern benennt rechtliche Rahmenbedingungen für die gemeinwohlorientierte Nutzung.[55]

Eine spezifische Form der „Weiterverwendung von Daten“ ist die im EHDS geregelte Sekundärnutzung von Gesundheitsdaten, welche bei öffentlichen Stellen vorliegen oder die sich die öffentlichen Zugangsstellen zugänglich machen. Zudem regelt der EHDS auch die Möglichkeit eines direkten Verfügbarmachens durch private „vertrauenswürdige Gesundheitsdateninhaber" (Art. 72 EHDS). Insofern bestehen zwischen DGA und EHDS Überschneidungen, wobei es sich beim DGA um das allgemeinere Gesetz zum EHDS handelt, soweit dessen Kapitel IV die **Weiterverwendung nur von Gesundheitsdaten** regelt. Im Anwendungsbereich des EHDS kommen auch die allgemeineren Normen des DGA zur Anwendung, soweit keine speziellen EHDS-Regeln bestehen.

[52] Böning/Riechert in Augsberg/Düwell/Müller, S. 225 f.
[53] Insofern unklar, aber missverständlich ErwGr 52 S. 3 EHDS, Bernhardt/Ruhmann/Weichert, DANA 1/2023, 22.
[54] Verordnung (EU) 2022/868 v. 30.05.2022, ABl. EU v. 03.06.2022, L 152/1.
[55] Bieresborn , Gesundheitsrecht.blog Nr. 33, 2023, 12.

3.4 Gesundheitsdatennutzungsgesetz, SGB V und andere

Das „Gesetz zur **verbesserten Nutzung von Gesundheitsdaten**“[56] regelt die Verwendung von Gesundheitsdaten zu „gemeinwohlorientierten Forschungszwecken und zur datenbasierten Weiterentwicklung des Gesundheitswesens als lernendes System“. Damit sollen die absehbaren Vorgaben des EHDS nationalgesetzlich umgesetzt werden. Das Gesetz besteht aus 6 Artikeln, insbesondere aus dem Gesundheitsdatennutzungsgesetz (GDNG, Art. 1) und Änderungen des fünften Buchs Sozialgesetzbuch (SGB V, Art. 3).

Gesetzessystematisch problematisch ist die Aufsplittung zwischen GDNG, das für sämtliche Gesundheitsdaten gelten soll, und den Sozialgesetzbüchern (SGB V, X, XI), die nur für Gesundheitsdaten aus der gesetzlichen Kranken- und Pflegeversicherung (GKV, GPV) Gültigkeit haben. Hintergrund dieser Aufsplittung ist die beschränkte **Gesetzgebungskompetenz** des Bundes im Gesundheitsbereich. Diese besteht für die „Sozialversicherung“ (Art. 74 Nr. 12 GG), also für die GKV und die GPV und die damit zusammenhängende Datenverarbeitung, nicht für die zu privat Versicherten. Selbst wenn die Bundeszuständigkeit „Förderung der wissenschaftlichen Forschung“ (Art. 74 Nr. 13 GG) extensiv ausgelegt wird[57], werden damit nicht sämtliche vorgesehenen Sekundärnutzungen abgedeckt. Die Länder sind u. a. für Bereiche wie die Universitätsklinika, weitgehend das Krankenhauswesen und für das öffentliche Gesundheitswesen zuständig (Art. 70 Abs. 1 GG). Soweit die im Gesundheitswesen tätigen Stellen nicht hoheitlich organisiert sind, kann auf die Gesetzgebungskompetenz des Bundes für das „Recht der Wirtschaft“ (Art. 74 Nr. 11 GG) zurückgegriffen werden. Der Kompetenzkonflikt hinsichtlich der Sekundärnutzung von Gesundheitsdaten im deutschen Recht wird mit dem Wirksamwerden des EHDS, also 2029 aufgelöst, da der EHDS eigene einheitliche Rechtsgrundlagen für die Sekundärnutzung schafft. Europarecht geht nationalen Gesetzen vor (Art. 288 AEUV).[58] Bis dahin können nur die deutschen Gesetze Eingriffe ins Recht auf informationelle Selbstbestimmung legitimieren, da auch die DSGVO in Bezug auf Gesundheitsdaten weitgehend auf das „Recht der Mitgliedstaaten“ verweist (Art. 9 Abs. 2 lit. b, g, h i, j DSGVO).[59] Ob die Regelungen des GDNG, die weitgehend die Vorgaben des Art. 9 Abs. 2 DSGVO wiederholen, ohne diese näher zu spezifizieren, den Anforderungen an die nationale Umsetzung von Öffnungsklauseln genügen, ist fraglich.[60]

Das zentrale operative Instrument zur Sekundärnutzung von Gesundheitsdaten in Deutschland gemäß dem GDNG und dem SGB V ist das **Forschungsdatenzentrum Gesundheit (FDZ)**. Das FDZ beschränkt sich hinsichtlich besonderer Datenarten (GKV-Abrechnungsdaten,

[56] G. v. 22.03.2024, BGBl. I Nr. 102, zuvor Gesetzentwurf der BReg v. 08.09.2023 BR-Drs. 434/23 = BT-Drs. 20/9046.
[57] Von Kielmansegg, VerwArch 2021, 132 ff.; Kuss/Langenheim CR 2024, 791 f.
[58] Weichert GuP 2023, 184; Weichert DANA 2/2024, 67.
[59] Kühling/Schildbach NZS 2020, 45.
[60] DSK GDNG-Stellungnahme, 5 f.; Kuss/Langenheim CR 2024, 793.

s. u. 5.2; ePA-Daten, s. u. 5.3) auf gesetzlich Versicherte (§§ 303a ff. SGB V) unter Einbeziehung der Daten aus der Pflege (§ 303b Abs. 1 SGB V). Diese unübersichtliche Regelungsstruktur ist gesetzessystematisch nicht überzeugend.

3.5 Gesundheitsdatennutzungsverordnung

Am 11.11.2024 veröffentlichte das Bundesministerium für Gesundheit (BMG) den Entwurf einer „Verordnung zur näheren Regelung von Verfahren nach dem Gesetz zur verbesserten Nutzung von Gesundheitsdaten“ (FDZGesV-E).[61] Dort ist in den §§ 1, 2 vorgesehen, dass die Pseudonymisierungsaufgaben bei der Datentransparenz gemäß den §§ 303a ff. SGB V vom Robert-Koch-Institut als Vertrauensstelle wahrgenommen wird, die Aufgaben des Forschungsdatenzentrums (FDZ) vom **Bundesinstitut für Arzneimittel und Medizinprodukte** (BfArM)(§ 2 Abs. 2 FDZGesV-E). Die Vorgängerregelung der FDZGesV ist die Datentransparenzverordnung (DaTraV), die mit der Gültigkeit der FDZGesV außer Kraft tritt (§ 22 Abs. 2 FDZGesV-E).

3.6 Anforderungen an die normativen Grundlagen

Der sich aus der Verfassung ergebende **Wesentlichkeitsgrundsatz**, wonach die wesentlichen Voraussetzungen für Grundrechtseingriffe und für den Grundrechtsschutz vom Parlament geregelt werden müssen, bestimmt, welche Fragestellungen der Sekundärnutzung einer exekutiven Rechtsverordnung überlassen werden können. Der Umstand, dass wesentliche Fragen des Zugangsverfahrens zu Gesundheitsdaten entweder gar nicht oder nur in einer Rechtsverordnung geregelt werden (§§ 17-20 FDZGesV-E), verletzt den Wesentlichkeitsgrundsatz.[62]

Aus dem Gebot der **Normenklarheit** resultiert die Pflicht, dass die Regeln für die Betroffenen verständlich sind und dass auf komplizierte Verweisungen verzichtet wird.[63] Während der EHDS sowohl hinsichtlich seiner Regelungsinhalte wie auch der Regelungszwecke nachvollziehbar und verständlich ist, verstoßen die nationalen Regelungen zur Sekundärnutzung von Gesundheitsdaten in mancher Hinsicht gegen das Bestimmtheitsgebot: Das Regelungsgeflecht von GDNG und den verstreuten Normen im SGB V ist selbst für den rechtskundigen Anwender und überhaupt nicht für den betroffenen Menschen durchschaubar. Die Verwendung von unbestimmten Rechtsbegriffen, ohne dass zu deren Anwendung prozessual begrenzende Regelungen bestehen, machen die Sekundärnutzung von Gesundheitsdaten (s. u. 5, 7, 9, 10) zu einer Rätselaufgabe respektive zu einem Glückspiel.

---

[61] BMG-Referentenentwurf v. 12.11.2024, https://www.bundesgesundheitsministerium.de/service/gesetze-und-verordnungen/detail/verordnung-zur-naeheren-regelung-von-verfahren-nach-dem-gesetz-zur-verbesserten-nutzung-von-gesundheitsdaten.html, kritisch dazu Weichert, Gesundheitsdatenforschung ja – aber bitte mit Datenschutz!, 19.11.2024, Kurzlink: https://heise.de/-10053620.

[62] DSK GDNG-Stellungnahme, 4.

[63] Petri in Simitis/Hornung/Spiecker, Art. 9Rn. 70 m. w. N.; Kühling/Schildbach NZS 2020, 46.

Die DSGVO macht allgemeine datenschutzrechtliche Vorgaben, die – soweit auf nationales Recht in Öffnungs- oder Spezifizierungsklauseln in der DSGVO verwiesen wird – konkretisiert werden müssen. Es genügt nicht, die Vorgaben der DSGVO im nationalen Recht zu wiederholen.[64] Derartige Verstöße gegen das **Normwiederholungsverbot** finden sich in mehreren nationalen Regelungen zur Sekundärnutzung von Gesundheitsdaten (z. B. § 4 Abs. 5 GDNG).[65]

4 Personenbezug

Bei der Datenverarbeitung gemäß dem EHDS und den nationalen Umsetzungsgesetzen handelt es sich weitgehend um die **Verarbeitung personenbezogener Daten**, also von „Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person“ beziehen (Art. 4 Nr. 1 DSGVO). Angesichts der Sensitivität dieser Daten sollen in Umsetzung des Grundsatzes der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) die Daten nur in pseudonymisierter oder gar anonymer Form zur Verfügung gestellt werden (ErwGr 72 EHDS).

Bei der Sekundärnutzung elektronischer Gesundheitsdaten soll durch Pseudonymisierung oder Anonymisierung die **Identifizierung der betroffenen Personen ausgeschlossen** werden (Art. 55 Abs. 3, 66 Abs. 3 EHDS; ErwGr 53 S. 6; 65 S. 11, 12; 72 S. S. 4-9 EHDS). Vorrang hat die Anonymisierung. Sollen Daten in pseudonymer Form genutzt werden, so muss im Antrag und in der Genehmigung der Sekundärnutzung begründet werden**,** „warum die Verarbeitung nicht mit anonymisierten Daten erfolgen kann“ (Art. 67 Abs. 2 lit. e, 68 Abs. 1 lit. c EHDS; § 303e Abs. 3 S. 4, Abs. 4 S. 1 SGB V).

4.1 Pseudonymisierung

Pseudonymisierung ist „die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne **Hinzuziehung zusätzlicher Informationen** nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“ (Art. 4 Nr. 5 DSGVO).

Die Pseudonymisierung dient der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO), also der zweckbezogenen Beschränkung der Datenverarbeitung auf das „notwendige Maß“. Es handelt

[64] EuGH 30.03.2023 – C-34/21 Rn. 57 ff., NJW 2023, 1641 ff.; Weichert in Däubler u. a.. Einleitung Rn. 35a; Hornung/Spiecker in Simitis/Hornung/Spiecker, Einleitung Rn. 267.
[65] DSK GDNG-Stellungnahme, 4.

sich zugleich um eine Maßnahme zur Erhöhung der Verarbeitungssicherheit (Art. 32 Abs. 1 lit. a DSGVO). Pseudonymisierte Daten sind **regelmäßig personenbeziehbar**.[66]

In § 303c, 303d SGB V ist detailliert ein Verfahren beschrieben, wie die Daten der gesetzlichen Kranken- und Pflegeversicherung unter Einbeziehung des Spitzenverbands der Krankenkassen und einer Vertrauensstelle pseudonymisiert und dem **Forschungsdatenzentrum** zur weiteren Verarbeitung bereitgestellt werden.[67] Weitere Details werden durch Rechtsverordnung des BMG festgelegt (§ 303a Abs. 4 Nr. 3 SGB V, § 4--12 FDZGesV-E). Als Vertrauensstellte wird in § 2 Abs. 1, S. 1, Abs. 3 FDZGesV-E das Robert Koch-Institut bestimmt, das diese Aufgabe „eigenständig und getrennt von seinen übrigen Aufgaben" wahrnehmen soll. Das Nähere soll „im Rahmen der Aufsicht", also durch das BMG geregelt werden.

Über das Pseudonym besteht die Möglichkeit verschiedene Datensätze aus unterschiedlichen Quellen einer Person zuzuordnen. So ist es auch praktisch möglich, wieder einen direkten Personenbezug herzustellen. Wegen der Vielzahl der vorhandenen Merkmalsangaben sind die im FDZ gespeicherten Einzeldatensätze einzigartig und bei Vorliegen von verfügbarem Zusatzwissen reidentifizierbar. Auf sie ist das **Datenschutzrecht** anwendbar.[68]

Eine **Bereitstellung pseudonymer Einzeldatensätze** ist nur erlaubt, wenn „der antragstellende Nutzungsberechtigte nachvollziehbar darlegt, dass die Nutzung pseudonymisierter Einzeldatensätze … erforderlich ist". Die Bereitstellung erfolgt „ohne Sichtbarmachung der Pseudonyme mit einer temporären Arbeitsnummer" (§ 303e Abs. 4 S. 1, 2 SGB V). Zulässig ist auf Pseudonym-Basis auch eine Verknüpfung der FDZ-Einzeldatensätze mit Daten aus gesetzlich geregelten medizinischen Registern (§ 303e Abs. 4a SGB V, § 4 Abs. 2 GDNG). Die Sekundärnutzung pseudonymer Gesundheitsdaten ist nur in einer sicheren Verarbeitungsumgebung erlaubt (§ 4 Abs. 5 GDNG, § 20 Abs. 2 S. 2 FDZGesV-E; s. u. 11.2).[69]

4.2 Anonymisierung

Art. 5 Abs. 3 lit. a ii DGA sieht vor, dass bei einer Weiterverwendung von Daten diese anonymisiert werden. Wirksam anonymisierte Daten unterliegen nicht mehr dem Datenschutzrecht und können aus persönlichkeitsrechtlicher Sicht **unbeschränkt weiterverarbeitet** werden:[70] „Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer

[66] Weichert in Däubler u. a, Art. 4 Rn. 71; Hansen in Simitis/Hornung/Spiecker, Art. 4 Nr. 5 Rn. 45; EDPB, Guidelines 01/2025 on Pseudonymisation v. 16.01.2025; VG Hamburg 28.07.2022 – 21 K 1802/21 Rn. 70 ff.
[67] Weichert MedR 2020, 540 f.
[68] Kühling/Schildbach NZS 2020, 43 f.
[69] Weichert in Dittrich/Dochow/Ippach, Kap. 15 Rn. 53-58.
[70] Weichert in Däubler u.a., Art. 4 Rn. 74; ErwGr26 S. 5, 6 DSGVO.

Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann“ (ErwGr 26 S. 5 DSGVO).

Die DSGVO enthält keine Definition des **Begriff Anonymisierung**. Anonymisierung wird allgemein verstanden als das Verändern personenbezogener Daten dergestalt, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.[71]

Dabei kommt es auf die Erkenntnisquellen an, die der speichernden Stelle als **Zusatzwissen** zur personenbezogenen Zuordnung direkt oder indirekt zur Verfügung stehen. Ob dieses Zusatzwissen legal oder unzulässig beschafft wird bzw. werden kann, ist unbeachtlich. „Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind“ (ErwGr 26 S. 3, 4 DSGVO).

Für die **Verfügbarkeit des Zusatzwissens** genügt eine theoretische Möglichkeit. Nicht beachtlich ist, dass diese Möglichkeit nicht in Anspruch genommen werden soll oder will. Eine absolute Anonymisierung ist bei hochkomplexen und umfangreichen Datensätzen oft praktisch nicht möglich. Wenn das Zusatzwissen nur unter einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft beschafft werden kann, genügt dies für die Anonymisierung. Hierbei ist ein objektiver Maßstab anzulegen; nicht beachtlich ist, wenn der Aufwand nur für die speichernde Stelle unverhältnismäßig ist; auch das Interesse der Stelle ist nicht erheblich.[72]

Der EHDS erkennt an, dass selbst bei Verwendung von dem Stand der Technik entsprechenden Anonymisierungsverfahren nach wie vor ein Risiko besteht, „dass die Fähigkeit zur Re-Identifizierung über die nach vernünftigem Ermessen wahrscheinlich eingesetzten Mittel hinaus verfügbar sein oder werden könnte“, etwa bei seltenen Krankheiten (ErwGr 92 S. 2, 3 EHDS). Bei Gesundheitsdaten hat sich immer wieder gezeigt, dass scheinbar anonymisierte Daten wieder einer konkreten Person zugeordnet werden

[71] BfDI, Anonymisierung personenbezogener Daten – Ein branchenübergreifender Praxisleitfaden für Industrieunternehmen, 2020, 3.
[72] Kühling/Klar in Kühling/Buchner, Art. 4 Nr. 1 Rn. 32; Kühling/Schildbach NZS 2020, 44 f.

konnten.[73] Keine wirksame Anonymisierung ist bei genetisch analysierbaren Gewebeproben sowie bei umfassenden Gendatensätzen möglich.[74] Das **Reidentifizierungsrisiko** ist von folgenden Aspekten abhängig: „dem Grad der Granularität, der Beschreibung der Merkmale der betroffenen Personen, der Anzahl der betroffenen Personen, beispielsweise wenn Daten in EHR, Krankheitsregistern, Biobanken oder personenbezogene Daten betroffen sind, bei denen das Spektrum der Identifizierungsmerkmale breiter ist, und der mögliche Kombination mit anderen Informationen, z. B. in sehr kleinen geografischen Gebieten, oder durch die technologische Entwicklung von Methoden, die zum Zeitpunkt der Anonymisierung nicht verfügbar waren“ (ErwGr 92 S. 5 EHDS). Denkbar ist, dass eine Reidentifizierung mit Hilfe von im Drittausland verfügbarem Zusatzwissen möglich ist (vgl. Art. 5 Abs. 13 DGA). Cybersicherheitsvorfälle sind ein schwer kalkulierbares Risiko, dass Reidentifizierungen möglich werden (vgl. ErwGr 93 S. 1 EHDS).

5 Art der Gesundheitsdaten

Elektronische Gesundheitsdaten, auf die der EHDS anwendbar ist (Art. 1 Abs. 1 EHDS), umfassen solche, die personenbezogen sind und solche, die keinen Personenbezug haben (Art. 2 Abs. 2 lit. c EHDS). Nicht erfasst werden Gesundheitsdaten, die nicht elektronisch bzw. digital verarbeitet werden. Die Terminologie der DSGVO gilt auch für den EHDS (Art. 2 Abs. 1 lit. a, Abs. 2 lit. a EHDS). Daher werden in Art. 4 Nr. 15 DSGVO Gesundheitsdaten und spezifisch in Art 4 Nr. 13 DSGVO genetische Daten definiert.[75]

Beispiele für Gesundheitsdaten sind „EHR (electronic health records), Daten zu Krankenversicherungsleistungen, Daten zur Abgabe von Arzneimitteln**,** Daten aus Krankheitsregistern oder Genomdaten, sowie Daten zu gesundheitsrelevanten Einflussfaktoren…, zum Beispiel Daten über den Konsum bestimmter Substanzen, den sozioökonomischen Status oder das Verhalten, und Daten über Umweltfaktoren wie etwa Verschmutzung, Strahlung, Umgang mit bestimmten chemischen Stoffen“ (ErwGr 56 S. 2 EHDS). Auf den ursprünglichen Zweck kommt es nicht an.

Als **Quellen** von Gesundheitsdaten erwähnt werden „Register für die Politikgestaltung, Register über Nebenwirkungen von Arzneimitteln oder Medizinprodukten“, Krebsregister sowie Register zu seltenen Krankheiten. Daten aus Wellness-Anwendungen kommen ebenso in Frage wie Daten über klinische Untersuchungen nach Abschluss der Untersuchung, die „vorzugsweise in einem strukturierten elektronischen Format“ bereit stehen sollten (Art. 51 Abs. 1 EHDS, ErwGr 56 S. 3 ff. EHDS). Der Katalog in Art. 51 Abs. 1 EHDS mit 17 Kategorien kann von den Nationalstaaten erweitert werden (Art. 51 Abs. 2 EHDS). Werden

[73] Beispiele dafür bei Wolfangel, Wenn alle erfahren, was einem fehlt, Die Zeit Nr. 13 v. 23.03.2023, 37.
[74] Weichert in Kühling-/Buchner, Art. 4 Nr. 13 Rn. 5.
[75] Böning/Riechert in Augsberg/Düwell/Müller, S. 221 f.

Gesundheitsdaten ergänzt, angereichert oder verbessert, so fallen auch diese Ergebnisse in den Anwendungsbereich des EHDS (ErwGr 57 EHDS).

Erfasst werden vom EHDS Gesundheitsdaten unabhängig von ihrer **Qualität und Nutzbarkeit**, wobei insofern eine Kennzeichnung angestrebt wird (ErwGr 85 EHDS). Dem Qualitätsziel entspricht der DSGVO-Grundsatz der Datenrichtigkeit (Art. 5 Abs. 1 lit. d DSGVO). Die Daten sollen den FAIR-Prinzipien (findable, accessible, interoperable, reusable) entsprechen (ErwGr 3 S. 2, ErwGr 85 S. 2 EHDS).

