Typoskript im Sinne des § 38 Abs. 4 UrhG;
das Original ist abgedruckt in NJW 2020, S. 3573 ff.

DER GLÄSERNE PATIENT: DYSTOPIE ODER ZUKUNFTSREALITÄT?

DATENGETRIEBENE GESUNDHEITSFORSCHUNG UNTER DER DSGVO UND DEM DIGITALE-VERSORGUNG-GESETZ

PROF. DR. MARIO MARTINI/MATTHIAS HOHMANN*

Datengetriebene Forschung gehört zu den wichtigsten Hoffnungsträgern der Medizin. Sie bewegt sich in einem Spannungsfeld zweier konfligierender Pole: Einerseits genießen Gesundheitsdaten besonderen Schutz (vgl. Art. 9 Abs. 1 DSGVO). Anderseits ist die Medizinforschung auf eine Privilegierung ihrer Datenverarbeitungen angewiesen, um ihre Ziele wirksam erreichen zu können. Wie sich dieser Antagonismus auflösen lässt, damit Big Data auch im Forschungsbereich sein Potenzial voll entfalten kann, ohne im gleichen Atemzug den Einzelnen als gläsernen Patienten seiner Intimsphäre zu berauben, gehört zu den offenen Rätseln unserer Zeit. Der Beitrag beteiligt sich an der Lösungssuche.

Von der Digitalisierung des Gesundheitswesens geht eine verlockende Verheißung aus: Gigantische Datenhalden und softwarebasierte Analyseinstrumente sollen die Grundlage für maßgeschneiderte Therapieansätze und innovative Behandlungsmethoden legen. Mit Hilfe hochwertiger Daten und Künstlicher Intelligenz – so die Hoffnung – lässt sich die medizinische Versorgung der Bevölkerung auf eine höhere Stufe heben. Diese Erwartungen sind nicht unbegründet: Je stärker der Einzelne und die Gesellschaft im digitalen Zeitalter Gesundheitsdaten erfassen, umso schneller wächst auch das Analyse- und Auswertungspotenzial des üppigen Datenschatzes.

Bahnbrechende Erfolge kann Künstliche Intelligenz u. a. bei der Diagnose von Hautkrebs[1] sowie bei der Brustkrebsfrüherkennung[2] erzielen. Algorithmen erkennen Tumore schnell und treffsicher anhand von CT-Bildern; sie identifizieren sogar Helligkeitsverteilungen innerhalb des Tumors, die sich dem bloßen Auge verschließen. Bundesgesundheitsminister *Jens Spahn* träumt gar bereits davon, „*dass wir in zehn bis 20 Jahren den Krebs besiegt haben*".[3] Aber auch der Bekämpfung des Corona-Virus setzen Forscher bereits erfolgreich auf Methoden maschinellen Lernens, um anhand von CT-Scans Infektionen zu erkennen[4] – ebenso bei so genannten seltenen Krankheiten, die viele Ärzte nur aus Büchern kennen. Algorithmen können dort im Idealfall gemeinsam mit großen Datensätzen zur zuverlässigen Diagnose sowie zu zielgerichteten Therapien wirksam beitragen und Betroffenen dadurch eine lange Odyssee mit vielen Fehldiagnosen ersparen.

In den Augen des Pessimisten lässt diese intensive Auswertung von Gesundheitsdaten demgegenüber unaufhörlich das dystopische Szenario einer Zukunft näher rücken, in der der Mensch nur noch als eine bloße Datenquelle fungiert und zum gläsernen Patienten mutiert. Denn jede noch so fortschrittliche Auswertungsmethode ist auf eine möglichst umfassende Basis von Patientendaten angewiesen.

In diesem Spannungsbogen zwischen Utopie und Dystopie hat der deutsche Gesetzgeber mit dem „Digitale-Versorgung-Gesetz" (DVG) unterdessen einen Vorstoß unternommen, um das Gesundheitssystem für datengetriebene Innovationen zu öffnen.[5] Das DVG soll Gesundheitsdaten für Forschungszwecke stärker nutzbar machen. Als Kernbaustein entwickelt das Gesetz die bisherige Datenaufbereitungsstelle, die sich allein für die Daten aus dem so genannten morbiditätsorientierten Risikostrukturausgleich[6] verantwortlich zeichnete, zu einem Forschungsdatenzentrum weiter: Bei ihm sollen sämtliche Abrechnungsdaten der gesetzlichen Krankenversicherungen (vermittelt über den Spitzenverband Bund der Krankenkassen [GKV]) in einem zentralen Datenpool zusammenfließen – ohne die Einwilligung der Versicherten (vgl. § 303b Abs. 3 SGB V). Das Forschungsdatenzentrum bereitet die zusammengeführten Leistungsdaten in der Folge auf, um sie auf Antrag der Forschung zur Verfügung zu stellen (§ 303d Abs. 1 Nr. 4 SGB V n. F.).