Das GDNG verweist bzgl. der erfassten Daten auf die DSGVO und umfasst auch Sozialdaten (§ 2 Nr. 1 GDNG).[76] In **spezifischen Regelungen** (§ 4 GDNG, §§ 303a ff, 363 SGB V) erfolgen Einschränkungen des jeweiligen Anwendungsbereichs.

Der **Umfang** der von der Sekundärnutzung betroffenen Daten ist äußerst weit, was auf Kritik stößt.[77] Werden von natürlichen Personen digitale Zwillinge mit Angaben zu biologischen, genetischen und psychologischen Eigenschaften, Merkmalen und Werten erstellt,[78] so sind diese Zwillinge Gegenstand der Regelungen zur Sekundärnutzung von Gesundheitsdaten. Die deutsche Datenschutzkonferenz wies darauf hin, dass die Einbeziehung der Daten aus Wellness-Anwendungen hohen Qualitätsanforderungen nicht genügt, aber eine hohe Eingriffsqualität hat. Die Aufnahme von gesundheitsrelevanten Faktoren, einschließlich sozialer, umweltbedingter und verhaltensbezogener Angaben zu Lebensstil, Wohlbefinden und Verhalten sei kritisch zu bewerten.[79]

5.1 Gesetzlich und Privatversicherte

Der EHDS **unterscheidet nicht** bei Gesundheitsdaten danach, ob sie im Rahmen der gesetzlichen Krankenversicherung (GKV) oder anders entstanden sind. Er zielt darauf ab, dass die Daten für die Sekundärnutzung „so vollständig wie möglich“ sind (ErwGr 53 S. 4 EHDS).

Im Forschungsdatenzentrum des BfArM (FDZ) werden bisher nur Gesundheitsdaten von **gesetzlich Kranken- bzw. Pflegeversicherten** verarbeitet. Dies ergibt sich aus der systematischen Stellung im SGB V (§§ 303a ff. SGB V) und ausdrücklich aus den §§ 303b Abs. 1 u.1a, 303e Abs. 1, 363 Abs. 1 SGB V. Das GDNG zielt dagegen auf die Bereitstellung von Gesundheitsdaten unabhängig vom Versichertenstatus der Betroffenen (§ 1 Abs. 1, 2 GDNG). Das GDNG geht den Regelungen des SGB vor (§ 1 Abs. 3 GDNG), es beschränkt sich aber nicht hierauf. Dessen ungeachtet nehmen informationelle Eingriffsregelungen im GDNG auf das SGB

[76] Böning/Riechert in Augsberg/Düwell/Müller, S. 222.
[77] Buchholtz/Schmalhorst/Brauneck MedR 2024, 473.
[78] Gruber/Zihlmann u. Kellmeyer in Augsberg/Düwell/Müller, S. 161 ff., 297 ff.
[79] DSK, EHDS-Stellungnahme v. 27.03.2023, 4.

V Bezug, etwa bzgl. der Verknüpfung von FDZ-Daten mit denen der Krebsregister (§ 4 GDNG), so dass faktisch Privatversicherte nicht oder nur begrenzt betroffen sind.

Ziel der Sekundärnutzung ist es, die gemeinwohlorientierte Forschung und die datenbasierte Weiterentwicklung des Gesundheitssystems zu ermöglichen und damit die Gesundheitsversorgung und Pflege zu verbessern (Art. 1 Abs. 1, 53 Abs. 1 EHDS, § 1 Abs. 1, 2 GDNG). Hierfür bedarf es auch der Gesundheitsdaten von nicht gesetzlich Versicherten. Dass diese von Nutzungsregelungen nach dem SGB V nicht erfasst sind, ist kompetenzrechtlich (s. o. 3.4) und historisch begründet (s.o. 3.1). Eine sachliche Rechtfertigung für diese **Ungleichbehandlung** besteht jedoch nicht. Hierin liegt ein Verstoß gegen Art. 3 GG.[80]

Die Ungleichbehandlung besteht für sämtliche im bzw. über das **SGB V geregelten Sekundärnutzungen**, also die Verarbeitung von GKV-Abrechnungsdaten (s. u. 5.2), die Datenzusammenführung von Krebsdaten (s. u. 5.4), die Daten in elektronischen Patientenakten (§ 363 SGB V) wie auch die der Teilnehmenden am Genom-Sequenzierungsprojekt (§ 64e SGB V, s. u. 5.5). Ein Verstoß gegen den Gleichheitsgrundsatz liegt nicht vor, soweit für die informationellen Eingriffe zusätzlich eine Betroffeneneinwilligung gefordert ist, also beim Genom-Modellprojekt. Wird der Eingriff vom Fehlen eines Widerspruchs abhängig gemacht, so bei der Nutzung der ePA-Daten, besteht für die Verhinderung des informationellen Eingriffs ein Handlungszwang der Betroffenen, so dass auch insofern eine nicht legitimierte Ungleichbehandlung gegenüber privat Versicherten erfolgt.

5.2 GKV-Abrechnungsdaten

Die pseudonyme Speicherung von Daten der **gesetzliche Kranken- und Pflegeversicherung** im FDZ ist in § 303 Abs. 1 SGB V geregelt und wird in § 3 FDZGesV-E präzisiert.[81] Erfasst sind zu jedem Betroffenen Alter (Geburtsjahr, Sterbedatum), Geschlecht und Wohnort (Postleitzahl), Angaben zum Versicherungsverhältnis (u. a. Kasse, Versichertentage, Status), die Kosten- und Leistungsdaten nach den §§ 295-295b , 300, 301, 301a, 302 SGB V u. § 105 SGB XI mit präzisen Angaben zu Leistungserbringern, Behandlungsart, Diagnosen und Befunde , Operationen, Kostenangaben, Arzneimitteln, Krankenhausbehandlungen, Pflegeleistungen.

Die GKV- bzw. GPV-Abrechnungsdaten haben nur eine **beschränkte Aussagekraft** über das tatsächliche Gesundheitsgeschehen in einer Gesellschaft, da die Kodierung der Abrechnungssachverhalte aus Abrechnungsgründen sich nicht zwingend an den realen Hintergründen ausrichtet. Die Aussage dieser Daten bezieht sich eher auf das ärztliche Abrechnungsverhalten und die Kosten des Gesundheitssystems. Falsche Zuordnungen zu den

[80] Weichert GuP 2023. 186.
[81] Die Verordnungsermächtigung findet sich in § 303a Abs. 4 Nr. 1 SGB V.

tatsächlich behandelten Krankheiten können im Fall einer Reidentifizierung dessen ungeachtet für die Betroffenen zu massiven Schäden und Beeinträchtigungen führen.[82]

5.3 Elektronische Patientenakte

Gemäß §§ 341, 342 SGB V wird von jedem gesetzlich Krankenversicherten bei Dienstleistern der Krankenkassen jeweils eine elektronische Patientenakte (ePA) geführt, soweit die betroffene Person dem nicht widersprochen hat. Sie dient der Bereitstellung von Informationen im Rahmen der Gesundheitsversorgung und enthält Angaben „insbesondere zu Befunden, Diagnosen, durchgeführten und geplanten Therapiemaßnahmen sowie zu Behandlungsberichten“ (§ 341 Abs. 1 S. 1, Abs. 2 SGB V). Die ePA wird gemäß § 363 SGB V pseudonymisiert an das FDZ übermittelt und dort für die in § 303e Abs. 2 SGB V genannten Zwecke zugänglich gemacht, soweit Versicherte dem nicht nach § 363 Abs. 5 SGB V widersprochen haben. Der **Widerspruch gegen die FDZ-Speicherung** erfolgt über ein Smartphone oder über eine Ombudsstelle der Krankenkasse und kann (nur) nach den gesetzlich genannten Zwecken differenziert werden (§ 8 FDZGesV-E, s. u. 12.4).

5.4 Krebsdaten

§ 4 GDNG sieht die Verknüpfung der pseudonymisierten FDZ-Daten mit den pseudonymisierten Daten der **klinischen Krebsregister** nach § 65c SGB V vor.[83] Es gehört zu den Aufgaben der Datenzugangs- und Koordinierungsstelle (DKS, s. u. 6.2 u. 10.1), Anträge zur Verknüpfung der FDZ-Daten mit denen der klinischen Krebsregister zu prüfen, zu genehmigen, die Verknüpfung vorzunehmen und die Daten Nutzungsberechtigten zur Verfügung zu stellen (§ 3 Abs. 2 Nr. 10, § 4 Abs. 2 S. 1 GDNG).

5.5 Gendaten

Gemäß Art. 2 Abs. 2 lit. a EHDS umfasst der Begriff der Gesundheitsdaten alle elektronisch verarbeiteten genetischen Daten i. S. v. Art. 4 Nr. 13 DSGVO, auch wenn sich diese nicht direkt auf Gesundheitsmerkmale beziehen (Art. 2 Abs. 1 lit. a EHDS). Art. 4 Nr. 13 DSGVO definiert genetische Daten als „personenbezogene Daten zu den **ererbten oder erworbenen genetischen Eigenschaften** einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden“.

Als nach Art. 51 Abs. 1 EHDS von Dateninhabern bereitzustellende Daten werden u. a. genannt: menschliche genetische, epigenomische und genomische Daten (lit. f), weitere molekulare Daten (lit.g) oder Daten aus Biobanken (lit. q). Die **umfassende Anwendbarkeit** ist, soweit es um den Schutz der Daten geht, sinnvoll, da eine Abgrenzung der Gendaten

[82] Erbst, Plötzlich dpressiv, Der Spiegel Nr. 6 v. 01.02.2025, 36 f.
[83] Zur Sensitivität von Krebsdaten VG Hamburg 28.07.2022 – 21 K 1802/21 Rn. 106.

hinsichtlich ihrer Gesundheitsrelevanz faktisch nicht möglich ist. Die konkrete Sekundärnutzung gemäß dem EHDS setzt aber voraus, dass ein in Art. 53 Abs. 1 EHDS genannter Gesundheitszweck verfolgt wird.

Die Bundesregierung hat in einer Protokollerklärung zum EHDS darauf hingewiesen, dass die Übertragung von genetischen Daten gemäß ihrem Verständnis **nur mit Einwilligung** möglich ist, dass es also nicht genügt, insofern ein Widerspruchsrecht einzuräumen.[84] Genetische Untersuchungen zu medizinischen Zwecken sind in Deutschland nur durch einen Arzt nach Aufklärung und Beratung und erteilter Einwilligung zulässig (§§ 7-10 GenDG). Die Mitteilung der Ergebnisse bedarf der ausdrücklichen und schriftlichen Einwilligung der betroffenen Person (§ 11 Abs. 3 GenDG).

Dies gilt auch für die Teilnahme an „**Modellvorhaben zur umfassenden Diagnostik und Therapiefindung mittels Genomsequenzierung** bei seltenen und bei onkologischen Erkrankungen“ (§ 64e SGB V). Hierfür werden nach einheitlichen Standards Gendaten von Leistungsträgern in pseudonymisierter Form in Genomrechenzentren gespeichert und über einen Plattformträger, das BfArM, ausgetauscht, um Nutzungsberechtigten folgende Auswertungszwecke zu ermöglichen: „1. Verbesserung der Versorgung durch umfassende Diagnostik und Therapiefindung mittels einer Genomsequenzierung, 2. Qualitätssicherung, 3. Evaluation des Modellvorhabens, 4. wissenschaftliche Forschung“ (§ 64e Abs. 1 S. 3 SGB V). Das BfArM erfüllt also insofern die Funktionen einer Zugangsstelle (s. u. 6.2), das Robert-Koch-Institut die der Vertrauensstelle im Rahmen des Pseudonymisierungsverfahrens (s. o. 4.1). Auch die Regelungen zur Datenbereitstellung und -nutzung entsprechen denen des GDNGs.

Angesichts der deutschen Protokollerklärung und der umfassenden gesetzlichen Einwilligungsanforderungen ist die Bereitstellung dieser Daten für Sekundärzwecke wohl hinreichend gesetzlich **legitimiert**. Die konkreten Sekundärnutzungen leiden aber an den generell in Deutschland hierfür geltenden verfahrensrechtlichen Defiziten (s. u. 6-10).

5.6 Psychisch-Krankendaten

Weder der EHDS noch die in Deutschland geltenden Regelungen zur Sekundärnutzung differenzieren danach, ob sich die Daten auf körperliche bzw. somatische oder auf seelische bzw. psychische Beeinträchtigungen bzw. Zustände beziehen. Zweifellos kann insofern keine klare Grenzlinie gezogen werden. Es ist aber offensichtlich, dass seelische Erkrankungen für die Betroffenen mit spezifischen Belastungen verbunden sind. Dies gilt zum einen, soweit den Daten nicht konsentierte Zwangsmaßnahmen gemäß den durch die Bundesländer erlassenen

[84] Council oft he European Union 30.01.2024 Summary Report Permanent Representatives Committee 16641/23 CRS CRP 42 v. 30.01.2024, S. 14, https://data.consilium.europa.eu/doc/document/ST-16048-2023-REV-1/en/pdf; die DSK, EHDS-Stellungnahme v. 27.03.2023, 4, forderte, Gendaten völlig aus der EHDS-Anwendung auszunehmen.

Maßregelvollzugs- und Psychischkrankengesetzen zugrunde liegen.[85] Unabhängig davon sind die Diskriminierungsrisiken in der Gesellschaft allgemein und im Arbeitsleben speziell für seelisch Kranke besonders hoch. Die Vertrauensbeziehung zwischen dem Heilberuf und dem Patienten muss bei psychologischer oder psychiatrischer Behandlung besonders intensiv sein. Daher im Rahmen der rechtlich geforderten **Verhältnismäßigkeitsprüfung** des Eingriffs bei einer Sekundärnutzung bei der Einbeziehung psychischer Krankheiten besonders hohe Maßstäbe anzusetzen.[86]

5.7 Daten zur sexuellen Orientierung

Wegen dem damit verbundenen Diskriminierungsrisiko sind „Daten zum Sexualleben oder der sexuellen Orientierung“ nach Art. 9 Abs. 1 DSGVO gesteigert schutzbedürftig. Diese betreffen in besonderer Weise die **persönliche Intimsphäre**.[87] Diese Datenkategorie wird zwar nicht umfassend vom EHDS und den nationalen Regelungen zur Sekundärnutzung erfasst, doch besteht eine Schnittmenge zu den Gesundheitsdaten, etwa wenn es sich um Geschlechtsumwandlungen, um sexuelle Störungen oder um sexualitätsbedinge seelische oder auch somatische Krankheiten handelt. Bei in den Intimbereich hineinreichenden Gesundheitsdaten sind die Regelungen zur Sekundärnutzung von Gesundheitsdaten grds. anwendbar. Eine Bereitstellung und eine Verarbeitung für diese Zwecke unterliegt einer gesteigerten Verhältnismäßigkeitsprüfung. Ein völliges Verarbeitungsverbot gilt, wenn der Kernbereich privater Lebensgestaltung betroffen ist.[88]

5.8 Aufbewahrungsdauer

Der EHDS enthält keine Regelungen zur **Löschung von Gesundheitsdaten**. Daher gelten grundsätzlich die Löschungsregelungen der DSGVO, die u. a. eine Ausnahme von der Löschpflicht für wissenschaftliche Forschungszwecke vorsehen (Art. 17 Abs. 3 lit. b DSGVO). Die Speichermindestdauer für ärztliche Dokumente beträgt 10 Jahre (§ 630 f Abs. 3 BGB, § 10 Abs. 3 MBOÄ). Im Hinblick auf Arzthaftungsrisiken wird teilweise eine darüber hinausgehende Speicherdauer von 30 Jahren empfohlen.[89] Spezifische Speicherpflichten gehen teilweise, z. B. gemäß der Röntgen- und der Strahlenschutzverordnung (§ 30 Jahre), darüber hinaus.[90] GKV-Daten sind bei den Sozialleistungsträgern i. d. R. spätestens nach 10 Jahren zu löschen (§ 304 SGB V).

---

[85] BVerfG 08.06.2021 – 2 BvR 1314 – 2 BvR 1314/18 Rn. 65, NStZ-RR 2021, 356.
[86] Art. 29-Datenschutzgruppe WP 217 v. 09.04.2014; S. 52; siehe diie Fälle von BVerfG 25.09.2023 – 1 BvR 2219/20, NVwZ 2024, 416; BVerfG 13.04.2022 – 2 BvR 447/22, WM 2022, 925.
[87] Petri in Simitis/Hornung/Spiecker, Art. 9 Rn. 23; Weichert in Däubler u.a., Art. 9 Rn. 43.
[88] BVerfG 03.03.2004 – 1 BvR 2378 u. 1 BvR 1984/99, NJW 2004, 999, 1002 m. w. N.
[89] So z. B. Rehborn in Prütting, Medizinrecht, 3. Aufl. 2014, § 10 MBOÄ Rn. 19.
[90] Siehe z. B. Kassenärztliche Vereinigung Niedersachsen, Ärztliche Aufbewahrungsfristen, https://www.kvn.de/internet_media/Mitglieder/Praxisf%C3%BChrung/Datenschutz/Datenschutzerkl%C3%A4rung_+%C3%84rztliche+Aufbewahrungsfristen-p-9724.pdf.

Die an das FDZ übermittelten Daten sollten gemäß dem DVG 2019 im FDZ 30 Jahre lang gespeichert werden. Diese Frist wurde 2024 auf 100 Jahre verlängert (§ 303d Abs. 4 SGB V). Ob diese lange Aufbewahrungsfrist verhältnismäßig ist, ist mit guten Gründen zu bezweifeln.[91] Art. 17 Abs. 3 lit. d DSGVO legitimiert eine Verarbeitung für Forschungszwecke nur, wenn eine kürzere Speicherfrist die Erreichung der Ziele unmöglich machen oder ernsthaft beeinträchtigen würde. Bei einer Vorratsdatenspeicherung für Forschungszwecke generell und einer Ungewissheit bzgl. der konkreten Sekundärnutzungszwecke ist es praktisch unmöglich, hinsichtlich der durch die DSGVO benannten Grenze eine klare Feststellung der Erforderlichkeit vorzunehmen. Eine gewisse Nützlichkeit für medizinische Forschung kann bei praktisch jedem qualifizierten medizinischen Einzelfalldatensatz zeitlich unbegrenzt angenommen werden, wenn damit ein Nachweis für einen tatsächlich bestehenden gesundheitlich relevanten Sachverhalt erfolgt. Für akute Gesundheitsfragestellungen verlieren Daten mit der Zeit ihre Relevanz. Es ist naheliegend, im Interesse der Wahrung des Verhältnismäßigkeitsgrundsatzes eine Abstufung bei der Speicherdauer vorzunehmen. Die aus Sicht der natürlichen betroffenen Person praktisch unbefristete **Speicherfrist von 100 Jahren** kann nur unter der Voraussetzung als verhältnismäßig angesehen werden, dass eine Reidentifizierung absolut ausgeschlossen wird.

6 Beteiligte

Der EHDS unterscheidet im Rahmen der Sekundärnutzung zwischen Dateninhabern, Zugangsstellen und Datennutzern. Dateninhaber und Zugangsstellen können als **Verantwortliche** (Art. 4 Nr. 7, Art. 24 ff. DSGVO) oder als **Auftragsverarbeiter** (Art. 4 Nr. 8, Art. 28 f. DSGVO) tätig sein, je nachdem, ob sie über die Zwecke der Verarbeitung (mit) bestimmen oder nicht. Datennutzer sind in jedem Fall Verantwortliche hinsichtlich der Nutzung. Wenn Dateninhaber oder Zugangsstelle über die Zwecke mitbestimmen (Art. 74 EHDS), was bei der Zugangsstelle regelmäßig der Fall ist (Ausnahme Art. 72 EHDS), sind sie „gemeinsam Verantwortliche“ (Art. 26 DSGVO, ErwGr 79 EHDS).

6.1 Gesundheitsdateninhaber

Gemäß Art. 51 EHDS haben Gesundheitsdateninhaber[92] Gesundheitsdaten für die Sekundärnutzung zur Verfügung zu stellen. Die äußerst weite **Definition** des Gesundheitsdateninhabers erfolgt in Art. 2 Abs. 2 Nr. f EHDS:

„jede natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle im Gesundheitswesen oder im Pflegesektor, soweit erforderlich einschließlich Erstattungsdiensten, sowie jede natürliche oder juristische Person, die Produkte oder Dienstleistungen für die Gesundheitsversorgung, das Gesundheitswesen oder den Pflegesektor

[91] DSK GDNG-Stellungnahme, 9.
[92] Zur Begrifflichkeit nach dem GDNG Kuss/Langenheim CR 2024, 793 f.

entwickeln, die Wellness-Anwendungen entwickelt oder herstellt, die Forschungstätigkeiten im Bereich des Gesundheitswesens oder des Pflegesektors durchführt, oder die als Mortalitätsregister fungiert, sowie jedes bzw. jede Organ, Einrichtung oder sonstig Stelle der Union, die entweder

i) nach geltendem Unionsrecht oder geltendem nationalen Recht in ihrer Eigenschaft als Verantwortlicher oder gemeinsam Verantwortlicher dazu berechtigt oder verpflichtet ist, personenbezogene elektronische Gesundheitsdaten für die Gesundheitsversorgung oder die Pflege oder für Zwecke der öffentlichen Gesundheit, der Erstattung, der Forschung, der Innovation, der Politikgestaltung, der amtlichen Statistik, der Patientensicherheit oder der Regulierung zu verarbeiten; oder

ii) *die Fähigkeit besitzt, nicht personenbezogene elektronische Gesundheitsdaten durch die Kontrolle der technischen Konzeption eines Produkts und der damit zusammenhängenden Dienste zur Verfügung zu stellen, auch durch die Erfassung von, die Bereitstellung von, die Einschränkung des Zugangs zu oder den Austausch von solchen Daten."*

Vertrauenswürdige Gesundheitsdateninhaber unterliegen erhöhten Datensicherheitsanforderungen an ihre „sicheren Verarbeitungsumgebungen" (Art. 72, 87 Abs. 1 EHDS, s. u. 11.1). Die Sekundärnutzung von deren Gesundheitsdaten muss nicht über die Zugangsstellen, sondern kann gemäß einem vereinfachten Verfahren direkt erfolgen. Den Zugangsstellen kommen in diesen Fällen nur administrative Aufgaben zu (Art. 72 Abs. 5, 6 EHDS).