---

* *Mario Martini* ist Lehrstuhlinhaber an der DUV Speyer und Leiter des Programmbereichs „Transformation des Staates in Zeiten der Digitalisierung" am Deutschen Forschungsinstitut für öffentliche Verwaltung. *Matthias Hohmann* war dort Forschungsreferent. Der Aufsatz fasst zentrale Erkenntnisse einer Monographie zum Thema zusammen, die die Autoren gegenwärtig bearbeiten.

[1] *Esteva/Kuprel* et al., Nature 542 (2017), 115 ff.

[2] *Pisano*, Nature 577 (2020), 35 ff.

[3] *Bröcker/Quadbeck*, Jens Spahn sieht gute Chancen, dass Krebs in 20 Jahren besiegt ist, RP ONLINE v. 1.2.2019.

[4] *Xu/Jiang* et al., Deep Learning System to Screen Coronavirus Disease 2019 Pneumonia, 2020.

[5] Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz - DVG) vom 09.12.2019 (BGBl. I 2019, 2562). Vgl. zum Regelungsgehalt auch *Kühling/Schildbach*, NZS 2020, 41 ff.

[6] Er stellt einen Finanzausgleich zwischen den gesetzlichen Krankenversicherungen her, der den Divergenzen in der Risikostruktur der Mitglieder Rechnung trägt (vgl. § 266 f. SGB V).

Die Breitenwirkung der Maßnahmen ist beträchtlich, betreffen sie doch jeden der rund 72,9 Mio. gesetzlich krankenversicherten Bürger. Es überrascht daher nicht, dass das Gesetz eine Kontroverse politische Diskussion entflammte.[7] In den Augen der einen unternimmt der Gesetzgeber einen längst überfälligen Schritt in Richtung einer digitalen Gesundheitsvorsorge. Für die anderen opfert er den Datenschutz auf dem Altar der Innvovationsgläubigkeit, um einer unreflektierten Technikeuphorie zu huldigen.

I. Faktische und normative Anonymisierung im Gesundheitsdatenschutz

Seine Gesundheitsdaten stellt der Einzelne im Zweifel dann gerne unbekümmert in den Dienst der Gemeinschaft, wenn er davon ausgehen kann, dass diese zuverlässig anonymisiert sind. Anonymisiert sind Daten – entgegen verbreiteter Meinung – aber nicht schon dann, wenn der Name, die Anschrift und das Geburtsdatum als identifizierende Merkmale herausgetrennt sind. Anonym sind sie nach dem Maßstab der DSGVO vielmehr erst dann, wenn ihnen *jeder* auch nur potenzielle Personenbezug fehlt:[8] Es muss mit hinreichender Sicherheit feststehen, dass kein Rückschluss auf irgendeine konkrete Person möglich ist. Die DSGVO kennt insoweit auch kein erlaubtes, subjektives Risiko. Weisen Daten objektiv aus der Ex-ante-Perspektive ein Personenbezug auf, dann kann sich der Verantwortliche daher nicht darauf berufen, dass er nicht die Absicht hatte, bestimmte Personen zu identifizieren.[9] Es genügt schon, dass ein Dritter über das notwendige (Zusatz-)Wissen verfügt, um Daten mit verhältnismäßigen Mitteln einer bestimmten Person zuzuordnen (sog. relativer Personenbezug).[10] Verantwortliche müssen deshalb bspw. auch das Risiko eines Datenlecks oder Hackerangriffs berücksichtigen, wenn sie das (Re-)Identifikationspotenzial ihrer Datenbestände bewerten.

1. Autonomes Konzept einer rechtlichen Anonymisierung

Im Big-Data-Zeitalter lässt sich im Behandlungskontext nahezu jedem Datum ein Personen- oder gar ein Gesundheitsbezug abringen. Insbesondere medizinische Daten, etwa ein Blutbild oder ein EKG-Verlauf, sind so individuell, dass sich der Bezug zur ursprünglichen Person technisch nicht gänzlich aufheben lässt.[11] Gerade die unerkannten Verknüpfungsmöglichkeiten und damit die für Menschen nicht ersichtlichen Identifikatoren sind es, die das Fundament des neuen Analysepotenzials bilden. Unter diesen Prämissen verkommt die Vorstellung einer vollständigen technischen Anonymisierung zunehmend zur Illusion. Das heißt aber auch: Medizinforscher müssen im Zweifel immer davon ausgehen, dass sie mit personenbezogenen