Gerichte und andere **Einrichtungen des Justizwesens** fallen nicht unter die Definition des Begriffs „Gesundheitsdateninhaber" (ErwGr 63 S. S. 4, 6 EHDS).

Von der Bereitstellungspflicht **ausgenommen** sind natürliche Personen, sowie Kleinstunternehmen, also ein Unternehmen, „das weniger als 10 Personen beschäftigt und dessen Jahresumsatz bzw. Jahresbilanz 2 Mio. EUR nicht überschreitet" (Art. 50 Abs. 1 i. V. m. Art. 1 Abs. 3 Anhang Empfehlung 2003/361/EG).

Die Dateninhaber werden gemäß Art. 52 Abs. 2 EHDS verpflichtet, der Zugangsstelle die bei ihnen verfügbaren Gesundheitsdaten darzustellen und auch, welche Daten aus Gründen des Geheimschutzes nicht verfügbar gemacht werden. Im Fall einer Datengenehmigung haben die Dateninhaber der Zugangsstelle die einschlägigen **Gesundheitsdaten zur Verfügung zu stellen** (Art. 60 Abs. 1, 2 EHDS).

6.2 Zugangsstellen für Gesundheitsdaten

Der EHDS sieht für die Regulierung der Primärnutzung der Gesundheitsdaten je EU-Mitgliedstaat „mindestens eine Stelle für digitale Gesundheit" vor (Art. 19 ff. EHDS). Für die Sekundärnutzung werden von den Mitgliedsstaaten jeweils eine oder mehrere **Zugangsstellen für Gesundheitsdaten** benannt (Art. 55 Abs. 1 EHDS). Diese müssen mit personellen,

finanziellen und technischen Ressourcen, dem erforderlichen Fachwissen und der erforderlichen Infrastruktur ausgestattet werden (Art. 55 Abs. 2 EHDS).

Die Zugangsstellen sind für praktisch sämtliche behördlichen Aktivitäten im Zusammenhang mit der **konkreten Sekundärdatennutzung** zuständig: Behandlung der Zugangsanträge und Genehmigung sowie Umsetzung des Zugangs (Vermittlung, Anforderung und Bereitstellung der Daten, Kontrolle der Nutzung, Beratung und Bereitstellung von Informationen zur Sekundärnutzung, Art. 57 EHDS). Die konkrete prozedurale, organisatorische und technische Umsetzung des Zugangs ist in den Art. 66 ff. EHDS geregelt.[93]

§ 3 GDNG etabliert das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) als „zentrale **Datenzugangs- und Koordinierungsstelle** für Gesundheitsdaten“ (DKS) und überträgt diesem die Aufgaben der Zugangsstelle, also die Vermittlung und Bereitstellung der Daten, das Herstellen von Transparenz und die Beratung. Das BfArM soll organisatorisch und technisch Konzepte erstellen, und – als erste praktische Umsetzung – die Verknüpfung des FDZ mit den Krebsregistern voranzubringen (§ 3 Abs. 2 Nr. 9, 10 GDNG). Ein das BfArM beratender Arbeitskreis soll u. a. mit Vertretern der datenhaltenden Stellen, von Patientenorganisationen, von Leistungserbringern und aus der Gesundheitsforschung etabliert werden (§ 3 Abs. 4 GDNG).

Das BfArM ist der Betreiber des **Forschungsdatenzentrums** (FDZ), das vom BMG im Benehmen mit dem BMBF bestimmt wurde (§ 303a Abs. 1 S. 2 SGB V, § 2 Abs. 2 FDZGesV-E).[94]

6.3 Gesundheitsdatennutzer

Gesundheitsdatennutzer ist „eine natürliche oder juristische Person, einschließlich der Organe, Einrichtungen oder sonstigen Stellen der Union, die aufgrund einer Datengenehmigung, einer genehmigten Gesundheitsdatenanfrage oder einer **Zugangserlaubnis** eines befugten Teilnehmers der HealthData@EU rechtmäßig Zugang zu elektronischen Gesundheitsdaten für die Sekundärnutzung erhalten hat“ (Art. 2 Abs. 2 lit. u EHDS). Datennutzer kann jede natürliche oder juristische Person sein (s. u. 9.1).

7 Sekundärzwecke

Die Sekundärnutzung im **EHDS** dient vielen Zwecken, die „**dem allgemeinen Interesse der Gesellschaft** dienen“ (Art. 53 Abs. 1 EHDS, ErwGr 58 S. 1, 2 EHDS): öffentliche Gesundheit (u. a. bei schwerwiegenden, grenzüberschreitenden Gesundheitsgefahren), Überwachung, Qualitätssicherung[95], Patientensicherheit, lit. a), Politikgestaltung und Regulierungstätigkeit

[93] Bernhardt/Ruhmann/Weichert, DANA 1/2023, 19 f.
[94] Buchholtz/Schmalhorst/Brauneck MedR 2024, 475 f. stellen heraus, dass es sich beim FDZ als Zugangsstelle um einen Datentreuhänder handeln würde; ähnlich wohl DSK, EHDS-Stellungnahme v. 27.03.2023, 7.
[95] Zum Begriff und zur Abgrenzung zur Behandlung Schneider, Sekundärnutzung, S. 25 ff.

(lit. b), Statistik (lit. c), Bildungs- und Lehrtätigkeit im Gesundheits- und Pflegewesen (lit. d), wissenschaftliche Forschung (incl. Entwicklung und Innovation von Produkten und Dienstleistungen), Trainieren, Testen und Bewerten von Algorithmen, Medizinprodukten, In-Vitro-Diagnostika, KI-Systeme, digitale Gesundheitsanwendungen (lit. e), Verbesserung von Pflege und Gesundheitsversorgung und personalisierte Medizin (lit. f). Die im EHDS genannten Sekundärzwecke können sich gegenseitig überlappen. Die Weite und ungenügende Bestimmtheit der zulässigen Zwecke wird aus guten Gründen kritisiert (s.o. 3.6).[96]

Die vom potenziellen Datennutzer angestrebten Sekundärnutzungszwecke sind im Zugangsantrag präzise zu benennen (Art. 67 Abs. 2 lit. b EHDS). Die **Zugangsgenehmigung** beschränkt die Verarbeitung auf die darin genannten Zwecke (Art. 68 Abs. 1 lit. a, b, Abs. 10 lit. b EHDS).

Das **GDNG** nennt als übergeordnete Zwecke die gemeinwohlorientierte Forschung und die „datenbasierte Weiterentwicklung des Gesundheitssystems als lernendes System“: „Das Ziel der Nutzung von Gesundheitsdaten ist, eine sichere, bessere und qualitätsgesicherte Gesundheitsversorgung und Pflege zu gewährleisten, Forschung und Innovation zu fördern und das digitalisierte Gesundheitssystem auf Grundlage einer soliden Datenbasis weiterzuentwickeln“ (§ 1 Abs. 1 u. 2 GDNG).

Das GDNG macht keine generellen Vorgaben zu den Sekundärzwecken. Bzgl. der Verknüpfung des FDZ mit den **Krebsregistern** verweist es auf § 303e Abs. 2 u. 3 SGB V sowie bzgl. der Nutzung der Landeskrebsregister auf Landesrecht (§ 4 Abs. 2 Nr. 2 GDNG).

§ 303e Abs. 2 SGB V wurde mit der jüngsten Gesetzesnovelle inhaltlich so erweitert, dass er die wesentlichen in Art. 53 Abs. 1 EHDS aufgeführten Zwecke erfasst und teilweise präzisiert. In **§ 303 Abs. 2 S. 1 SGB V** werden die Zwecke genannt, die mit den im FDZ vorhandenen Daten verfolgt werden dürfen: Steuerungsaufgaben der Kollektivvertragspartner (Nr. 1) Qualitätssicherung und -verbesserung (Nr. 2) Leistungsplanung (Nr. 3), Gesundheitsforschung (Nr. 4), Politikgestaltung (Nr. 5), Wirksamkeitsanalysen von Versorgungsverträgen (Nr. 6) Gesundheitsberichterstattung und Statistik (Nr. 7) „Wahrnehmung gesetzlicher Aufgaben in den Bereichen öffentliche Gesundheit und Epidemiologie“ (Nr. 8), „Entwicklung, Weiterentwicklung und Überwachung der Sicherheit von Arzneimitteln, Medizinprodukten, Untersuchungs- und Behandlungsmethoden, Hilfs- und Heilmitteln, digitalen Gesundheits- und Pflegeanwendungen sowie Systemen der Künstlichen Intelligenz im Gesundheitswesen einschließlich des Trainings, der Validierung und des Testens dieser Systeme der Künstlichen

[96] Böning/Riechert in Augsberg/Düwell/Müller, S. 242; Buchholtz/Schmalhorst/Brauneck MedR 2024, 473.

Intelligenz“ (Nr. 9) sowie entsprechende Nutzenbewertung (Nr. 10). Der fast uferlos formulierte Katalog ist abschließend.[97]

Eine spezifische Zweckregelung enthält § 6 Abs. 2 S. 1 GDNG, wonach die datenverarbeitenden Gesundheitseinrichtungen, also die Dateninhaber i. S. d. EHDS, ihre Daten auch für folgende eigene Zwecke nutzen dürfen: Qualitätssicherung, Förderung der Patientensicherheit, Forschung, Statistik.[98] Eine derartige **Eigennutzung** ist im EHDS nicht explizit vorgesehen, aber auch nicht ausgeschlossen. Der EHDS fokussiert sich auf die Sekundärnutzung durch andere als die datenhaltende Stelle.

7.1 Gemeinwohl

Übergeordnete Anforderung an alle Sekundärzwecke ist, dass diese dem **Gemeinwohl** zu dienen haben.[99] Zwar ergibt sich dies nicht explizit aus Art. 53 EHDS. Doch stellen die Erwägungsgründe klar, dass die Sekundärnutzung dem „gesellschaftlichen Nutzen“ dienen und „aus wichtigen Gründen des öffentlichen Interesses“ erfolgen soll (ErwGr 53 S. 1, ErwGr 54 S. 7 EHDS), wobei der Betroffenenschutz in jedem Fall zu wahren ist (ErwGr 54 S. 11 EHDS). Es muss dem grundrechtlichen Erfordernis genügt werden, wonach Grundrechtseinschränkungen nur im Rahmen einer Interessenabwägung erfolgen dürfen. Der Wesensgehalt der Grundrechte und die Verhältnismäßigkeit müssen gewahrt bleiben (Art. 52 Abs. 1 GRCh).[100] Bei der Abwägung mit dem Gemeinwohl ist relevant, dass Daten mit einer besonders hohen Schutzbedürftigkeit von sehr vielen, ja möglicherweise von Millionen von Menschen verarbeitet werden.[101]

Die Sekundärnutzung von Gesundheitsdaten ist eine Weiterverwendung i. S. d. DGA, so dass der Art. 5 Abs. 2 DGA anwendbar ist: „Die Bedingungen für die Weiterverwendung müssen in Bezug auf die Datenkategorien, die Zwecke der Weiterverwendung und die Art der Daten, deren Weiterverwendung erlaubt wird, **nichtdiskriminierend, transparent, verhältnismäßig und objektiv gerechtfertigt** sein. Diese Bedingungen dürfen nicht der Behinderung des Wettbewerbs dienen.“

Konsequenterweise hat der **deutsche Gesetzgeber** in § 1 Abs. 2 u. 3 GDNG das Gemeinwohlerfordernis prominent fixiert. Dass dem genügt wird, muss bei jeder Sekundärnutzung gesondert festgestellt werden. Gesetzestechnisch unglücklich ist, dass bei der Anwendung des § 303e Abs. 2 SGB V keine direkte Verweisung auf die im GDNG

[97] Hierzu Kühling/Schildbach NZS 2020, 47: Weichert DANA 2/2024, 69; kritisch Böning/Riechert in Augsberg/Düwell/Müller, S. 243; zur ethischen Rechtfertigung der Sekundärnutzung Niggemeier in Augsberg/Düwell/Müller, S. 286 ff m. w. N.
[98] Dazu Kuss/Langenheim CR 2024, 791 ff.
[99] DSK, EHDS-Stellungnahme v. 27.03.2023, 6.
[100] Bieresborn, Gesundheitsrecht.blog Nr. 33, 2023, 5.
[101] Bretthauer/Spiecker gen. Döhmann JZ 2020, 996.

enthaltene Gemeinwohlklausel erfolgt. Sie gilt in allen diesen Fällen, da das GDNG den Regelungen des SGB V vorgeht.

Nicht minder unglücklich ist, dass für die Umsetzung der Gemeinwohlklausel keinerlei Kriterien bestehen.[102] Dies gilt vor allem für die Grenzziehung zwischen privaten, insbesondere **kommerziellen Zwecken** und Gemeinwohlzwecken. Es tut dem Gemeinwohl keinen Abbruch, wenn mit einer Datennutzung auch private eigennützige Ziele mitverfolgt werden, etwa dass ein Forschungsvorhaben eine Promotion oder Habilitation zum Ziel hat.[103] Um aber die Privilegierungen einer Sekundärnutzung in Anspruch nehmen zu können, genügt es nicht, dass auch das Gemeinwohl im Fokus steht, vielmehr muss dort der Schwerpunkt liegen. Hierzu ein Beispiel aus der Pharmaforschung: Es genügt für die Zulassung einer Sekundärforschung nicht, dass neue wirksame Arzneimittel entwickelt werden sollen. Vielmehr muss auch gewährleistet sein, dass die Ergebnisse der Forschung der Allgemeinheit zugutekommen und verfügbar gemacht werden, so dass auch Konkurrenten auf dem Markt davon profitieren und dass die Gesundheitsversorgung mit dem neuen Arzneimittel zu angemessenen Kosten ermöglicht wird. Dies setzt eine Klarstellung im Rahmen der Genehmigung, Transparenz der Sekundärnutzung sowie eine wirksame regulierende Aufsicht hinsichtlich der Ergebnisverwendung voraus.[104]

7.2 Forschungszwecke

Wissenschaftliche Forschung ist durch Art. 5 Abs. 3 S. 1 GG und Art. 13 S. 1 GRCh grundrechtlich geschützt. Sie ist deshalb gemäß dem EHDS und der DSGVO europarechtlich privilegiert: „Der **Begriff der Zwecke wissenschaftlicher Forschung** sollte weit ausgelegt werden und die technologische Entwicklung und die Demonstration, die Grundlagenforschung, die angewandte Forschung und privat finanzierte Forschung einschließen. Zu den Tätigkeiten im Zusammenhang mit der wissenschaftlichen Forschung zählen Innovationstätigkeiten, wie etwa das Trainieren von KI-Algorithmen, die in der Gesundheitsversorgung oder in der Pflege natürlicher Personen eingesetzt werden könnten, sowie die Bewertung und Weiterentwicklung bestehender Algorithmen und Produkte für solche Zwecke“ (ErwGr 61. S. 8, 9 EHDS). Im Ergebnis knüpft der Forschungsbegriff an den grundrechtlichen Schutz der Forschungsfreiheit an (s. o. 2.5).

Während der Begriff der Forschung verfassungsrechtlich geprägt ist (s. o. 2.5) und im EHDS zumindest umschrieben wird, verzichten die **nationalen Regelungen** zur Sekundärnutzung vollständig auf eine Konkretisierung. Dies führt zur Unsicherheit bei der Rechtsanwendung.[105]

[102] Weichert DANA 2/2024, 69.
[103] Kühling/Schildbach NZS 2020, 48.
[104] Ähnlich Böning/Riechert in Augsberg/Düwell/Müller, S. 248.
[105] Weichert GuP 2023, 187.

Europäisches und nationales Gesetzes- wie auch Verfassungsrecht müssen ineinandergreifen, wobei das Verfassungsrecht bestimmend ist.

Der Forschungszweck steht bei der Legitimation der Zweckänderungen der Gesundheitsdaten im EHDS im Vordergrund. Dies entspricht der **Privilegierung in der DSGVO**, wonach wissenschaftliche Forschungszwecke oder statistische Zwecke (bei Beachtung von Art. 89 Abs. 1 DSGVO) mit den ursprünglichen Zwecken nicht als unvereinbar gelten sollen (Art. 5 Abs. 1 lit. b DSGVO). Die Pflicht zur Datenlöschung soll nicht bestehen, wenn gemäß Art. 89 Abs. 1 DSGVO verarbeitete Daten „die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt“ (Art. 17 Abs. 3 lit. d DSGVO). Zwar haben Betroffene ein Recht auf Widerspruch gegen eine derartige Datenverarbeitung, aber nur, soweit diese nicht „zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich“ ist (Art. 21 Abs. 6 DSGVO). Unter den gleichen Voraussetzungen können auch auf gesetzlicher Grundlage Ausnahmen von den Rechten auf Auskunft, Berichtigung und Einschränkung der Verarbeitung vorgesehen werden (Art. 89 Abs. 2 i. V. m. Art. 15, 16, 18 u. 21 DSGVO).

Um derart privilegiert zu sein, bedarf es für die Datenverarbeitung der Sicherstellung von Garantien, „dass **technische und organisatorische Maßnahmen** bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird, was durch eine wirksame Pseudonymisierung erreicht werden kann“ (Art. 89 Abs. 1 DSGVO).

Die Privilegierung der Forschung in der DSGVO wird durch die Erwähnung als zulässiger Sekundärzweck in Art. 53 Abs. 1 lit. e EHDS bekräftigt und für den „Bereich des Gesundheitswesens oder Pflegesektors“ konkretisiert. Dabei nimmt diese Privilegierung nicht nur Bezug auf Art. 9 Abs. 2 lit. j DSGVO zur Gesundheitsforschung, sondern auch zu den in diesem Absatz aufgeführten Erlaubnistatbeständen in lit. h und i, wo generell auf die **Versorgung im Gesundheitsbereich sowie auf die dortige Sicherheit und Qualität** verwiesen wird.

Die DSGVO-Privilegierung wissenschaftlicher Forschung wird in § 27 **BDSG** weitgehend wortgleich übernommen und bzgl. der technisch-organisatorischen Maßnahmen konkretisiert. Die Daten sind zu anonymisieren, sobald dies der Zweck erlaubt, „es sei denn, berechtigte Interessen der betroffenen Person stehen dem entgegen“ (§ 27 Abs. 3 S. 1 BDSG). In § 22 Abs. 2 BDSG werden weitere mögliche Maßnahmen aufgeführt: Protokollierung (Nr. 2), Sensibilisierung der Beteiligten (Nr. 3), Benennung eines Datenschutzbeauftragten (Nr. 4), Zugangs-/Zugriffsbeschränkung (Nr. 5), Datenverschlüsselung (Nr. 7), spezifische Verfahrensregelungen (Nr. 10).

7.3 Sekundärzwecke generell

Mit dem EHDS wird die in der DSGVO privilegierte Gesundheits- und Pflegeforschung näher präzisiert. Unklar bleibt, wie die anderen in Art. 53 Abs. 1 EHDS genannten zulässigen

Sekundärzwecke mit Blick auf die DSGVO zu bewerten sind. So handelt es sich z. B. bei der „Sicherstellung hoher Qualitäts- und Sicherheitsstandards“, der „Politikgestaltung und Regulierungstätigkeiten“ oder den „Bildungs- oder Lehrtätigkeiten“ nicht um „Forschung“, zumeist auch nicht, wenn es um „die Verbesserung der Pflege, der Optimierung der Behandlung und der Gesundheitsversorgung“ geht (lit. a, b, d u. f). Alle Alternativen lassen sich aber den in Art. 9 Abs. 2 lit. h u. i DSGVO genannten Zwecken zuordnen. Es ist erklärtermaßen nicht Ziel des EHDS, die DSGVO aufzuweichen (ErwGr 5, 8, 9 EHDS). Daraus ergibt sich die Notwendigkeit, bei der Auslegung des EHDS den **von der DSGVO gesetzten Rahmen** zu beachten (ErwGr 52 S. 8-10 EHDS).

Dabei kann aber nicht immer auf die spezifischen Privilegierungsregelungen der DSGVO zur Forschung zurückgegriffen werden.[106] Angesichts des Schutzzweckes sowohl der DSGVO wie auch des EHDS für die Betroffenen sind die Schutzregelungen für die von Forschung Betroffenen in der DSGVO als Mindeststandard bzgl. der darüber hinausgehenden EHDS-Zwecke anzuwenden. Da diese EHDS-Zwecke jedoch nicht denselben verfassungsrechtichen Schutz wie den der Forschungsfreiheit genießen, ist im Rahmen der Grundrechtsabwägung ein **höherer Betroffenenschutz** nötig. Dies betrifft insbesondere das Datenminimierungsgebot; Außerhalb der Forschung ist daher immer mit anonymisierten Daten zu arbeiten. Zudem sind für sämtliche EHDS-Sekundärzwecke weitere Schutzvorkehrungen nötig (Verfahrenssicherungen, Transparenzanforderungen, sichere Verarbeitungsumgebung, s. u. 8-11).

7.4 Verbotene Zwecke

Gemäß Art. 54 EHDS sind Sekundärnutzungen auf die in der Genehmigung (Art. 68 EHDS) gestatteten Zwecke beschränkt. Zwecke sind ausgeschlossen, die natürlichen **Personen schaden** bzw. schaden können (lit. a, d). Ein Kriterium dafür ist, dass die Nutzung Tätigkeiten dient, „die im Widerspruch zu im nationalen Recht festgelegten Bestimmungen stehen“ (lit. e). Ein Nutzungsverbot gilt auch für Entscheidungen in Bezug auf Arbeits- oder Verbraucherverträge und „Werbe- und Vermarktungstätigkeiten“ (lit. b, c). Als untersagte Nutzungsbeispiele werden genannt: „um Versicherungsbeiträge zu erhöhen, Handlungen durchzuführen, die möglicherweise zum Nachteil der natürlichen Personen in Verbindung mit Beschäftigung, Rente oder Bankwesen wären, einschließlich bei der Vergabe von Hypotheken, Produkte oder Behandlungen zu bewerben, Entscheidungen im Einzelfall zu automatisieren, natürliche Personen zu re-identifizieren oder schädliche Produkte zu entwickeln“ (ErwGr 62 S. 1, 2 EHDS). Verboten ist zudem das Entwickeln von illegalen Drogen, alkoholischen Getränken, Tabak- und Nikotinerzeugnissen, Waffen und Suchtprodukten (lit. d).

Diese Vorgaben werden in § 303e Abs. 3a SGB V umgesetzt, wobei präzisierend erwähnt wird, dass Nutzungen verboten sind, bei denen ein unangemessenes **Risikos für die öffentliche**

[106] Mit Bezug zu den GDNG-Zwecken Böning/Riechert in Augsberg/Düwell/Müller, S. 237.

Sicherheit und Ordnung oder für den Schutz personenbezogener Daten entsteht (S. 1 Nr. 1). Abzulehnen ist ein Antrag zudem bei dem begründeten Verdacht einer genehmigungswidrigen Nutzung (S. 1 Nr. 2) oder wenn mehrere Zugangsanträge die Arbeitsfähigkeit des FDZ gefährden (S. 1 Nr. 3).

Die aufgeführten Kriterien lassen sich ohne Not mit dem Ziel in Einklang bringen, dass eine Sekundärnutzung nur zu Gemeinwohlzwecken erlaubt sein soll. Der **Ausschluss von vertragsgestaltenden Zwecken** stellt klar, dass eine Privatnützigkeit nicht im Vordergrund stehen darf.

7.5 Verhältnismäßige Zwecke

Die zentrale rechtliche Problematik des EHDS besteht darin, dass grundsätzlich alle Gesundheitsdaten, denen eine hohe individuelle Sensitivität zukommt und ein hohes Diskriminierungsrisiko innewohnt, für einen umfangreichen Strauß von Zwecken zur Verfügung gestellt wird, deren Einschränkung zunächst nur darin besteht, dass diese eine Gesundheitsrelevanz haben müssen. Während die Ausschlussgründe relativ bestimmt formuliert sind, sind die zulässigen Sekundärzwecke stark interpretationsfähig. Dies hat zur Folge, dass zwischen klar erlaubten und verbotenen Zwecken ein **großer Interpretationsspielraum** besteht, soweit nicht weitere Eingrenzungen der erlaubten Zwecke erfolgen.

Der EHDS verzichtet auf Einschränkungen hinsichtlich einer evtl. gesteigerten Erforderlichkeit und begnügt sich damit, **Angemessenheit** zu verlangen (Art. 66 Abs. 1 EHDS) und auf das Datenminimierungsbot und auf eine projektbezogene Vertraulichkeit hinzuweisen. Um verhältnismäßig zu sein, müssen die Verwendungszwecke präzisiert werden auf solche, mit denen prospektiv ein erheblicher Gewinn für die öffentliche Gesundheit einhergeht.[107] Dies schließt einen individuellen Gesundheitsgewinn nicht aus, da das Wohl eines Einzelnen auch im öffentlichen Interesse liegen kann (s. o. 7.1).

Angesichts der Offenheit und Breite der zugelassenen Zwecke kommt es für die Bereitstellung in jedem Fall auf eine **Abwägung** an, wozu im EHDS nur wenige Anhaltspunkte bereitgestellt werden. Selbst wenn man die in Art. 9 Abs. 2 lit. h, i und j DSGVO aufgeführten Zwecke mitliest (ErwGr 52 EHDS), bleibt man hinsichtlich der Abwägung bei der Genehmigung der Zugangsberechtigung im Ungewissen. Wenig hilfreich ist dabei, dass viele Zwecke keinen oder zumindest nur einen sehr indirekten Grundrechts- oder Verfassungsbezug haben.[108] Außerhalb des Forschungsbereichs ist nicht erkennbar, weshalb für die verfolgten Zwecke ein Personenbezug nötig sein könnte. Insofern genügen als Datengrundlage anonymisierte Daten.

[107] Ähnlich Cimina, vom EDPS zit. in Krempl, EU-Gesundheitsdatenraum: Patientendaten-Freigabe für Sekundärdaten umkämpft, www.heise.de 30.11.2022, Kurzlink: https://heise.de/-7361089.
[108] Bernhardt/Ruhmann/Weichert DANA 1/2023, 22 f.

Der Umstand, dass dies nicht explizit geregelt ist, führt zu einem Mangel hinreichender Bestimmtheit (s. o. 3.6).[109]

Ein direkter Grundrechtsbezug der Sekundärnutzung besteht, wenn für diese die **Forschungsfreiheit** einschlägig ist. Die grundrechtlich begründete Privilegierung der Forschung in der DSGVO findet im EHDS keine explizite konkretisierende Entsprechung. Die vorgesehenen Zwecke werden materiell- und prozessrechtlich gleich geregelt. Dies steht im Widerspruch zu dem Grundsatz, dass wesentlich Unterschiedliches unterschiedlich zu behandeln ist. Dogmatisch einzig möglich, aber wenig befriedigend ist insofern ein Rückgriff auf das Datenminimierungsgebot (Art. 5 Abs. 1 lit. c DSGVO) und die Annahme, dass für den Fall, dass kein Forschungsprivileg eingreift, keine pseudonyme, sondern nur eine anonyme Verarbeitung „angemessen und erheblich“ ist.

8 Nutzungsgeheimnis

Der EHDS macht keine Aussagen zur Datennutzung für **Sicherheitszwecke**: „Mit dieser Verordnung wird keine Ermächtigung zur Sekundärnutzung von Gesundheitsdaten zum Zwecke der Strafverfolgung geschaffen. Die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung durch die zuständigen Behörden sollte nicht zu den Zwecken der Sekundärnutzung gehören, die unter die vorliegende Verordnung fallen. … Darüber hinaus bleiben die Befugnisse der zuständigen Behörden, für die Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten gemäß den gesetzlichen Bestimmungen elektronische Gesundheitsdaten zu erhalten, von dieser Verordnung unberührt“ (ErwGr63 S. 1, 2 EHDS; Art. 1 Abs. 9 lit. b EHDS).

Der EHDS regelt verbindlich bestimmte Zweckänderungen. Bzgl. der Zweckverfolgung außerhalb der EU können die Mitgliedstaaten verlangen „dass personenbezogene elektronische Gesundheitsdaten ausschließlich in der Union zur Wahrnehmung der in der vorliegenden Verordnung vorgesehenen Aufgaben gespeichert und verarbeitet werden dürfen, es sei denn, es gilt ein gemäß Artikel 45 der Verordnung (EU) 2016/679 gefasster Angemessenheitsbeschluss“ (ErwGr 93 S. 4 EHDS). Die **Regelungsbefugnis der Mitgliedstaaten** wird also auf außerhalb des EHDS liegende Zwecke begrenzt. Die Übermittlungsregelungen der DSGVO sind dabei zu beachten.

8.1 Forschungsgeheimnis

Die Nutzung von Gesundheitsdaten für Sicherheits- und insbesondere für **Strafverfolgungszwecke** wird vom EHDS nicht erfasst. Hierzu bestehende nationale Regelungen müssen insofern Art. 10 DSRL-JI beachten, der für besondere Datenkategorien

[109] Weichert MedR 2020, 544.

einen weiten europarechtlichen Rahmen lässt: Die Verarbeitung von Gesundheitsdaten für Zwecke der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten ist erlaubt, „wenn sie unbedingt erforderlich ist und vorbehaltlich geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person erfolgt“, und wenn sie u. a. nach dem Recht des Mitgliedsstaats zugelassen wird (lit. a).

Es obliegt also dem deutschen Gesetzgeber, insofern Regeln festzulegen, die mit nationalem Verfassungsrecht vereinbar sind. Dies hat er in Bezug auf Gesundheitsdaten generell unterlassen. Detailliert geregelt ist in Bezug auf die Strafverfolgung nur der Schutz des **Patientengeheimnisses** mit einem Zeugnisverweigerungsrecht der Heilberufler und einem entsprechenden Beschlagnahmeverbot (§§ 53 Nr. 3, 53a, 97Abs. 2 StPO). Dieser Schutz erstreckt sich jedoch nicht auf sekundär gemäß dem EHDS genutzte Gesundheitsdaten. Die sekundär Nutzungsberechtigten sind weder Gehilfen noch Mitwirkende des primär Daten verarbeitenden Heilberuflers. Dies gilt übrigens auch schon für die Krankenkassen und deren Dienstleister z. B. hinsichtlich der Speicherung der ePA.[110]

Wird die Zugangsmöglichkeit zu Patientengeheimnissen über den EHDS und das GDNG auf einen größeren Kreis von Datenempfängern erweitert, ohne dass diese einen Zeugnis- und Beschlagnahmeschutz haben, so eröffnen sich insbesondere für Strafverfolgungsbehörden neue Zugänge zu Patientengeheimnissen. Die digitale Aufbereitung der Gesundheitsdaten sind für die Strafverfolgungsorgane ein verlockendes Angebot, zumal die Datenkategorien der Dateninhaber leicht zugänglich und die Datennutzung transparent sein sollen (vgl. Art. 57 Abs. 1 lit. j EHDS). Die **Reidentifizierung der pseudonymisierten Daten** ist für Strafverfolger ein geringes Problem, zumal deren bestehende Ermittlungsmöglichkeiten zum Erlangen des für die Reidentifizierung nötigen Zusatzwissens umfassend sind (§§ 94 ff., 160 ff. StPO).

Eine entsprechende **Erweiterung der hoheitlichen Erkenntnismöglichkeiten** ist nicht Intention der umfassenden Zulassung der Sekundärnutzung von Gesundheitsdaten. Vielmehr stünde sie im Widerspruch zum Zweck des Patientengeheimnisses, sich umfassend einem Berufshelfer anvertrauen zu können (s. o. 2.1).[111]

Es war deshalb naheliegend, dass die Datenschutzbehörden im Rahmen eines erleichterten Zugangs zu gesundheitlichen Forschungsdaten ein **gesetzliches Forschungsgeheimnis** als strafprozessualen Schutz fordern. Dies nütze zugleich dem Vertrauen in die Forschung.[112] Konsequenterweise waren ein Zeugnisverweigerungsrecht und ein Beschlagnahmeverbot in

[110] Wissenschaftliche Dienste Deutscher Bundestag, Strafprozessuale Einzelfragen zur Beschlagnahme einer elektronischen Patientenakte, WD 7 - 3000 - 021/23, 23.03.2023, S. 7 ff. m. w. N., a. A. BReg. BT-Drucks. 15/1525 v. 08.09.2003, S. 167 f. u. BT-Drs. 20/5779 v. 24.03.2023, 66 f.
[111] Siehe zur ähnlichen Problematik der ePA Wissenschaftliche Dienste Deutscher Bundestag, Strafprozessuale Einzelfragen zur Beschlagnahme einer elektronischen Patientenakte, 23.03.2023, Az WD 7 – 3000 – 021/23.
[112] DSK, EHDS-Stellungnahme v. 27.03.2023, 4, 11; DSK, Petersberger Erklärung v. 24.11.2022; so auch schon 67. DSK v. 25./26.03.2004, Einführung eines Forschungsgeheimnisses für medizinische Daten; Dazu auch Pöttgen, Medizinische Forschung, S. 230 f. m. w. N.

einem ersten Referentenentwurf des BMG zum GDNG (von Juni 2023) vorgesehen, was aber im weiteren Gesetzgebungsverfahren wieder gestrichen wurde.[113]

Eine solche Vertraulichkeitssicherung ist zum Schutz der durch die Forschungsfreiheit gewährleisteten wissenschaftlichen Methode **verfassungsrechtlich geboten**.[114] Durch eine gesetzliche Regelung würde die bisher bestehende Rechtsunsicherheit beseitigt und das Vertrauen der Betroffenen sowie der datenhaltenden Stellen in die Wahrung der Vertraulichkeit bei der wissenschaftlichen Nutzung gestärkt. Ohne eine solche Regelung des Forschungsgeheimnisses besteht das Risiko, dass der Forschung die dringend für wissenschaftliche Vorhaben benötigten Gesundheitsdaten z B. wegen Betroffenenwidersprüchen vorenthalten bleiben.[115]

8.2 Weiterentwicklung zu einem Sekundärnutzungsgeheimnis

Stand bisher bei der Diskussion um die Sekundärnutzung von Gesundheitsdaten die grundrechtlich geschützte Forschung im Vordergrund, so eröffnen der EHDS, das GDNG und dem folgend das SGB V einen erheblich weiteren Nutzungsbereich. Die Sekundärzwecke sind möglicherweise weder verfassungsrechtlich noch gemäß der DSGVO privilegiert. Bei der Sekundärnutzung wird normativ kein Unterschied zwischen nicht privilegierten EHDS-Nutzungen und Forschungszwecken vorgenommen (s. o. 7.2). Ziel muss es bleiben, das **Patientengeheimnis bei der Sekundärnutzung** generell abzusichern (s. o. 2.1). Angesichts der Offenheit der potenziellen Datennutzer und des Umstands, dass diese bei der Nutzung durch Pseudonymisierung nur unzureichend geschützte Patientengeheimnisse erlangen können, ist es nötig, das heute schon verfassungsrechtlich abzuleitende Forschungsgeheimnis auf ein Sekundärnutzungsgeheimnis zu erweitern. Ein solcher Bedarf besteht nur dann nicht, wenn vor einer Übermittlung der Gesundheitsdaten an die Datennutzenden eine wirksame Anonymisierung erfolgt (s. o. 4.2). Dies ist aber, da die nach den im EHDS und im GDNG geregelten und ermöglichten Datennutzungen nicht zwischen Forschung und anderen Zwecken unterscheiden, bisher nicht gewährleistet.

9 Datenzugangsberechtigte

Der EHDS nennt die Datenzugangsberechtigten **Gesundheitsdatennutzer** (s. o. 6.3). Da diese personell oder institutionell nicht weiter eingegrenzt werden, kann dies jede natürliche oder juristische Person sein.[116] Diese ist befugt, eine Gesundheitsdatenanfrage gemäß Art. 69 EHDS zu stellen. Gemäß Art. 68 Abs. 1 lit. d EHDS muss ein Antragsteller für die

[113] Weichert GuP 2023, 186.
[114] BVerfG 25.09.2023 – 1 BvR 2219/20 Rn. 13-15; NVwZ 2024, 416.
[115] Weichert, Rahmenbedingungen, S. 114 m. w. N.
[116] Das EU-Parlament wollte den Zugriff beschränken auf Personen," die nachweisliche eine berufliche Verbindung zum Gesundheitswesen, zum Bereich der öffentlichen Gesundheit oder zur medizinischen Forschung hat", vgl. Böning/Riechert in Augsberg/Düwell/Müller, S. 241 f.

Zugangsgenehmigung Folgendes nachweisen: Er „ist im Hinblick auf die Zweckbestimmungen der Datennutzung qualifiziert und verfügt über angemessenes Fachwissen, einschließlich beruflicher Qualifikationen in den Bereichen Gesundheitsversorgung, Pflege, öffentliche Gesundheit oder Forschung, im Einklang mit ethischen Standards und den geltenden Rechts- und Verwaltungsvorschriften."

9.1 Das Jedermannrecht nach nationalem Recht

Das GDNG enthält keine Regelung, in der nähere Voraussetzungen für die Datenzugangsberechtigten bzw. für die Antragsteller aufgeführt werden. Bzgl. des Zugangs zu Krebsregister- und FDZ-Daten wird auf das SGB V verwiesen. In § 303e Abs. 1 S. 2 SGB V heißt es für jede Form der FDZ-Nutzung: „Nutzungsberechtigt sind **natürliche und juristische Personen** im Anwendungsbereich der Verordnung (EU) 2016/679, soweit diese zur Verarbeitung zur Verarbeitung der Daten berechtigt sind." Damit erfolgte gegenüber dem seit 2019 geltenden Kreis der potenziellen Datennutzer eine umfassende Ausweitung. Zunächst wurden nur ausdrücklich aufgeführte Stellen berechtigt: Krankenkassen, GKV-, Ärzte- und Patienten-Verbände, öffentliche Stellen. Forschungseinrichtungen mussten Hochschulen sein oder „sonstige Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung, sofern die Daten wissenschaftlichen Vorhaben dienen" (§ 303e Abs. 1 Nr. 8 SGB V-alt). Der im Gesetzgebungsverfahren von der FDP kommende Vorschlag, auch pharmazeutischen Unternehmen, Herstellern von Medizinprodukten, von Diagnostikleistungen und von digitalen Gesundheitsleistungen den Datenzugang zu ermöglichen, war mit Enthaltung der AfD von den anderen Fraktionen noch abgelehnt worden.[117]

Solche Einschränkungen sind nicht mehr vorgesehen. Nötig ist nur noch, dass der Datennutzer darlegt, dass er die erbetenen Daten für die von ihm genannten in Abs. 2 erlaubten Zwecke benötigt.[118] Unterliegt der Datennutzer nicht dem § 203 StGB, so ist er nach dem Verpflichtungsgesetz zur Geheimhaltung zu verpflichten (§ 303e Abs. 4 S. 3 SGB V). Die Verpflichtung auf das **Berufsgeheimnis** ist keine wirksame Qualifizierungsanforderung an Nutzungsberechtigte. § 203 StGB hat zudem in der strafrechtlichen Praxis bisher kaum eine Bedeutung. Ermittlungen sind selten, trotz einer Vielzahl von tatsächlichen Verstößen; über Sanktionierungen nach § 203 StGB ist nichts bekannt (s.u. 14.1).[119]

9.2 Anforderungen an Nutzungsberechtigte

Das Fehlen jeglichen Nachweiserfordernisses von **Zuverlässigkeit und Qualifikation** hinsichtlich der Datennutzer ist ein erheblicher gesetzlicher Mangel, zumal das FDZ-Zugangsrecht so formuliert ist, dass eine Nutzungsberechtigung besteht, wenn den formalen Anforderungen an den Nutzungsantrag entsprochen wird. Es fehlt an Garantien, wie im EHDS

[117] BT-Drs. 19/14867, v. 06.11.2019, S. 82 f., 84 ff., 98; Weichert MedR 2020, 541.
[118] Kritisch Weichert DANA 2/2024, 69.
[119] Weichert MedR 2020, 545 m. w. N.

vorgesehen, mit denen die schwerwiegenden informationellen Eingriffe durch die pseudonyme Nutzung von Gesundheitsdaten, verhältnismäßig sein können.[120] Bisher gibt es für den Nachweis der Zuverlässigkeit und Qualifikation zum Umgang mit sensitiven Daten keine Regelungen. Diese können darin bestehen, dass der Erwerb eines entsprechenden Zertifikats gefordert wird, das eine Ausbildung und bestimmte Prüfungen voraussetzt.

10 Zugangsverfahren

Das Verfahren der Zugangsgenehmigung zu Gesundheitsdaten für Sekundärzwecke und die Art der Zugangsgewährung sind von zentraler Bedeutung für die Sicherung des Datenschutzes.[121] Hierfür sind auf **nationaler Ebene** Standardverfahren vorzusehen (ErwGr 73 S. 1 EHDS). Die Kommission kann zwecks Harmonisierung der national zu regelnden Verfahren Vorlagen bereitstellen (ErwGr 73 S. 12 EHDS). Zentral im Zugangsverfahren sind die „Zugangsstellen für Gesundheitsdaten“, wovon in jedem EU-Mitgliedstaat mindestens eine einzurichten ist (ErwGr 64 S. S. 1, 2 EHDS, s. o. 6.2).

10.1 Zugangsstelle für Gesundheitsdaten

Art. 55 EHDS regelt die rechtlichen Rahmenbedingungen für die Einrichtung der „Zugangsstellen für Gesundheitsdaten“ (künftig nur Zugangsstellen). Sie setzen die in den Art. 57-59 EHDS geregelten Aufgaben und Pflichten um. Die Zugangsstellen sind mit den nötigen personellen, finanziellen und technischen Ressourcen sowie den erforderlichen Räumlichkeiten und der erforderlichen (technischen und organisatorischen) Infrastruktur auszustatten (Art. 55 Abs. 2 S. 1 EHDS).

In § 3 Abs. 1 GDNG ist die Einrichtung einer **zentralen Datenzugangs- und Koordinierungsstelle** (DKS) beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) vorgesehen. Gemäß der Gesetzesbegründung ist dies nur ein „erster Schritt“ für den Aufbau einer Infrastruktur.[122] Da aber schon jetzt Zugangsbefugnisse zu sensitiven Daten gewährt werden, müssen zu Beginn des Aufbaus der Zugangsinfrastruktur grundrechtssichernde Verfahren bestehen. Hierzu gehört es, dass die Verfahren unabhängig und transparent durchgeführt werden. Die Regelung zur Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten (DKS) in § 3 GDNG zielt erkennbar darauf ab, eine Zugangsstelle i. S. v. Art. 55 EHDS zu schaffen.

Bzgl. der Verknüpfung der FDZ-Daten mit den **Krebsregisterdaten** hat die DKS die Aufgaben der Entgegennahme, Prüfung und Genehmigung der Datenzugangsanträge (§ 4 Abs. 2-4

[120] Weichert GuP 2023, 187
[121] Generell dazu BVerfG 15.12.1983 – 2 BvR 209/83, 419, 422; a. A. wohl in Bezug auf das FDZ Kühling/Schildbach NZS 2020, 48.
[122] BT-Drs. 20/9046 (= BR-Drs. 434/23), S. 48; kritisch Weichert DANA 2/2024, 68.

GDNG) sowie der technischen Verknüpfung und Übermittlung an die Datennutzenden in einer „sicheren Verarbeitungsumgebung“ (§ 4 Abs. 5-8 GDNG).

In den §§ 303a SGB V wird nicht der Begriff der Zugangsstelle verwendet. Inhaltlich werden die entsprechenden Aufgaben umfassend vom **Forschungsdatenzentrum** (§ 303a Abs. 1 SGB V) wahrgenommen: 1. Aufbereitung und 2. Qualitätssicherung der angelieferten Daten, Prüfung der Zugangsanträge, Bereitstellung für die Nutzungsberechtigten (§ 303d Abs. 1 SGB V).

10.2 Unabhängigkeit der Genehmigungsstelle

Der EHDS formuliert Anforderungen an die Zugangsstelle: „Zugangsstellen für Gesundheitsdaten sollten ihre Entscheidungen über den Zugang zu elektronischen Daten für die Sekundärnutzung unbeeinflusst treffen und jegliche Interessenkonflikte vermeiden. Daher 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. Die Unabhängigkeit von Zugangsstellen für Gesundheitsdaten sollte jedoch nicht bedeuten, dass sie keinen Kontroll- oder Überwachungsmechanismen in Bezug auf ihre finanziellen Ausgaben unterliegen oder einer gerichtlichen Überprüfung unterzogen werden können“ (ErwGr 64 S. 7-9 EHDS).

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, beispielsweise durch Pseudonymisierung und Anonymisierung von Datensätzen, sowie die Bereitstellung von Daten in sicheren Verarbeitungsumgebungen“. Interessenkonflikte sind mit den einschlägigen Interessenträgern zu vermeiden (Art. 55 Abs. 4 EHDS).

Der EHDS enthält zwar keine Aussagen zur **Interessenunabhängigkeit der Mitarbeitenden**, sondern nur in Bezug auf indirekt involvierte Mitarbeitende. Dies lässt sich aber auf die Mitarbeitenden der Zugangsstelle übertragen: „Die Mitarbeiter der Marktüberwachungsbehörden sollten weder direkt noch indirekt in wirtschaftliche, finanzielle oder persönliche Interessenkonflikte geraten, die als Beeinträchtigung ihrer Unabhängigkeit angesehen werden könnten, und sie sollten sich insbesondere nicht in einer Situation befinden, die die Unparteilichkeit ihres beruflichen Verhaltens direkt oder indirekt beeinträchtigen könnte. Die Mitgliedstaaten sollten das Auswahlverfahren für Marktüberwachungsbehörden festlegen und veröffentlichen. Sie sollten sicherstellen, dass das Verfahren transparent ist und Interessenkonflikte verhindert werden“ (ErwGr48 EHDS).

Zur Unabhängigkeit der Zugangsstelle enthält das GDNG keine Festlegungen. § 303 Abs. 2 SGB V regelt, dass das Forschungsdatenzentrum (ebenso wie die Vertrauensstelle zur Pseudonymisierung) „räumlich, organisatorisch und personell eigenständig zu führen“ ist. Dem BMG kommt die **Rechtsaufsicht** zu.

Weitergehende Regelungen kann das BMG per **Rechtsverordnung** treffen (§ 3 Abs. 3 GDNG, § 303a Abs. 4 SGB V). Nach § 3 Abs. 3 GDNG können im Benehmen mit dem BMBF, aber ohne Zustimmung des Bundesrats, die Regeln zur Unabhängigkeit der Aufgabenwahrnehmung geändert werden. In § 2 Abs. 3 S. 1, 3 FDZGesV-E ist vorgesehen, dass das BfArM seine Aufgabe des FDZ eigenständig und getrennt von seinen übrigen Aufgaben wahrnimmt, wobei das Nähere „im Rahmen der Aufsicht“ geregelt werden soll.

Die Unabhängigkeit der Zugangsstelle, insbesondere im Rahmen des **Zugangsgenehmigungs-Verfahrens,** ist im deutschen Recht bisher nicht gewährleistet.[123] 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.[124] 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 starke Einbindung in das vom BMG weisungsabhängige BfArM und die Befugnis des BMG, durch Verordnung Vorgaben zur Unabhängigkeit zu machen, widersprechen dem Erfordernis der Unabhängigkeit.

Dies gilt insbesondere für die Zugangsgewährung zu Daten für die Forschung (Art. 53 Abs. 1 lit. e EHDS). Im Interesse der **Unabhängigkeit wissenschaftlicher Forschung** müssen Anträge auf Datenzugang ausschließlich nach fachlichen Kriterien beschieden werden. Politische 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.[125]

Um solchen Interessen etwas entgegensetzen zu können, bedarf es neben der Weisungsfreiheit einer hohen Qualifikation der Entscheidenden sowie der prozeduralen **Einbindung pluraler Interessen**. Eine rein beratende Einbindung von weiteren Interessenträger, wie sie in § 3 Abs. 4 GDNG vorgesehen ist, genügt nicht.[126] Es bedarf einer

[123] DSK GDNG-Stellungnahme, 4 f.
[124] 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.
[125] Bernhardt/Ruhmann/Weichert DANA 1/2023, 23.
[126] Weichert GuP 2023, 187; vgl. Böning/Riechert in Augsberg/Düwell/Müller, S. 247..

Verselbständigung der Zugangsstelle, einer Sicherstellung der Weisungsfreiheit der Zugangsstelle sowie einer Einbindung qualifizierter Interessen (s. u. 10.3). Die Kontrolle der unabhängigen Zugangsstelle durch eine umfassende Transparenz gegenüber Betroffenen sowie gegenüber der Öffentlichkeit muss gewährleistet werden (s. u. 10.6).

Problematisch ist nicht nur die weitgehende Bestimmungsmacht des BMG hinsichtlich der Sekundärnutzungsbefugnis von Gesundheitsdaten. Kritisch zu hinterfragen sind auch die sehr weitgehenden Befugnisse der exekutiven EU-Kommission zum **Erlass von delegierten Rechtsakten** (Art. 78 Abs. 5, 97 EHDS). Dem EU-Parlament wird insofern ein zeitlich begrenztes Veto-Recht zugestanden. Angesichts der Detailliertheit des EHDS und der möglichen parlamentarischen Kontrolle wahren aber diese exekutiven Einflussmöglichkeiten den verfassungsrechtlichen Rahmen (s. o. 3.6).[127]

10.3 Qualifikation der Genehmigungsstelle

Hinsichtlich der Leitung der Zugangsstellen erklärt der EHDS: „Die Mitglieder der Governance- und Entscheidungsstellen der Zugangsstellen für Gesundheitsdaten und deren Personal sollten über die erforderlichen Qualifikationen, Erfahrungen und Kompetenzen verfügen“ (ErwGr 64 S. 12 EHDS). Für die gesamte Zugangsstelle wird das erforderliche Fachwissen eingefordert (Art. 55 Abs. 2 lit. b EHDS).

Um ein qualifiziertes Vorgehen zu gewährleisten, verlangt Art. 55 Abs. 4 EHDS, dass die Zugangsstelle „aktiv mit Vertretern der einschlägigen **Interessenträger zusammen(arbeitet)**, insbesondere mit Patientenvertretern, Gesundheitsdateninhaber und der Gesundheitsdatennutzer“.

§ 3 Abs. 4 GDNG sieht vor, dass bei der DKS im Benehmen mit dem BMG und dem BMBF ein „**Arbeitskreis zur Gesundheitsdatennutzung**“ eingerichtet wird (s. o. 10.2). In diesem sollen datenhaltende Stellen, Patientenorganisationen, Leistungserbringer und Gesundheitsforschende vertreten sein. Einbezogen werden können „Vertreter weiterer betroffener Gruppen und Institutionen. Vertreter von Datenschutzaufsichtsbehörden werden nicht erwähnt. Dem Arbeitskreis kommt eine beratende Funktion zu bzgl. „der Ausgestaltung, Weiterentwicklung und Evaluation der Aufgabenstellen“ (S. 3). In § 303d Abs. 2 SGB V ist ebenso vorgesehen, dass das FDZ einen beratenden Arbeitskreis „zur Sekundärnutzung von Versorgungsdaten“ einrichtet. Zu beteiligen sind dabei „die maßgeblichen Verbände der Selbstverwaltung, Institutionen der Gesundheits- und Versorgungsforschung, Bundes- und Landesbehörden sowie Patientenorganisationen auf Bundesebene“.

[127] Zur Fassung des Kommissionsentwurfes Bernhardt/Ruhmann/Weichert, DANA 1/2023, 23 f.

Das BMG wird gemäß § 3 Abs. 3 Nr. 1 u. 2 GDNG befugt, in einer **Rechtsverordnung** das Nähere zu regeln zur „Einrichtung und Organisation“ der DKS sowie zu „den Einzelheiten der Wahrnehmung der Aufgaben“.

Damit ist nicht hinreichend gewährleistet, dass bei der Zugangsstelle die nötige **Qualifikation und Fachkompetenz** besteht und im Rahmen der Aufgabenwahrnehmung zum Einsatz kommt.

10.4 Antrag auf Sekundärnutzung

Die Antragstellung auf Sekundärnutzung von Gesundheitsdaten wird im Detail auf **nationaler Ebene** geregelt (ErwGr 73 S. 2-9 EHDS). Für eine Genehmigung des Datenzugangs nennt Art. 68 Abs. 1 EHDS Kriterien, die im Antragsverfahren erfüllt sein müssen. Dies sind die Darstellung des Zwecks (lit. a) und der benötigten Daten (lit. b), bei Nutzung von Pseudonymdaten die Begründung, weshalb anonyme Daten nicht ausreichen (lit. c), die Wahrung der Vertraulichkeit durch technisch-organisatorische Maßnahmen (lit. e) und die Erfüllung ethischer Anforderungen (lit. f).

Für die Antragstellung auf Verknüpfung der FDZ-Daten mit denen der **klinischen Krebsregister** verlangt § 4 Abs. 2 Nr. 3 GDNG den Nachweis, dass „schutzwürdige Interessen der betroffenen Person nicht beeinträchtigt werden oder das öffentliche Interesse an der Forschung das Geheimhaltungsinteresse der betroffenen Person überwiegt und das spezifische Reidentifikationsrisiko in Bezug auf die beantragten Daten bewertet und unter angemessener Wahrung des angestrebten wissenschaftlichen Nutzens durch geeignete Maßnahmen minimiert worden ist“. § 303d Abs. 1 Nr. 2 SGB V erteilt dem FDZ die Aufgabe, die Anträge auf Nutzung der dort gespeicherten Daten zu prüfen.

§ 303a Abs. 4 Nr. 4 SGB V berechtigt das BMG, das Nähere zur Aufgabenwahrnehmung und Antragsbearbeitung per **Rechtsverordnung** zu regeln. So sieht § 17 Abs. 1 FDZGesV-E vor, was der Antrag auf Sekundärnutzung von FDZ-Daten (GKV-Abrechnungsdaten, ePA-Daten) enthalten muss: Identität des Antragstellers (Nr. 1), Nutzungszweck (Nr. 2), methodischer Ansatz der Datenverarbeitung (Nr. 3), Datenarten (Nr. 4), beteiligte Personen (Nr. 5), Zusammenführung mit anderen Datenbeständen (Nr. 6). Der Antragstellende muss sich zudem verpflichten, keine Reidentifizierung der pseudonymisierten Daten vorzunehmen, „geeignete technische und organisatorische Maßnahmen umzusetzen“ und keine Zweckänderung vorzunehmen (§ 17 Abs. 2 FDZGesV-E). Nach Erfassung und Prüfung des Antrags entscheidet das FDZ über den Antrag (§ 18 FDZGesV-E).

10.5 Datenschutzkonzept

Für die Erteilung einer Zugangsgenehmigung bedarf es des Nachweises ausreichender **technischer und organisatorischer Maßnahmen**, „um den Missbrauch der elektronischen Gesundheitsdaten zu verhindern und die Rechte und Interessen des

Gesundheitsdateninhabers und der betroffenen natürlichen Personen zu schützen“ (Art. 68 Abs. 1 lit. e EHDS). Es geht also darum, sich im Genehmigungsverfahren zu vergewissern, dass bei der Datennutzung das Datenschutzrecht beachtet wird. Der Detailliertheitsgrad bzgl. der Umsetzung des Datenschutzes wird – abgesehen von der Pflicht zur Begründung der Notwendigkeit pseudonymer Einzeldatensätze (lit. c) – nicht vorgegeben. Die Präzisierung obliegt daher nationalen Regelungen.

Präzisierungen können im Hinblick auf die Datenminimierung, die Umsetzung eines Rechte- und Rollenkonzeptes, die Protokollierung und deren Kontrolle, sowie zu Prozessabläufen und zu Datenflüssen erfolgen.[128]

Die nationalen Regelungen vertrauen fast ausschließlich darauf, dass über eine „sichere Verarbeitungsumgebung“ der technische Datenschutz gewahrt wird (s. u. 11.1). Insofern ist das Sozialrecht präziser. In § 75 SGB X werden für die Beforschung von Sozialdaten und insbesondere von besonderen Kategorien von Daten gemäß Art. 9 Abs. 1 DSGVO konkretere Anforderungen gestellt. Gemäß § 75 Abs. 1 S. 4 SGB X ist in jedem Fall ein Datenschutzkonzept vorzulegen. Darin muss der Forschende darlegen, dass er sich qualifizierte Überlegungen zu einer datenschutzgerechten Projektdurchführung gemacht hat. Gemäß § 75 Abs. 4a S. 3 SGB X kann bei übergreifenden Forschungsprojekten „die Vorlage einer **unabhängigen Begutachtung des Datenschutzkonzeptes**“ verlangt werden. Entsprechende Anforderungen sind auch hinsichtlich der Sekundärnutzung von Gesundheitsdaten nötig.[129] So ist vorstellbar, dass die Sekundärnutzung von der Vorlage eines Datenschutz-Zertifikats (vgl. Art. 42 DSGVO) abhängig gemacht wird.[130]

10.6 Transparenz des Verfahrens und der Datennutzung

„Die Zugangsstellen für Gesundheitsdaten sollten sicherstellen, dass die **Sekundärnutzung transparent** ist, indem sie die Öffentlichkeit über die erteilten Datengenehmigungen und ihre Begründungen, die Maßnahmen zum Schutz der Rechte natürlicher Personen, die Art und Weise, wie natürliche Personen ihre Rechte in Bezug auf die Sekundärnutzung ausüben können, und die Ergebnisse der Sekundärnutzung informieren, auch durch Links zu wissenschaftlichen Veröffentlichungen. Diese Informationen über die Ergebnisse der Sekundärnutzung sollten gegebenenfalls auch eine vom Gesundheitsdatennutzer bereitzustellende Zusammenfassung für Laien umfassen. Diese Transparenzpflichten ergänzen die in Artikel 14 der Verordnung (EU) 2016/679 festgelegten Verpflichtungen.“ Damit soll gewährleistet werden, dass „natürliche Personen verstehen können, ob ihre Daten gemäß Datengenehmigungen für die Sekundärnutzung bereitgestellt werden“ (ErwGr 66).

[128] Kuss/Langenheim CR 2024, 795.
[129] Vgl. VG Hamburg 28.07.2022 – 21 K 1802/21 Rn. 119.
[130] Böning/Riechert in Augsberg/Düwell/Müller, S. 246.

Die **Datennutzer informieren die Zugangsstellen** spätestens 18 Monate nach Abschluss der Verarbeitung der pseudonymisierten Gesundheitsdaten „über die Resultate oder Ergebnisse der Sekundärnutzung und unterstützen sie dabei, diese Informationen auch auf den Websites der Zugangsstellen für Gesundheitsdaten zu veröffentlichen“. Sie müssen hierbei die Datenquellen angeben (Art. 61 Abs. 4 UAbs. 1 u. 4 EHDS). Darüberhinausgehend trifft sie auch eine eigene Pflicht zur Veröffentlichung ihrer Ergebnisse innerhalb von 18 Monaten nach Beendigung der Sekundärdatennutzung (Art. 61 Abs. 4 UAbs. 1 EHDS).

Die Zugangsstellen sind verpflichtet, ein öffentliches Informationssystem zu unterhalten, um den Verpflichtungen nach Art. 58 EHDS nachzukommen (Art. 57 Abs. 1 lit. f EHDS). Art. 58 Abs. 1 EHDS begründet eine Vielzahl von Informationspflichten der Zugangsstelle gegenüber natürlichen Personen. Diese beziehen sich bzgl. der **konkreten Datennutzungen** auf die Rechtsgrundlage (lit. a), die technischen und organisatorischen Schutzmaßnahmen (lit. b), die Datennutzer, die Datensätze, die Einzelheiten zu den Zwecken der Datengenehmigung (lit. f) und auf die Ergebnisse oder Resultate der Datennutzungs-Projekte (lit. g).

Die Zugangsstellen **informieren allgemein** darüber hinaus gemäß Art. 58 EHDS über ihre eigenen Kontaktdaten (Abs. 1 lit. e EHDS), über die Rechte der Betroffenen hinsichtlich der Sekundärnutzung (Abs. 1 lit. c) und des Datenschutzes (Abs. 1 lit. d) sowie über ein bestehendes Widerspruchsrecht gegen die Sekundärnutzung (Abs. 2).

Hinsichtlich der **Transparenz des Genehmigungsverfahrens** bestehen mehrere nationale Regelungen: So stellt die DKS einen öffentlichen Metadaten-Katalog über die im Gesundheitswesen vorhandenen und zugänglichen Gesundheitsdaten und über die jeweiligen Datenhalter zur Verfügung (§ 3 Abs. 2 Nr. 1 GDNG). Die DKS führt ein „öffentliches Antragsregister“ mit Informationen zu den bei ihr gestellten Datenzugangsanträgen und „zu deren Ergebnissen“ (§ 3 Abs. 2 Nr. 7 GDNG). Zudem hat die DKS allgemein die Öffentlichkeit über seine Aktivitäten zu informieren (§ 3 Abs. 2 Nr. 6 GDNG).

Für die Antragsverfahren zu und die **Bereitstellung von FDZ-Daten** sieht § 303d Abs. 1 Nr. 6 SGB V „ein öffentliches Antragsregister mit Informationen zu den antragstellenden Nutzungsberechtigten, zu den Vorhaben, für die Daten beantragt wurden, und deren Ergebnissen“ vor. Als Pflichtangaben in diesem Register sind vorgesehen „1. Name und Kontaktdaten des Nutzungsberechtigten“, 2. die Nutzungszwecke, 3. der Titel des Vorhabens, 4. eine kurze Ergebnisdarstellung nach Veröffentlichung und 5. „das Jahr der Entscheidung über den Antrag“ (§ 19 FDZGesV-E). Mit Zustimmung des Antragstellers können weitere Informationen aufgenommen werden.

10.7 Bewertung der Transparenzregeln

Die Transparenzregeln haben eine **dreifache Zielrichtung**: Sie sollen 1. die Menschen generell über die Sekundärnutzung und die ihnen zustehenden Rechte informieren, 2. von konkreten

Datennutzungen Betroffenen Hinweise geben, um ihnen so Rechtsschutzmöglichkeiten zu eröffnen,[131] und 3. Öffentlichkeit bzgl. der Sekundärnutzungen herstellen, um für die demokratischen und wissenschaftlichen Instanzen Hinweise über die Praxis und für evtl. nötige Kritik zu geben. Transparenzpflichten sind geeignete Vorkehrungen zur verfassungsrechtlichen Kompensation informationeller Eingriffe.[132]

Die Transparenzpflichten betreffen auch **Forschungsvorhaben** und die Forschenden. Diese Pflichten sind im Hinblick auf Art. 5 Abs. 3 GG bzw. Art. 13 GRCh nicht angreifbar: Die Veröffentlichung von Ergebnissen ist ein zentraler Bestandteil des die Wissenschaft kennzeichnenden öffentlichen Dialogs. Hierüber können die Durchführung der Projekte und deren Ergebnisse hinterfragt und überprüft werden.[133] Dass auch schon Anträge zu Forschungsvorhaben zu veröffentlichen sind, rechtfertigt sich aus dem Umstand, dass mit der Sekundärnutzung in das Recht auf informationelle Selbstbestimmung von Betroffenen eingegriffen wird, was durch diese überprüfbar sein muss.[134] Die im GDNG vorgesehene Transparenzpflicht bzgl. der Sekundärnutzung wird als Kompensation für die Begrenzung der Betroffenenrechte gerechtfertigt.[135]

Es ist irritierend, dass die Regeln zur Registrierungspflicht des § 8 GDNG und zum FDZ-Antragsregister (§ 303d Abs. 1 Nr. 6 SGB V, § 19 FDZGesV-E) sowie die künftig wirksamen EHDS-Regelungen stark **voneinander abweichen**. So sieht § 8 GDNG überhaupt kein Antragsregister vor mit Informationen zum Genehmigungsverfahren und dessen Ergebnis. Vielmehr wird die Registrierungspflicht erst mit dem „Beginn der Datenverarbeitung“ begründet (S. 1).

Es gibt keinen Anlass, Vorhaben, die auf einer **Patienteneinwilligung** basieren, von der Transparenzpflicht auszunehmen, so wie dies in § 8 S. 1 GDNG der Fall ist. Dies gilt besonders, solange 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.[136]

Ungeeignet ist in § 8 GDNG die Regelung, dass eine Publikationspflicht nicht bestehen soll, wenn das Forschungsvorhaben auf Grundlage eines Gesetzes bereits **an anderer Stelle registriert** wurde (S. 2). Betroffene können so nicht erkennen, ob ihre Daten von einem Vorhaben betroffen sein können.

Dass mit öffentlichen Mitteln geförderte Forschungsvorhaben einer Veröffentlichungspflicht unterworfen werden, sollte selbstverständlich sein. Unverhältnismäßig ist schließlich die

[131] DSK GDNG-Stellungnahme, 7; VG Hamburg 28.07.2022 – 21 K 1802/21 Rn. 119.
[132] Weichert DANA 2/2024, 70.
[133] Weichert, Rahmenbedingungen, S. 21 f. m. w. N.
[134] Ausführlich Weichert, Rahmenbedingungen, S. 23 ff.
[135] BT-Drs. 20/9046, 59; GDNG-Referentenentwurf 9/2023, S. 32; dazu Weichert GuP 2023, 186.
[136] Weichert, Rahmenbedingungen, S. 99 f.

Regelung des § 8 S. 4 GDNG, wonach Behörden bestimmen können, dass zum **Schutz öffentlicher Belange** i. S. v. § 3 IFG von ihnen beauftragte Vorhaben nicht registriert werden müssen. Der Verweis auf die in § 3 IFG enthaltene Schutzregelung öffentlicher Belange berücksichtigt nicht, dass im GDNG die Forschungsgrundlage personenbeziehbare Informationen sind, mit deren Nutzung Eingriffe in das Grundrecht auf Datenschutz erfolgen. Um die Interessen der Betroffenen, etwa zwecks Rechtsschutz zu wahren, muss ein Mindestmaß an Transparenz bestehen.

Das **FDZ-Antragsregister** kennt die Einschränkungen des GDNG nicht. Doch auch insofern bestehen Defizite, die dazu führen, dass die Transparenzzwecke nicht erreicht werden. So fehlt es an einer Bekanntgabe der in Anspruch genommenen Quellen und Daten. Ohne diese können die Betroffenen nicht erkennen, ob sie betroffen sein können. Der Zeitpunkt der Genehmigungsentscheidung ist mit genauem Datum zu benennen, nicht wie geregelt, nur als Jahresangabe. Wünschenswert ist, dass auch der Zeitpunkt der Antragstellung bekannt gegeben wird, damit das Genehmigungsverfahren bei der Zugangsstelle nachvollzogen werden kann.

Ungenügend ist es zudem, dass nur eine „kurze Ergebnisdarstellung nach **Veröffentlichung von Ergebnissen** oder Verweise auf die Publikationen“ verpflichtend sein soll (§ 19 Abs. 1 Nr. 4 FDZGesV-E).[137] Aus einer kurzen Ergebnisdarstellung kann im Nachhinein nicht erkannt werden, inwieweit die starken informationellen Eingriffe in Betroffenenrechte durch das Ergebnis legitimiert sind. Eine solche Ex-post-Bewertung kann natürlich grds. nicht dazu führen, dass eine genehmigte Datennutzung nachträglich für unzulässig erklärt wird. Wohl aber können hieraus Schlüsse über den Datennutzer, die von ihm verfolgte (wissenschaftliche) Qualität sowie über die verfolgte Fragestellung für die Zukunft gezogen werden. Auch kann festgestellt werden, ob den Genehmigungsanforderungen genügt wurde. Eine Publikationspflicht darf zudem nicht davon abhängig gemacht werden, dass bei der Sekundärnutzung neue Erkenntnisse erlangt wurden. Scheitert ein Projekt, so können und müssen evtl. auch hieraus Schlüsse gezogen werden. Daher ist selbst der Umstand, dass ein Projekt ohne neue Erkenntnisse abgeschlossen werden musste, zu veröffentlichen.[138] Schließlich können Publikationen in möglicherweise schwer erreichbaren oder teuren Fachzeitschriften die Ergebnisdarstellung über das Internet nicht ersetzen, sondern nur ergänzen.

11 Sekundärnutzung konkret

Die Datennutzer dürfen die Gesundheitsdaten nur gemäß der ihnen erteilten Genehmigung verarbeiten (Art. 61 Abs. 1 EHDS). Ihnen ist es verboten, eine Reidentifizierung der

[137] Vgl. Böning/Riechert in Augsberg/Düwell/Müller, S. 249.
[138] Weichert, Rahmenbedingungen, S. 23.

pseudonymen Daten vorzunehmen oder dies auch nur zu versuchen (Art. 61 Abs. 3 EHDS). Verboten ist auch eine Weitergabe der Daten.

Das GDNG enthält entsprechende Vorgaben. Eine Weitergabe der erlangten Daten bedarf einer gesetzlichen Grundlage (§ 7 Abs. 4 GDNG). Die EHDS-Vorgaben präzisierend wird – der Regelung des § 203 Abs. 3 u. 4 StGB folgend – klargestellt, dass eine Datenweitergabe an **Gehilfen und Mitwirkende** erlaubt ist (§ 7 Abs. 3 GDNG).

11.1 Technische Umsetzung in der sicheren Verarbeitungsumgebung

Während die Datensicherheit bei der Primärnutzung durch die Mitgliedstaaten geregelt wird, wobei Art. 7 und 8 GRCh zu beachten sind (Art. 86 EHDS), erfolgt die Normierung der Sekundärnutzung direkt im EHDS. Diese soll in einer **sicheren Verarbeitungsumgebung** erfolgen, bei der strenge technische Vorkehrungen und Sicherheitsgarantien gelten.[139] 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).

Der EHDS verweist auf den Data Governance Act (DGA). Die Zugangsstellen i. S. d. EHDS sind die „**zuständigen Stellen**“ i. S. d. Art. 7 DGA, welche die sichere Verarbeitungsumgebung bereitstellen. Gemäß Art. 5 Abs. 3 lit. b u. c DGA erfolgt die Weiterverwendung der Daten „innerhalb der physischen Räumlichkeit“ der öffentlichen Stelle „sofern ein Fernzugriff nicht erlaubt werden kann, ohne die Rechte und Interessen Dritter zu gefährden“. Die öffentliche Stelle soll dabei die Kontrolle über die Verarbeitung bewahren (Art. 5 Abs. 4 DGA).

Es ist also auch möglich, bei weiteren Stelle, „**anerkannten altruistischen Organisationen**“ gemäß Kapitel IV (Art. 16-24) DGA Gesundheitsdaten für Sekundärzwecke zu verarbeiten (Art. 73 Abs. 4 EHDS).

Art. 1 Nr. 20 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

[139] DSK, EHDS-Stellungnahme v. 27.03.2023, 3.

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).

Erfolgt die **Sekundärnutzung grenzüberschreitend** (Art. 1 Abs. 2 lit. e EHDS) im Rahmen des „Zugangsdienstes der Union für Gesundheitsdaten“ HealthData@EU, so sind die technisch-organisatorischen wie inhaltlichen Anforderungen ebenso einzuhalten (Art. 75 Abs. 6, 9 EHDS, ErwGr 79 EHDS). Über Risiken und Vorfälle in sicheren Verarbeitungsumgebungen soll ein europaweiter Austausch – unter Einbeziehung eines Ausschusses für den europäischen Gesundheitsdatenraum (EHDS-Ausschuss) – erfolgen (ErwGr 95 S. 4-6 EHDS).

Die inhaltlichen Anforderungen für die Verarbeitungsumgebung werden in der **DSGVO** konkretisiert und zwar dort insbesondere in den Art. 25 und 32 DSGVO. Formell bedarf es einer Datenschutz-Folgenabschätzung gemäß Art. 35, 36 DSGVO (ErwGr 15 DGA). Parallel anwendbar bleiben die Cybersicherheitsanforderungen der Verordnung (EU) 2024/2847 (ErwGr 112 EHDS).[140]

Zur Gewährleistung einheitlicher Bedingungen ist die EU-Kommission u. a. befugt, „technische und organisatorische Anforderungen sowie Anforderungen an die Informationssicherheit, die Vertraulichkeit, den Datenschutz und die Interoperabilität der sicheren Verarbeitungsumgebungen“ in **Durchführungsakten** festzulegen (Art. 75 Abs. 12 EHDS, ErwGr 105 22. Sp. EHDS).

Die sichere Verarbeitungsumgebung beim Dateninhaber oder der Zugangstelle kann durch diese sowohl als Verantwortlicher (Art. 24 ff. DSGVO) wie auch als Auftragsverarbeiter (Art. 28 DSGVO) zur Verfügung gestellt werden. Der EHDS geht offenbar davon aus, dass bzgl. einer Sekundärnutzung beide Formen der **Verantwortlichkeit** gegeben sein können (ErwGr 79 EHDS).

Das **GDNG** sieht vor, dass die Zugangsstelle Konzepte erstellt „zur Nutzung von sicheren Verarbeitungsumgebungen als Maßnahme zur Verbesserung des Datenschutzes und der Datensicherheit im Rahmen der Weiterverarbeitung von Gesundheitsdaten“ (§ 3 Abs. 2 Nr. 9a GDNG). Für die Verknüpfung von Daten des FDZ und der Krebsregister muss eine sichere Verarbeitungsumgebung durch geeignete technische und organisatorische Maßnahmen

[140] Cyberresilienz-Verordnung v. 23.10.2024, ABl. EU v. 20.11.2024

sichergestellt sein, so dass „die Verarbeitung durch die Antragstellenden auf das für den jeweiligen Nutzungszweck erforderliche Maß beschränkt ist und insbesondere ein Kopieren der Daten verhindert werden kann“ (§ 4 Abs. 5 S. 2 GDNG). Das BMG wird ermächtigt, das technische Verfahren zur Verknüpfung durch Rechtsverordnung zu regeln und dort die „Anforderungen an sichere Verarbeitungsumgebungen“ festzulegen (§ 4 Abs. 9 GDNG).

Hinsichtlich der **Datensicherheit beim FDZ** bestehen in § 303e Abs. 4 S. 2 Nr. 2 SGB V entsprechende Anforderungen. Es muss durch geeignete technische und organisatorische Maßnahmen sichergestellt werden, dass die Verarbeitung durch den Nutzungsberechtigten „auf das erforderliche Maß beschränkt und insbesondere ein Kopieren der Daten verhindert werden kann“. Das FDZ legt „im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik die erforderlichen spezifischen, technischen und organisatorischen Maßnahmen fest, um die Datenverarbeitung in der sicheren Verarbeitungsumgebung durch den Nutzungsberechtigten auf das erforderliche Maß zu beschränken und um das Risiko einer Identifizierung einzelner Betroffener zu minimieren“ (§ 20 Abs. 2 S. 3 FDZGesV-E).

Vor der erstmaligen Bereitstellung von FDZ-Daten an Nutzungsberechtigte hat eine **Datenschutzfolgenabschätzung** nach Art. 35 DSGVO zu erfolgen (§ 22 Abs. 3 FDZGesV-E).

Die **Praktikabilität** eine Datenverarbeitung ausschließlich in der sicheren Verarbeitungsumgebung des FDZ bzw. einer Zugangsstelle ist insbesondere für Forschende, die weitere externe Datensätze in ihrem Vorhaben einbeziehen, derzeit nicht zu beurteilen. Diese hängt stark davon ab, welche Gestaltungsmöglichkeiten den Datennutzern im Rahmen der Verarbeitungsumgebung zugestanden werden.[141]

11.2 Zentrale oder dezentrale Verarbeitung?

Der EHDS macht keine Vorgaben, **wo** die für die Sekundärnutzung **vorgesehenen Daten gespeichert** werden, bevor sie den Datennutzenden bereitgestellt werden. Dies erfolgt regelmäßig bei den Dateninhabern (Art. 50 EHDS). Möglich ist aber auch, dass die Daten schon bei der Zugangsstelle empfangen, pseudonymisiert, kombiniert, aufbereitet und zusammengestellt werden (Art. 57 Abs. 1 lit. b EHDS). Ebenso möglich ist die Bereithaltung der Daten in Registern[142], ja selbst in grenzüberschreitenden Registern oder Datenbanken (ErwGr. 56, 82, 87 EHDS, Art. 51 Abs. 1 lit. k, l, o, Art. 76 EHDS).

Mit dem **FDZ** steht eine zentrale Datensammlung für die Sekundärnutzung zur Verfügung, in der bundesweit sämtliche GKV-Abrechnungsdaten sowie die GKV-ePA-Daten, soweit kein Widerspruch erfolgt ist, gespeichert werden.[143]

[141] Kritisch Weichert MedR 2020, 544.
[142] Stollmann/Stenzel in Dittrich/Dochow/Ippach, Kap. 16 (S. 251 ff.).
[143] Zur Kritik der zentralen Speicherung anlässlich der Gesetzgebung Weichert MedR 2020, 540.

Zentrale Datenspeicherungen ermöglichen es, ohne größeren Aufwand eine Vielzahl unterschiedlicher Auswertungen vorzunehmen. Dies gilt auch für spezielle Fragestellungen, zu denen es nur wenige aussagekräftige Datensätze gibt, etwa bei der Erforschung seltener Krankheiten. Das Ziel, für die Gesamtbevölkerung **repräsentative Auswertungen** vornehmen zu können, kann über zentrale Datenbanken einfacher erreicht werden als bei einem Zusammenführen dezentraler Datensätze.

Zentrale große Datensammlungen ermöglichen zudem eine **Anonymisierung durch Aggregierung**, selbst wenn viele Merkmal ausgewertet werden (sog. K-Anonymität).[144] Qualitätsdefizite bei einzelnen Datensätzen haben dort eine geringere Auswirkung auf ein Gesamtergebnis.

Ein Problem zentraler Datensammlungen, die das Zusammenführen von Daten aus unterschiedlichen Quellen nötig macht, kann darin bestehen, dass bei Melde-Defiziten die inhaltliche Richtigkeit und Aktualität leidet. Auf Primärnutzungen basierende Datenspeicherungen haben regelmäßig die Vorteile einer größeren **Sachnähe und Qualität**, einer höheren Aktualität und Richtigkeit.

Aus **Datenschutz- und Datensicherheitssicht** sind dezentrale Quellen vorzugswürdig. Mit ihnen wird eher dem Datenminimierungsgebot (Art. 5 Abs. 1 lit. c DSGVO) entsprochen. Das Risiko einer Vorratsdatenverarbeitung von nicht erforderlichen Daten wird erhöht (s. o. 5.8). Zentrale Datensammlungen werden bei Cyberangriffen von Kriminellen bevorzugt. Erfolgreiche Angriffe auf eine zentrale Infrastruktur haben größere Beeinträchtigungen bzgl. der Verfügbarkeit und Vertraulichkeit zur Folge. Andererseits ergeben sich bei einer zentralisierten Datenhaltung Einsparungen und Effizienzgewinne. Dies gilt auch für die Einrichtung von Datensicherheitsmaßnahmen. Der EuGH hat festgestellt, dass mit einer zentralen Datenspeicherung erhöhte Risiken einhergehen können. Dadurch erreichte Wirksamkeitsverbesserungen könnten diese Risiken aber legitimieren.[145]

Im Zusammenhang mit europaweiten HealthData@EU erwähnt der EHDS das Konzept „Besser die **Fragen zu den Daten bringen**, statt die Daten selbst zu übertragen“ (ErwGr 79 S. S. 2 EHDS). Dieses Konzept sieht im Interesse der Datenminimierung vor, dass eine Auswertung gemäß einer Fragestellung eines (Forschungs-)Projektes schon beim Dateninhaber erfolgt und dem Datennutzer nur noch aggregierte (anonymisierte) Daten bereitgestellt werden.

12 Betroffenenrechte

Der EHDS baut auf dem Schutz der DSGVO auf und erweitert die dort gewährten Rechte (ErwGr 8 u. 9 EHDS). Den Betroffenen steht gemäß dem EHDS in Bezug auf die für diese

[144] Hansen in Simitis/Hornung/Spiecker, Art. 4 Nr. 5 Rn. 56.
[145] EuGH 16.12.2008 – C-524/06, Rn. 62, DVBl 2009, 173.

geltenden Schutzregelungen ein umfassendes **Recht auf Beschwerde** zu. Die Beschwerden können bei einer Primärnutzung an die Stellen für digitale Gesundheit und bei einer Sekundärnutzung an die Zugangsstellen adressiert werden (Art. 81 EHDS, ErwGr 99 EHDS). Betrifft eine Beschwerde den Datenschutz, so wird die EHDS-Beschwerde an die Datenschutzaufsichtsbehörden zur weiteren Bearbeitung weitergegeben (Art. 81 Abs. 4 i. V. m. Art. 71 EHDS, ErwGr 99 S. 6 EHDS).

Neben dem individuellen Beschwerderecht sieht der EHDS zudem vor, dass sich – gemäß national vorzusehendem Recht – Betroffene auch durch eine „Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht, deren satzungsmäßige Ziele im öffentlichen Interesse liegen und die im Bereich des Schutzes personenbezogener Daten tätig sind“ vertreten lassen können (Art. 101 EHDS, ErwGr 100 EHDS). Eine entsprechende Möglichkeit einer **kollektiven Interessenvertretung** sieht in Bezug auf Datenschutzverstöße Art. 80 Abs. 1 DSGVO vor (vgl. § 2 Abs. 2 Nr. 11 UKlaG).

12.1 Beschränkung der Betroffenenrechte?

Beschränkungen der datenschutzrechtlichen Betroffenenrechten sind gemäß Art. 23 Abs. 1 DSGVO möglich. Diese sind aber grundsätzlich nicht auf die Sekundärnutzung von Gesundheitsdaten gemäß dem EHDS anwendbar. Zwar sieht Art. 23 Abs. 1 lit. e DSGVO einen „Schutz wichtiger Ziele des **allgemeinen öffentlichen Interesses**“ etwa „im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit“ vor. Es ist aber nicht erkennbar, wie sekundär genutzte Daten, mit denen keine individuellen Zwecke verfolgt werden, durch die Wahrnehmung individuelle Betroffenenrechte beeinträchtigt sein können. Mit Blick auf Forschungszwecke sieht Art. 89 Abs. 1 DSGVO Ausnahmemöglichkeiten vor.[146]

Betroffenenrechte bestehen grds. auch in Bezug auf **pseudonymisierte Daten**.[147] Art. 71 Abs. 8 EHDS regelt für den Gesundheitsdateninhaber, dass er allein für Zwecke der Umsetzung des Widerspruchsrechts gegen die Sekundärnutzung nicht verpflichtet ist, Informationen zur Identifizierung vorzuhalten. Diese Regelung entspricht dem Art. 11 DSGVO im Hinblick auf sämtliche Betroffenenrechte gemäß der DSGVO, wenn die vorgesehene Pseudonymisierung der „bloßen Einhaltung dieser Verordnung“ dient. Der Pseudonymisierung bei den EHDS-Zugangsstellen kommt auch die Funktion einer späteren Zuordnung von weiteren Datensätzen zu. Die Regelungen des Art. 71 Abs. 8 EHDS bzw. des Art. 11 DSGVO sollen die Datenminimierung im Einzelfall fördern.[148] Sie finden aber keine Anwendung, wenn eine gesetzliche angeordnete Pseudonymisierung für Sekundärzwecke erfolgt, mit der ein quellenübergreifender Identifikator z. B. für Gesundheitsdaten erstellt wird, der der

[146] Etwas eingeschränkter Böning/Riechert in Augsberg/Düwell/Müller, S. 228.
[147] Dix in Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 15 Rn. 12; Däubler in Däubler u.a. (En. 40), Art. 15 Rn. 4.
[148] Weichert in Kühling/Buchner, Art. 11 Rn. 11.

Zuordnung von Datensätzen aus verschiedenen Quellen zu einer Person dient.[149] Die Regelungen des Art. 71 Abs. 8 EHDS bzw. des Art. 11 DSGVO sind nur relevant, wenn die Pseudonyme ausschließlich zwecks Datenminimierung genutzt werden, ohne dass sie darüber hinausgehend **Zuordnungszwecken** dienen. Daher gelten diese Regelungen auch nicht, wenn die Pseudonyme eine Rückmeldung im Fall eines „wesentlichen Befundes" ermöglichen (s. u. 12.5).

Art. 11 DSGVO entbindet von der Pflicht zur Wahrung der Betroffenenrechte nur, wenn der Verantwortliche nachweisen kann, dass er die betroffene Person nicht identifizieren kann. Anderes gilt, wenn die betroffene Person zur Ausübung ihrer Rechte **zusätzliche Informationen** bereitstellt, die ihre Identifizierung ermöglichen (Art. 11 Abs. 2 S. 2 DSGVO). So kann z. B. der Betroffene Merkmalsangaben gegenüber einem Verantwortlichen zur Verfügung stellen, die primär genutzten Gesundheitsdaten (z. B. Angaben zur Diagnose, die behandelnden Einrichtung, zu Operationsangaben) entsprechen, die der Sekundärnutzung zur Verfügung gestellt wurden. Solche Merkmals-Datensätze eignen sich als „Pseudonyme" zur Zuordnung der sekundär genutzten Gesundheitsdatensätze zu dem Betroffenen. Über eine solche Zuordnung ist eine Reidentifizierung der pseudonymisierten Sekundärdaten und damit die Wahrnehmung der Betroffenenrechte möglich.

12.2 Betroffenentransparenz

Art. 14 DSGVO sieht eine **Informationspflicht** vor, wenn Daten nicht beim Betroffenen erhoben wurden. Dies ist im Fall einer Sekundärnutzung generell der Fall. In Ergänzung zu Art. 14 DSGVO sollen die EHDS-Zugangsstellen „sicherstellen, dass die Sekundärnutzung transparent ist, indem sie die Öffentlichkeit über die erteilten Datengenehmigungen und ihre Begründungen, die Maßnahmen zum Schutz der Rechte natürlicher Personen, die Art und Weise, wie natürliche Personen ihre Rechte in Bezug auf die Sekundärnutzung ausüben können, und die Ergebnisse der Sekundärnutzung informieren, auch durch Links zu wissenschaftlichen Veröffentlichungen. Diese Informationen über die Ergebnisse der Sekundärnutzung sollten gegebenenfalls auch eine vom Gesundheitsdatennutzer bereitzustellende Zusammenfassung für Laien umfassen" (ErwGr 66 S. 1, 2 EHDS).

Eine individuelle Informationspflicht soll gem. Art. 14 Abs. 5 lit. b DSGVO nicht bestehen, wenn die Erteilung der Information einen unverhältnismäßigen Aufwand erfordern würde, insbesondere bei wissenschaftlichen Forschungszwecken. Eine **Ausnahme von der Informationspflicht** kann gemäß lit. c auf Grundlage einer Rechtsvorschrift zudem gegeben sein, wenn geeignete Maßnahmen zum Schutz der berechtigten Betroffeneninteressen bestehen (vgl. ErwGr 66 S. 3).

[149] Weichert DANA 2/2024, 71; Weichert GuP 2023, 187; Weichert MedR 2020, 543.

Demgemäß regelt Art. 58 Abs. 1 u. 2 EHDS eine allgemeine **Transparenzpflicht für die Zugangsstellen**:

„(1) Die Zugangsstellen für Gesundheitsdaten machen Informationen über die Bedingungen, unter denen elektronische Gesundheitsdaten für die Sekundärnutzung zur Verfügung gestellt werden, öffentlich verfügbar, auf elektronischem Wege leicht durchsuchbar und für natürliche Personen zugänglich. Diese Informationen enthalten Angaben

- *a) über die Rechtsgrundlage für die Gewährung des Zugangs zu elektronischen Gesundheitsdaten für den Gesundheitsdatennutzer;*
- *b) über die technischen und organisatorischen Maßnahmen, die zum Schutz der Rechte natürlicher Personen ergriffen werden;*
- *c) über die geltenden Rechte natürlicher Personen hinsichtlich der Sekundärnutzung;*
- *d) über die Modalitäten, unter denen natürliche Personen ihre Rechte gemäß Kapitel III der Verordnung (EU) 2016/679 wahrnehmen können;*
- *e) über die Identität und die Kontaktdaten der Zugangsstelle für Gesundheitsdaten;*
- *f) darüber, wer Zugang zu elektronischen Gesundheitsdatensätzen erhalten hat und zu welchen Datensätzen sie Zugang erhalten haben, sowie zu Einzelheiten der Datengenehmigung bezüglich der Zwecke der Verarbeitung dieser Daten gemäß Artikel 53 Absatz 1;*
- *g) die Ergebnisse oder Resultate der Projekte, für die die elektronischen Gesundheitsdaten verwendet wurden.“*

(2) Hat ein Mitgliedstaat vorgesehen, dass das Recht zum Widerspruch im Sinne von Artikel 71 über die Zugangsstellen für Gesundheitsdaten ausgeübt werden kann, so stellen die einschlägigen Zugangsstellen für Gesundheitsdaten öffentliche Informationen über das Verfahren des Widerspruchs bereit und erleichtern die Ausübung dieses Rechts.“

Die im EHDS festgelegten Transparenzpflichten 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).

Das GDNG und die §§ 303a ff. SGB V sehen keine individuelle Information der Betroffenen über die sie betreffende Sekundärnutzung vor (zu den allgemeinen Informationen s. o. 10.6). Zur Umsetzung des Widerspruchsrechts der Patienten gegen die Speicherung ihrer ePA im FDZ richten die Kranken- und Pflegekassen bzw. deren Dienstleister Ombudsstellen ein (§ 342a SGB V). Für die Umsetzung des Widerspruchsrechts ist in § 13 Abs. 1 FDZGesV-E zudem vorgesehen, dass über die Benutzeroberfläche eines geeigneten Endgeräts (**Datencockpit**) „Informationen über die Ausleitung von Daten aus der elektronischen Patientenakte“ in das FDZ nachvollziehbar zu machen sind.

12.3 Auskunftsanspruch

Art. 3 u. 4 EHDS sehen weit gehende Rechte von betroffenen Personen auf „Zugang zu ihren personenbezogenen elektronischen Gesundheitsdaten“ vor. Diese Rechte bestehen aber nur hinsichtlich der „Primärnutzung“,[150] nicht für die in Kapitel IV geregelt Sekundärnutzung. Da der Sekundärnutzung in jedem Fall eine Primärnutzung bei einem **Gesundheitsdateninhaber** vorausgegangen ist, finden insofern für diesen die weitgehenden Auskunftsrechte nach Art. 3 EHDS Anwendung. Hinsichtlich der Zugangsstellen und der Datennutzer ist Art. 3 EHDS jedoch nicht anwendbar.

Für diese gilt weiterhin der allgemeine **Auskunftsanspruch nach Art. 15 DSGVO** sowie dessen verfassungsrechtliche Grundlage in Art. 8 Abs. 2 S. 2 GRCh. Art. 15 Abs. 1 DSGVO begründet einen Anspruch auf Informationen über Verarbeitungszwecke, Datenkategorien und Empfänger (lit. a-c). Gemäß Art. 15 Abs. 2 DSGVO erstreckt sich dies auch auf eine „Kopie der personenbezogenen Daten“. Dient ein im Rahmen der Sekundärnutzung eingesetztes Pseudonym also auch der Zuordnung von Datensätzen aus verschiedenen Quellen zu einem namentlich nicht bekannten Patienten bzw. Betroffenen, dann sind Art. 11 DSGVO und Art. 71 Abs. 8 EHDS nicht anwendbar (s. o. 12.1). Die Betroffenen können dann über das für die Sekundärnutzung zur Datensatz-Zuordnung genutzte Pseudonym ihren Auskunftsanspruch durchsetzen.

Auch Art. 23 Abs. 1 lit. i DSGVO ist regelmäßig nicht anwendbar: Einem Auskunftsanspruch von Betroffenen stehen keine „**Rechte und Freiheiten anderer Personen**“ entgegen. Durch eine Auskunft werden die Dritten eingeräumten Sekundärnutzungsrechte nicht eingeschränkt (s. o. 12.1).[151]

Die der Sekundärnutzung zugeführten Einzeldatensätze sind regelmäßig pseudonym und personenbeziehbar. Das nationale Recht untersagt Nutzungsberechtigten eine **Reidentifizierung von Sekundärnutzungsdaten** (§ 7 Abs. 2 GDNG; § 303e Abs. 5 S. 2, 3 SGB V). Entsprechendes regelt der EHDS (Art. 61 Abs. 3 EHDS). Dies kann aber nicht für die Umsetzung des verfassungsrechtlich begründeten Auskunftsanspruchs[152] gelten. Hiergegen kann regelmäßig nicht argumentiert werden, eine Auskunft würde einen unverhältnismäßigen Aufwand erfordern (vgl. § 27 Abs. 2 S. 2 BDSG).[153] Gerade bei einem zentralisierten automatisierten Verfahren wie dem im FDZ kann durch die Etablierung von Standardabläufen der Aufwand für eine Reidentifizierung auf ein Minimum reduziert werden. Beim FDZ findet ein individualisiertes Verknüpfen von Datensätzen für Sekundärzwecke statt. Es ist nicht zu

[150] Böning/Riechert in Augsberg/Düwell/Müller, S. 229.
[151] VG Hamburg 28.07.2022 – 21 K 1802/21 Rn. 81.
[152] VG Hamburg 28.07.2022 – 21 K 1802/21 Rn. 80; Däubler in Däubler u.a., Art. 15 Rn. 1; Bäcker in Kühling/Buchner, Art. 15 Rn. 5, jeweils mit Verweis auf Art. 8 Abs. 2 S. 2 GRCh; zum nationalen Verfassungsrecht Weichert NVwZ 2007, 1005 f.
[153] Vgl. VG Berlin 06.02.2024 – 1 K 187/21.

rechtfertigen, dass diese Verknüpfung den Betroffenen selbst vorenthalten wird. Auch andere Erwägungen, die eine Auskunftsverweigerung begründen könnten (§ 83 Abs. 1 SGB X), sind nicht ersichtlich.

Eingriffe in das Auskunftsrecht sind nur auf gesetzlicher Grundlage zulässig, soweit diese sich als erforderlich erweisen. Sieht ein Gesetz eine Verschleierung der Personenidentität vor und dienen die verwendeten Pseudonyme einer eindeutigen Zuordnung zu einer Person, so muss das Gesetz auch einen Prozess festlegen, mit dem die Betroffenenrechte gewahrt werden können.[154] Da zudem vom Betroffenen die Bereitstellung bestimmter die Identifizierung ermöglichenden Daten problemlos gegenüber dem FDZ machbar ist, etwa indem von ihm individuelle Verschreibungs- oder Behandlungsdaten benannt werden, kann im Gesamtdatenbestand kann hierüber regelmäßig eine eindeutige Zuordnung erfolgen. Auch deshalb ist der **Ausschluss des Auskunftsrechts nach Art. 11 DSGVO** nicht gerechtfertigt (s. o. 12.1).

Nach übergeordnetem Recht besteht also ein Auskunftsanspruch, auch wenn in den §§ 303a ff. SGB V oder im GDNG bisher kein Verfahren vorgesehen ist, mit dem dieser Anspruch umgesetzt werden kann. Ein **geregeltes Verfahren** wäre im Fall des FDZ unter Einbindung von Krankenkasse und Vertrauensstelle möglich. Das FDZ enthält auf einzelne Personen zurückgehende Einzeldatensätze, die Sekundärnutzenden bereitgestellt werden können. Es sind keine Gründe erkennbar, diese Daten den Betroffenen vorzuenthalten.

Dass den Betroffenen ein Auskunftsrecht beim FDZ verweigert wird, verstößt gegen höherrangiges Recht und ist sowohl **verfassungs- wie auch europarechtswidrig**.[155]

12.4 Widerspruchsrecht

Der EHDS will den Konflikt zwischen Patientenautonomie und gesellschaftlichem Nutzen der Gesundheitsdaten dadurch lösen, dass er vorsieht, dass von den Mitgliedstaaten den Betroffenen ein (nicht begründungspflichtiges) Widerspruchsrecht **gegen die Sekundärnutzung** eingeräumt werden kann (Art. 71 EHDS).[156] Diese Möglichkeit kann sich auf die Sekundärnutzung generell oder auf bestimmte Daten beziehen. Im Fall eines Widerspruchs dürfen die Daten für Sekundärzwecke nicht mehr genutzt werden. Den Betroffenen sollen umfassende Informationen über ihr Widerspruchsrecht zur Verfügung gestellt werden.

Widersprüche bleiben jedoch unberücksichtigt, wenn gemäß dem nationalen Recht „aus wichtigen Gründen des öffentlichen Interesses“ für die wissenschaftliche Forschung oder „zum Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren“ „vollständige Datensätze“ benötigt werden (Art. 71 Abs. 4-7 EHDS, ErwGr 54 S. 5 ff.). Eine

[154] Weichert in Kühling/Buchner, Art. 11 Rn. 1a.
[155] Weichert MedR 2020, 543.
[156] Hierzu und zur Kritik Buchholtz/Schmalhorst/Brauneck MedR 2024, 474 f.

entsprechende **Durchbrechung des Widerspruchsrechts** ist im deutschen Recht bisher nicht vorgesehen.

Kein Widerspruchsrecht besteht in Deutschland bzgl. der Einmeldung von **GKV-Abrechnungsdaten** ins FDZ.[157]

Etwas anderes gilt bzgl. der Nutzung der ePA für Sekundärzwecke. Voraussetzung ist, dass überhaupt eine ePA für primäre, also für **Behandlungszwecke,** besteht. Auch insofern besteht in Deutschland ein Widerspruchsrecht.[158] Dieses kann die ePA insgesamt betreffen wie auch einzelne Dokumente. Bzgl. des Einstellens in die ePA muss bei „sexuell übertragbaren Infektionen, psychischen Erkrankungen und Schwangerschaftsabbrüchen“ in jedem Einzelfall vom Arzt auf die Widerspruchsmöglichkeit hingewiesen werden (§ 343 Abs. 1 S. 3, Abs. 3 S. 6 SGB V, vgl. § 343 Abs. 1a Nr. 13 SGB V).

§ 363 SGB V regelt die „Verarbeitung von Daten der elektronischen Patientenakte zu Forschungszwecken“. Darin ist ein Widerspruchsrecht vorgesehen, das sich auf Sekundärnutzungen von Daten aus der elektronischen Patientenakte (ePA) im FDZ bezieht. Ein Widerspruch, der „über die Benutzeroberfläche eines geeigneten Endgeräts oder gegenüber der Ombudsstelle“ der Krankenkasse erklärt wird, hat zur Folge, dass die ePA-Daten an das FDZ **nicht übermittelt** werden dürfen (§ 363 Abs. 5 SGB V) bzw. dort gelöscht werden müssen (§ 363 Abs. 6 SGB V). Unbeschadet eines Widerspruchs können Betroffene einwilligungsbasiert ihre ePA über das FDZ für ein bestimmtes Forschungsvorhaben zur Verfügung stellen (§ 363 Abs. 8 SGB V).

In Umsetzung der Verordnungsermächtigung in § 363 Abs. 7 SGB V können gemäß § 8 FDZGesV-E die Betroffenen ihren in § 363 Abs. 5 SGB V vorgesehenen Widerspruch gegen die Ausleitung ihrer Daten aus der elektronischen Patientenakte (ePA) insgesamt oder teilweise nur für einen oder mehrere der in § 303e Abs. 2 Abs. 2 SGB V genannten Zwecke erklären. Ein „**Teilwiderspruch**“ erstreckt sich also pauschal auf die dort genannten Zwecke (z. B. „Forschung“ generell); ein Widerspruch gegen einzelne Auswertungsprojekte ist nicht vorgesehen.[159] Mit Hilfe des durch die Kassen zur Verfügung zu stellenden Datencockpits sollen „Versicherte ihren Widerspruch auch über die Benutzeroberfläche eines geeigneten Endgeräts“ erklären können (§ 13 Abs. 2 FDZGesV-E).

Das Widerspruchsrecht gegen die Erstellung einer ePA generell wie auch gegen die Übermittlung an das FDZ waren zentraler Gegenstand der **öffentlichen Diskussion** über die generelle Einführung der ePA.[160] Dieses Recht war im Kommissionsentwurf zum EHDS noch überhaupt nicht vorgesehen. Es wurde, nicht zuletzt auf Drängen Deutschlands, im Trilog-

[157] Weichert MedR 2020, 542.
[158] Bretthauer NVwZ 2024, 1054.
[159] Kritisch dazu HBDI, 52. Tätigkeitsbericht Datenschutz, 2023, Kap. 12.1 (S. 178); DSK GDNG-Stellungnahme, 10..
[160] Wolfangel, Wenn alle erfahren, was einem fehlt, Die Zeit Nr. 13 v. 23.03.2023, 37.

Verfahren aufgenommen. In einer Protokollerklärung wies die Bundesregierung darauf hin, dass die Opt-out-Möglichkeit schon bei der Erstellung der ePA zur Wahrung der Autonomie des Patienten fundamental sei.[161]

Bis zum **Wirksamwerden des EHDS** hat sich das nationale Widerspruchsrecht an der DSGVO zu orientieren, wonach die vorgesehenen Regeln grds. bei Forschungsnutzungen möglich sind, soweit kompensierende Garantien vorgesehen sind (Art. 21 Abs. 6 DSGVO).[162] Nach dem Wirksamwerden des EHDS sind zudem dessen Regeln zu beachten, die aber einen großen nationalen Regelungsspielraum offenhalten.

12.5 Anspruch auf Rückmeldung?

Angesichts des Umstands, dass Forschende für ihre wissenschaftliche Tätigkeit über den EHDS Einzeldatensätze zur Verfügung gestellt bekommen, besteht für diese die Möglichkeit, zu den hinter diesen Datensätzen stehenden Personen neue Erkenntnisse zu gewinnen. Im Interesse des individuellen Gesundheitsschutzes sieht nun der EHDS eine Rückmeldung an Arzt oder Patienten vor. Forschung soll der **Optimierung der Behandlung** des Patienten oder anderer Personen zugutekommen (Art. 53 Abs. 1 lit. e u. f EHDS). Demgemäß wird die Zugangsstelle in Art. 58 Abs. 3 EHDS verpflichtet, die von einer Befundmitteilung betroffene Person oder die eingebundene Person des Heilberufs unter den „im nationalen Recht festgelegten Bedingungen“ zu informieren.

Gemäß Art. 61 Abs. 5 EHDS haben Gesundheitsdatennutzer, die im Rahmen ihrer Nutzung **wesentliche Befunde** erlangen in Bezug auf die Gesundheit einer natürlichen Person, deren Daten in dem Datensatz enthalten sind, die Zugangsstelle hierüber zu informieren: „Natürliche Personen sollten von den Gesundheitsdateninhabern über wesentliche Befunde im Zusammenhang mit ihrer Gesundheit informiert werden, die von Gesundheitsdatennutzern festgestellt wurden. Natürliche Personen sollten das Recht haben, zu beantragen, dass sie nicht über solche Erkenntnisse informiert werden“ (ErwGr 67 S. 1, 2 EHDS).

„Natürliche Personen haben das Recht, zu verlangen, nicht über solche Erkenntnisse informiert zu werden“ (Art. 58 Abs. 3 S. 3 EHDS). Damit wird das insbesondere im Bereich der Genetik allgemein anerkannte **Recht auf Nichtwissen** auf aus der Sekundärnutzung erlangte medizinische Erkenntnisse ausgeweitet. Eine Entsprechung findet sich auch in der DSGVO: Zum Schutz der „Patientensicherheit und der Ethik“ soll die in Art. 23 Abs. 1 lit. i DSGVO genannte Einschränkung gelten, dass aus Gründen des Schutzes „der betroffenen Person oder

[161] Council oft he European Union 30.01.2024 Summary Report Permanent Representatives Committee 16641/23 CRS CRP 42 v. 30.01.2024, S. 13 f., https://data.consilium.europa.eu/doc/document/ST-16048-2023-REV-1/en/pdf.
[162] Vgl. Weichert MedR 2020, 542 f.

der Rechte und Freiheiten anderer Personen“ eine Beschränkung der Betroffenenrechte“ möglich ist.[163]

Damit wird dem nationalen Gesetzgeber die Umsetzung der Rückmeldung und der konkreten Normierung des Rechts auf Nichtwissen übertragen. Im GDNG und im SGB V gibt es bisher keine entsprechenden Regelungen. Eine Normierung des Rechts auf Nichtwissen besteht bisher in Bezug auf **genetische Gesundheitsdispositionen** (§§ 8, 9 Abs. 2 Nr. 5 GenDG).

12.6 Anspruch auf Schadenersatz

Werden durch Verstöße gegen den EHDS bei Betroffenen Schäden verursacht, so besteht für diese ein Schadenersatzanspruch (Art. 100 EHDS). Dieser Anspruch besteht ergänzend zu möglichen Schadenersatzansprüchen gemäß Art. 82 DSGVO. Die hierzu ergangene **Rechtsprechung des EuGH**[164] ist auf den EHDS übertragbar (ErwGr 101 EHDS). Spezifische nationale Regelungen zum Schadenersatz im Rahmen der Sekundärnutzung bestehen nicht.

13 Kontrollen

Die Zugangsstellen erhalten gemäß dem EHDS die Befugnis, die Einhaltung der dortigen Regeln gegenüber Dateninhabern und Datennutzern zu überprüfen und alle erforderlichen **Informationen einzuholen** (Art. 63 Abs. 1 EHDS, ErwGr 71 S. 2 EHDS). Sie haben zudem die Befugnis, geeignete und verhältnismäßige Maßnahmen zu ergreifen, um EHDS-konforme Zustände herzustellen (Art. 63 Abs. 2-5 EHDS).

13.1 Datenschutzaufsicht

Die Datenschutzaufsichtsbehörden sind für die Überwachung und Durchsetzung der DSGVO zuständig (Art. 55 ff. DSGVO). Da der EHDS die Betroffenenrechte der DSGVO teilweise präzisiert und ergänzt (Art. 1 Abs. 2 lit. a EHDS)[165], sind die Aufsichtsbehörden auch insofern zuständig (Art. 65 EHDS). Sie sind mit den nötigen „finanziellen und personellen Ressourcen, Räumlichkeiten und der Infrastruktur“ auszustatten (ErwGr 23 S. 3 EHDS). Im Fall von **EHDS-bedingten Datenschutzverstößen** werden die Datenschutzaufsichtsbehörden von der Zugangsstelle hierüber informiert (Art. 63 Abs. 2 UAbs. 2 EHDS).

Die Datenschutzaufsicht über das BfArM übt die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) aus. Entsprechendes gilt für Dateninhaber und Datennutzer, soweit es sich um öffentliche Stellen des Bundes handelt (§ 9 Abs. 1 BDSG). Sind Dateninhaber

[163] Weichert in Däubler u.a., Art. 4 Rn. 129; Bäcker in Kühling/Buchner, Art. 23 Rn. 30.
[164] EuGH 04.10.2024 – C-507/23; EuGH 20.06.2024 – C-182/22 u. C-189/22; EuGH 20.06.2024 – C-590/22; EuGH 11.04.2024 – C-741/21; EuGH 07.03.2024 – C-479/22 P; EuGH 21.12.2023 – C-667/21, dazu Weichert MedR 2024, 593; EuGH 04.05.2023 – C-300/21, dazu Weichert GesR 2023, 572 f.
[165] Gem. Art. 1 Abs. 4 EHDS gelten Bezugnahmen auf die DSGVO auch für die entsprechenden Bestimmungen der VO (EU) 2018/1725 zum Datenschutz für EU—Stellen.

oder Datennutzer nicht-öffentliche (private) Stellen oder Behörden eines Landes oder von Kommunen, so ist grds. eine **Zuständigkeit** bei den Aufsichtsbehörden der Länder begründet (§ 40 BDSG, Datenschutzrecht der Länder).

§ 5 GDNG enthält eine Sonderregelung, wenn Vorhaben der **Versorgungs- und Gesundheitsforschung stellenübergreifend** durchgeführt werden, so dass mehr als eine Datenschutzbehörde zuständig ist. In diesen Fällen kann eine federführende Aufsichtsbehörde durch entsprechende Erklärungen aller beteiligten Verantwortlichen benannt werden. In den Datentransparenzregelungen des SGB V besteht keine Sonderzuweisung zur Datenschutzaufsicht. Die für übergreifende Forschungsvorhaben bisher geltende Regelung des 287a SGB V (alt) ist in § 5 GDNG aufgegangen. § 303e Abs. 6 SGB V geht von einer klaren Zuständigkeit aus und verweist damit auf § 5 GDNG und die Regelungen des allgemeinen Datenschutzrechts.

Ob von der Datenschutzaufsicht eine **wirksame Kontrolle** ausgeübt werden kann, ist fraglich. Zwar bestehen hierfür die rechtlichen Voraussetzungen. Doch dürften die nötigen Ressourcen bisher nicht zur Verfügung stehen. Bei hochsensitiven, zentralisierten hoheitlichen Formen der Datenverarbeitung, die keinen sonstigen öffentlichen Kontrollmechanismen oder einer hinreichenden Transparenz unterliegen, hat das BVerfG eine gegenüber den allgemeinen Mechanismen verstärkte Kontrolle, z. B. kontinuierliche Regelkontrollen, gefordert.[166] Sinnvoll wäre die Etablierung eines spezifischen länderübergreifenden gemeinsamen Kontrollgremiums, das z. B. regelmäßige Stichprobenprüfungen durchführt.[167]

13.2 Rechtsaufsicht

Außerhalb der Datenschutzaufsicht bestehen bei der Sekundärnutzung von Gesundheitsdaten bisher keine wirksamen Kontrollinstanzen. Die beim BMG angesiedelte Rechtsaufsicht kann **keine wirksame Kontrolle** gewährleisten. Ihm fehlt insofern das Personal, die Unabhängigkeit und wohl auch das nötige Knowhow (s. o. 10.2).[168]

14 Sanktionen

Die Zugangsstellen werden nach dem EHDS befugt, **Geldbußen sowie Durchsetzungsmaßnahmen** zur Umsetzung der EHDS-Vorschriften zu verhängen (Art. 63, 64 EHDS; ErwGr 71 S. 1, 102, 103 EHDS). Versuchen Datennutzer bereitgestellte pseudonymisierte Daten zu reidentifizieren, so sind sie den im EHDS vorgesehenen Geldbußen und Durchsetzungsmaßnahmen zu unterwerfen, wobei die Reidentifizierung als ein besonders schwerer Verstoß gegen den EHDS anzusehen ist (ErwGr 72 S. 10, 106 S. 2 EHDS).

[166] BVerfG 24.03.2013 – 1 BvR 1215/07, Rn. 116 f., NJW 2013, 1504.
[167] Weichert MedR 2020, 545.
[168] Weichert MedR 2020, 545.

Im Fall eines Verstoßes gegen das **Reidentifizierungsverbot** muss wegen der Bedeutung der Rechtsverletzung eine Feststellung und eine Sanktionierung gewährleistet sein. Ob dies bisher in der deutschen Rechtspraxis gewährleistet ist, kann bezweifelt werden, da das Sanktionieren von evidenten Datenschutzverstößen hier selten, zumeist verspätet und äußerst milde erfolgt.[169] Sanktionsandrohungen sind zwar ein notwendiger, aber nicht hinreichender Schutz bei der Sekundärverarbeitung pseudonymisierter Gesundheitsdaten.

14.1 Strafbarkeit

Der EHDS enthält keine Regelungen zur Strafbarkeit bei Verstößen. Gemäß Art. 99 EHDS erlassen die **Mitgliedstaaten** Vorschriften über Sanktionen, insbesondere für solche, die nicht mit Geldbußgen geahndet werden.

Nach § 9 Abs. 1 **GDNG** wird mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft, wer gegen das Zweckänderungs- und Weitergabe- oder das Reidentifizierungsverbot des § 7 Abs. 1 u. 2 GDNG 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“ (§ 9 Abs. 2 GDNG). Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind neben den Betroffenen auch der Verantwortliche sowie die zuständige Aufsichtsbehörde (§ 9 Abs. 3 GDNG). Diese Norm entspricht der datenschutzrechtlichen Strafnorm in § 42 BDSG, wobei jedoch der Strafrahmen in § 9 Abs. 1 GDNG gegenüber § 42 BDSG im Grundtatbestand geringer ist. Da insofern regelmäßig beide Straftatbestände vorliegen und § 42 BDSG und § 9 GDNG sich gegenseitig konsumieren können, kommt jeweils die Norm mit dem höheren Strafmaß zur Anwendung. Einen Verweis auf § 203 StGB (berufliche Schweigepflicht, Patientengeheimnis) enthält das GDNG nicht.

In den §§ 303a SGB V wird dagegen das **Patientengeheimnis** erwähnt. § 203 StGB soll gemäß § 303e Abs. 4 S. 2, 3 SGB V anwendbar sein, da Nutzungsberechtigte pseudonymer Gesundheitsdaten entweder Personen sein müssen, „die einer Geheimhaltungspflicht nach § 203 des Strafgesetzbuches unterliegen“ oder gemäß dem Verpflichtungsgesetz verpflichtet wurden. Inwieweit § 203 StGB bei der Sekundärnutzung anwendbar ist, ist unklar: Die Regelung setzt voraus, dass die unzulässig offenbarten Daten in der beruflichen Funktion (z. B. als Arzt) anvertraut wurde. Ein Anvertrauen durch den Betroffenen erfolgt im Fall der Sekundärnutzung nicht. § 303e SGB V kann aber nur so verstanden werden, dass mit dem Erteilen der Nutzungsberechtigung auch ein Anvertrauen erfolgt. Gemäß § 77 StGB kann der nach den §§ 205, 77 Abs. 1 StGB Betroffene einen Strafantrag stellen. Die kriminalpolitische Bedeutung von § 203 StGB ist gering. Strafrechtliche Verurteilungen nach dieser Norm sind nicht bekannt. Dies hat zur praktischen Folge, dass der Strafvorschrift des § 203 StGB vor

[169] So die Erfahrung des Netzwerks Datenschutzexpertise, siehe hierzu die unter https://www.netzwerk-datenschutzexpertise.de/dokument/datenschutz-im-gesundheitsbereich dokumentierten Fälle; anders wohl Kühling/Schildbach NZS 2020, 46.

allem Appellfunktion zukommt.[170] Die ist daher nicht geeignet, eine wirksame Garantie i. S. v. Art. 89 Abs. 1 DSGVO zu sein.

Bei jedem **Strafantrag** muss die Antragsfrist von 3 Monaten nach Kenntniserlangung von der Straftat gewahrt werden (§ 77b StGB). Die Gesetzesbegründung zum GDNG verweist auf das große Schadenspotenzial durch die Tatbegehung des § 9 GDNG.[171] 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 dann regelmäßig 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 Offizialdelikte auszugestalten.

14.2 Bußgelder

Art. 64 EHDS nennt die Voraussetzungen für die Verhängung von Bußgeldern durch die **Zugangsstellen**. Verstöße gegen Art. 60 u. 61 EHDS, in denen die Pflichten für Dateninhaber und Datennutzer festgelegt sind, werden mit Geldbußen in Höhe von maximal 10 Mio. Euro bzw. 2% des Jahresumsatzes eines Unternehmens sanktioniert (Art. 64 Abs. 2 EHDS). Maximal 20 Mio. Euro bzw. 4% des Jahresumsatzes können als Bußgeld bei einigen als schwerer eingestuften Verstößen verhängt werden. Hierzu gehört das Datenextrahieren aus einer sicheren Verarbeitungsumgebung sowie die Re-Identifizierung pseudonymer Gesundheitsdaten (Art. 64 Abs. 5 EHDS).

Erfolgt mit einem Verstoß gegen den EHDS zugleich ein Verstoß gegen die DSGVO, so ist hierfür die **Datenschutzaufsichtsbehörde** zuständig, die ein Bußgeld nach Art. 83 DSGVO erlässt (Art. 65 EHDS).

Das GDNG und die §§ 303a ff. SGB V sehen keine Bußgeldsanktionen vor. Dies bedeutet, dass es bis zum Wirksamwerden des EHDS keine spezifischen Bußgeldtatbestände gibt. Wohl aber sind Datenschutzverstöße im Rahmen der Sekundärnutzung von Gesundheitsdaten in jedem Fall **Verstöße i. S. v. Art. 83 DSGVO**, so dass auch schon aktuell die Datenschutzaufsichtsbehörden entsprechende Bußgelder verhängen können.

[170] Dittrich/Dochow/Ippach, in Dittrich/Dochow/Ippach, Kap. 2 Rn. 60 (S. 42).
[171] BT-Drs. 20/9046 (= BR-Drs. 434/23), 58.

14.3 Sonstige Sanktionen

Als zusätzliche Sanktion für den Fall eines Verstoßes gegen die Nutzungsvorgaben von FDZ-Daten ist vorgesehen, dass die zuständige Datenschutzbehörde hierüber und über die ergriffenen Sanktionen (Art. 58 Abs. 2 lit. b-j DSGVO) **das FDZ informiert**, was zur Folge hat, dass der Nutzungsberechtigte vom FDZ für bis zu zwei Jahre vom Datenzugang ausgeschlossen wird (§ 303e Abs. 6 SGB V).

Verstöße gegen den Datenschutz geben einen Hinweis auf eine fehlende Unzuverlässigkeit eines Datennutzers. Dass insofern ein Nutzungsausschluss nur bis maximal zwei Jahre vorgesehen ist, ist schwer zu erklären, zumal ein Verstoß ein Hinweis darauf sein dürfte, dass der Datennutzer unzuverlässig ist. Dies muss im Fall eines später erfolgenden Antrags in jedem Fall berücksichtigt werden. Unabhängig davon ist die Frage, wie lange die **Speicherdauer zu Datenschutzverstößen** von Datennutzern der Zugangsstelle für künftige Genehmigungsverfahren sein soll. Zwei Jahre sind insofern zu kurz bemessen; ein Vorhalten von mindestens zehn Jahren ist in solchen Fällen nötig, wobei die Frist von der Art und Schwere des Datenschutzverstoßes abhängig gemacht werden kann.

15 Ergebnis

Aus der Darstellung und der Analyse der heute schon sowie der künftig geltenden Regelungen zur Sekundärnutzung von Gesundheitsdaten ergeben sich in vieler Hinsicht Unklarheiten, Widersprüche und aus Grundrechtssicht Ergänzungsnotwendigkeiten. So berechtigt die Erwartungen an eine verbesserte Sekundärnutzung sind, so problematisch wäre nach dem aktuellen Recht die praktische Anwendung. Hieran ändert sich auch nichts durch den Umstand, dass die nationalen Regeln erkennbar nur Übergangsrecht sein sollen und noch keine umfassende Umsetzung des erst in mehr als 4 Jahren wirksam werdenden EHDS bezwecken. Es ist sinnvoll, eine Reform wie die der Gesundheitsdatennutzung sukzessive und modular vorzunehmen. Dabei ist es aber wichtig, **von Anfang an die vom Verfassungs- und vom Europarecht gesetzten Standards** zu beachten.

Die **geltenden Regelungen im GDNG und im SGB V** weisen Defizite auf. Das GDNG gilt als Rahmengesetz eigentlich allgemein, die Normen des SGB V regeln nur informationelle Eingriffe bei gesetzlich Versicherten. Die Defizite werden durch die geplante FDZGesV nicht behoben. Die grundrechtlichen Defizite des aktuell geltenden deutschen Rechts sind erheblich; die Vorgaben des EHDS sind insofern erheblich grundrechtsfreundlicher. Doch muss auch der EHDS im Hinblick auf die durch ihn ausgelöste massive Beeinträchtigung der Vertraulichkeit von Gesundheitsdaten auf den Grundrechts-Prüfstand gestellt werden. Auch insofern ist es von größter Bedeutung, dass im Vorfeld des Wirksamwerdens des EHDS die deutschen Gesetzgeber Recht und Praxis der Sekundärnutzung von Gesundheitsdaten grundrechtsfreundlich gestalten.

Folgende **Änderungen** sind dringend geboten[172]:

1. Es muss aus Gleichheitsgründen gewährleistet werden, dass informationelle Eingriffe für gesetzlich Versicherte nicht im einem größeren Maß erlaubt werden als für sonstige Menschen, etwa privat Versicherte (5.1).
2. Gesundheitsdaten mit Bezug zu psychischen Leiden und zur sexuellen Orientierung bedürfen rechtlich einer Schutzverstärkung (5.6, 5.7).
3. Die im FDZ vorgesehene pauschale Aufbewahrungsfrist von 100 Jahren bedarf zumindest einer Differenzierung und einer jeweils hierfür tragfähigen Begründung (5.8).
4. Es bedarf einer operativ handhabbaren Konkretisierung des Forschungsbegriffs, um privilegierte Sekundärnutzungen von weniger bedeutsamen abzugrenzen und bei Letzteren sicherzustellen, dass keine pseudonymisierten Einzeldatensätze zum Einsatz kommen (7.2, 7.5).
5. Es bedarf für die Gemeinwohlklausel des GDNG einer handhabbaren Operationalisierung (7.1).
6. Mit einem gesetzlichen Nutzungsgeheimnis oder zumindest einem Forschungsgeheimnis muss rechtssicher klargestellt werden, dass primär dem Patientengeheimnis unterliegende Daten nicht im Rahmen der Sekundärnutzung für Strafverfolgungszwecke verwendet werden können (8).
7. Es ist gesetzlich sicherzustellen, dass Sekundärnutzungen nur für Personen genehmigt werden, die hinreichende Nachweise für ihre Zuverlässigkeit und Qualifikation vorlegen (9.2).
8. Es muss gesetzlich sichergestellt werden, dass die Zugangsstellen bei ihrer Aufgabenwahrnehmung unabhängig und hinreichend qualifiziert sind (10.2, 10.3).
9. Bei Zugangsanträgen sollte die Vorlage eines validen Datenschutzkonzeptes verpflichtend gemacht werden.
10. Die Transparenz des Antrags-, Genehmigungs- und Bereitstellungsverfahrens sowie der konkreten Datennutzung muss so verbessert werden, dass Betroffene erkennen können, ob und inwieweit sie von Auswertungsprojekten betroffen sind (10.6, 10.7).
11. Nach Abschluss einer Sekundärnutzung müssen die Ergebnisse für die Allgemeinheit offengelegt werden (10.7).
12. Es muss ein Verfahren zur Wahrnehmung der Betroffenenrechte einschließlich des Auskunftsrechts in Bezug auf die pseudonymisierten Sekundärdatensätze etabliert werden (12).
13. Eine differenziertere Widerspruchsmöglichkeit für Betroffene wäre wünschenswert (12.4).
14. Es bedarf spezifischer Regelungen zur Sicherung eines Anspruchs auf Rückmeldung sowie des Rechts auf Nichtwissen (12. 5).

[172] Siehe auch Weichert ZfME 2025, 84 f.

15. Zur Gewährleistung wirksamer Datenschutzkontrollen ist eine institutionalisierte Organisation hierfür einzurichten (13.1).
16. Die Strafvorschriften sind als Offizialdelikte umzugestalten und mit den bestehenden Strafrechtsnormen abzustimmen (14.1).
17. Als zusätzliche Sanktionsmöglichkeit ist vorzugesehen, dass Personen von einer Datennutzung auch langfristig ausgeschlossen werden können (14.3).

Literatur

Augsberg, Steffen/Düwell, Marcus/Müller, Benjamin (Hrsg.), Datenzugangsregeln, 2024, https://zevedi.de/wp-content/uploads/2024/10/Datenzugangsregeln.pdf.

Bernhardt, Ute/Ruhmann, Ingo/Weichert, Thilo, EHDS – der Europäische Gesundheitsdatenraum, DANA 1/2023, 17-25 = Gutachten v. 27.02.2023, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2023_02_ehds.pdf.

Bieresborn, Dirk, Sekundärverwertung von Gesundheitssozialdaten zu Forschungszwecken – Datenschutz gegen Menschenwohl? 30.11.2023, Gesundheitsrecht.blog Nr. 33, 2023, https://gesundheitsrecht.blog/sekundaerverwertung-gesundheitssozialdaten/.

Bretthauer, Sebastian/Spiecker gen. Döhmann, Indra, Das Digitale-Versorgung-Gesetz als Einfallstor für eine Neujustierung von einstweiligem Rechtsschutz vor dem BVerfG und der Eingriffsqualität bei Datenverwendungen, JZ 2020, 990.

Buchholz, Gabriele/Schmalhorst, Louisa/Brauneck, Alissa, Der Gesetzgeber im Spannungsfeld zwischen Patientensouveränität und Forschungsinteressen – eine Bewertung der neuesten Gesetzgebungsaktivitäten auf EU-Ebene und nationaler Ebene, MedR 2024, 471-476.

Däubler, Wolfgang/Wedde, Peter/Weichert, Thilo/Sommer, Imke, EU-DSGVO und BDSG, 3. Aufl. 2024.

Dittrich, Tilmann/Dochow, Casten/Ippach; Jan (Hrsg.), Rechtshandbuch Cybersicherheit im Gesundheitswesen, 2024.

Dochow, Carsten, Grundlagen und normativer Rahmen der Telematik im Gesundheitswesen, 2017.

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), Stellungnahme v. 14.08.2023 zum Gesundheitsdatennutzungsgesetz – GDNG (GDNG-Stellungnahme), https://www.datenschutzkonferenz-online.de/media/st/23_08_14_DSK_Stellungnahme_GDNG-E.pdf.

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), Nutzung von Gesundheitsdaten braucht Vertrauen – Der Europäische Gesundheitsdatenraum darf das Datenschutzniveau der Datenschutz-Grundverordnung nicht aushöhlen (EHDS-Stellungnahme) v. 27.03.2023, https://datenschutzkonferenz-online.de/media/st/2023-03-27_DSK-Stellungnahme_EHDS.pdf.

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten

in der wissenschaftlichen Forschung, Entschließung v. 24.11.2022 (Petersberger Erklärung), https://www.datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf.

Kühling, Jürgen/Buchner, Benedikt (Hrsg.), DS-GVO BDSG Kommentar, 4. Aufl. 2024.

Kuss, Christian/Langenheim, Niccolo, Die Weiterverarbeitung von Gesundheitsdaten nach dem GDNG, CR 2024, 791-798.

Pöttgen, Nicole, Medizinische Forschung und Datenschutz, 2009.

Schneider, Uwe K., Sekundärnutzung klinischer Daten – Rechtliche Rahmenbedingungen, 2015, https://library.oapen.org/bitstream/handle/20.500.12657/39362/sekundarnutzung-klinischer-daten-rechtliche-rahmenbedingungen.pdf?sequence=1&isAllowed=y.

Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hrsg.), Datenschutzrecht, 2. Aufl. 2025.

Weichert, Thilo, Informed Consent und Datenschutz im Forschungskontext – Entwicklungen und deren Grenzen, ZfME 71 (2025), 70-87.

Weichert, Thilo, Gesundheitsdatennutzung ohne Datenschutz? DANA 2/2024, 66-73.

Weichert, Thilo, Gesundheitsdatennutzung contra heilberufliche Vertraulichkeit, GuP 2023, 183-188.

Weichert, Thilo, Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung, 2022 (Rahmenbedingungen), https://www.mwv-open.de/site/books/10.32745/9783954667000/download/8417/.

Weichert, Thilo, Gesundheitsreform – Einstieg in die pseudonyme Datenverarbeitung? DANA 4/1999, 21-24.

Abkürzungen

ABl.	Amtsblatt
Abs.	Absatz
AfD	Alternative für Deutschland
Art.	Artikel
Aufl.	Auflage
AufenthV	Aufenthaltsverordnung
BDSG	Bundesdatenschutzgesetz
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BMG	Bundesministerium für Gesundheit
BR-Drs	Bundesratsdrucksache
BReg	Bundesregierung
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
CR	Computer und Recht (Zeitschrift)
DANA	DatenschutzNachrichten
DGA	Data Governance Act
DKS	Datenzugangs- und Koordinierungsstelle
DSGVO	Europäische Datenschutz-Grundverordnung
DSK	Konferenz der Datenschutzbeauftragten des Bundes und der Länder
DSRL-JI	Datenschutzrichtlinie für Justiz und Inneres
DuD	Datenschutz und Datensicherheit (Zeitschrift)
DVG	Digitale Versorgung Gesetz
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EHDS	European Health Data Space – Europäischer Gesundheitsdatenraum
ePA	Elektronische Patientenakte
ErwGr	Erwägungsgrund
EU	Europäische Union
EuGH	Europäischer Gerichtshof
FDP	Freie Demokratische Partei
FDZ	Forschungsdatenzentrum Gesundheit
FDZGesV-E	Entwurf einer Forschungsdatenzentrum Gesundheit Verordnung
f/f.	fort-/folgend
G.	Gesetz
GDNG	Gesundheitsdatennutzungs-gesetz
GenDG	Gendiagnostikgesetz
GesR	Gesundheitsrecht (Zeitschrift)
GG	Grundgesetz
GKV	Gesetzliche Krankenversicherung
GRCh	Europäische Grundrechte-Charta
GuP	Gesundheit und Pflege (Zeitschrift)
GRCh	Europäische Grundrechte-Charta
HBDI	Der Hessische Beauftragte für Datenschutz und Informationsfreiheit
insbes.	insbesondere
i. V. m.	in Verbindung mit
JZ	Juristenzeitung
LfD/I	Landesbeauftragter für Datenschutz/und Informationsfreiheit
lit.	Buchstabe
LVerfG	Landesverfassungsgericht
MedR	Medizinrecht (Zeitschrift)
M. w. N.	mit weiteren Nachweisen
MBOÄ	Musterberufsordnung der Ärztekammern
MVVerfG	Verfassungsgericht Mecklenburg-Vorpommern

NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NStZ-RR	Neue Strafrechtszeitung Rechtsprechungsreport
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZS	Neue Zeitschrift für Sozialrecht
RL	Richtlinie
Rn.	Randnummer
RDV	Recht der Datenverarbeitung (Zeitschrift)
RStGB	Reichsstrafgesetzbuch
S.	Satz/Seite
SächsVerfGH	Sächsischer Verfassungsgerichtshof
SGB	Sozialgesetzbuch
s. o.	siehe oben
StGB	Strafgesetzbuch
STPO	Strafprozessordnung
s. u.	siehe unten
u.	und
u. a.	unter anderem/und andere
UAbs.	Unterabsatz
u. Ä.	und Ähnliches
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
v.	von
VerwArch	Verwaltungsarchiv (Zeitschrift)
VG	Verwaltungsgericht
vgl.	vergleiche
z. B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZfME	Zeitschrift für medizinische Ethik