---

[7] Vgl. nur *Fuest/Turzer,* Die Angst vor dem gläsernen Patienten, Welt.de v. 10.11.2019.
[8] *Ernst,* in *Paal/Pauly,* DSGVO, 2. Aufl. (2018), Art. 4 DSGVO Rn. 9; *Karg,* in *Simitis/Hornung/Spiecker gen. Döhmann,* DSGVO/BDSG, 2019, Art. 4 Nr. 1 DSGVO Rn. 57; *Roßnagel*, ZD 2019, 157 (159).
[9] *Ernst* (o. Fußn. 14), Rn. 13; *Schild* (o. Fußn. 14), Rn. 18.
[10] So grundsätzlich EuGH, ECLI:EU:C:2016:779, Rn. 49 – Breyer; vgl. auch *Martini/Weinzierl*, NVwZ 2017, 1251 (1252 f.); *Schantz*, NJW 2016, 1841 (1842 f.). A. A. *Albrecht/Jotzo,* Das neue Datenschutzrecht der EU, 2017, Teil 3, Rn. 3.
[11] Grundlegend *Ohm*, UCLA Law Review 2010, 1701-1776 (1716 ff.); vgl. auch *Deutscher Ethikrat,* Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, 30.11.2017, S. 140; *Niemann/Kevekordes*, CR 2020, 17 (18 f.).

Daten hantieren, selbst wenn nicht sie selbst, sondern erst ein Dritter Rückschlüsse auf die Identität einzelner Personen ziehen können (vgl. auch ErwGrd. 26 S. 3 DSGVO: „*von dem Verantwortlichen oder einem Dritten*"). Im Gesundheitsbereich gibt es im Grundsatz daher keine anonymen Daten mehr.

Der Unionsgesetzgeber läuft dadurch Gefahr, das Potenzial datengetriebener Medizinforschung im Korsett datenschutzrechtlicher Regulierung zu ersticken. *Pro futuro* sollte er die Möglichkeit einer *rechtlichen* Anonymisierung jenseits einer rechtlichen Anonymisierung schaffen. Sie sollte das datenschutzrechtliche Korsett dort lockern, wo Verantwortliche eine technische De-Anonymisierung zwar nicht mit abschließender Sicherheit ausschließen können, einen unbefugten Zugriff und die (Re-)Identifizierung betroffener Patienten aber durch technisch-organisatorische Sicherungsmaßnahmen hinreichend zuverlässig verhindern.[12]

Regulatorisch umsetzbar ist ein solches normatives Verständnis „anonymisierter Daten" etwa in Gestalt einer widerlegbaren Vermutung, die Daten unter spezifischen technischen Voraussetzungen – etwa dem Einsatz konkret benannter Anonymisierungstechniken nach dem aktuellen Stand der Technik – keinen Personenbezug mehr zuspricht. Wer die Daten gleichwohl einer Reidentifizierung zuführt, sieht sich dann einer hohen rechtlichen Sanktion, insbesondere Datenzugangsverboten, berufsrechtlichen Sanktionen und Straftatbeständen, ausgesetzt. Auf diese Weise bezieht der Unionsgesetzgeber den Nutzer sensibler Daten stärker in die Mitverantwortung ein und ebnet dadurch innovativen Forschungsansätzen den Weg, ohne die datenschutzrechtlichen Interessen der Betroffenen zu konterkarieren.

In Richtung einer solchen normativen Auflösung des Personenbezugs tastet sich auf nationaler Ebene das DVG vor. Es implementiert eine umfassende, mehrfache Pseudonymisierung mit Hilfe einer eigenständigen Vertrauensstelle. Diese erweiterte Pseudonymisierung soll sicherstellen, dass niemand – allen voran nicht die späteren wissenschaftlichen Nutzer der Daten – aus den Datensätzen auf die Identität des einzelnen Versicherten schließen kann (vgl. § 303c Abs. 2 S. 2 SGB V).[13] Ergänzend erlegt der Gesetzgeber den Nutzern der Daten ein strafbewehrtes Re-Identifizierungsverbot auf: Es untersagt ihnen insbesondere die bereitgestellten Daten zu verarbeiten, um einen Personenbezug herzustellen (§ 303e Abs. 5 S. 4 SGB V).[14] Dieser Ansatz einer mehrfachen Pseudonymisierung durch voneinander unabhängige öffentliche Stellen mit umfassendem Re-Identifizierungsverbot und Sanktionen (§ 303e Abs. 6 S. 2 SGB V) kann dem unionalen Datenschutzrecht eine regulatorische Blaupause liefern.

---

[12] Ähnlich auch *Hornung/Wagner*, CR 2019, 565 (573 f.). Grundlegend zu diesem Ansatz *Schwartz/Solove*, New York University Law Review 86 (2011), 1814 (1866 ff.).
[13] Vgl. *Kühling/Schildbach*, NZS 2020, 41 (46).
[14] Vgl. zum Kontext dieser Regelungen im Sozialdatenschutz *Kühling/Schildbach*, NZS 2020, 41 (46).

2. Unionale Implementierung eines Datentreuhandmodells

Dem besonderen Bedürfnis, in einer Welt wachsender Verknüpfungs- und schwindender Anonymisierungsmöglichkeiten wirksamen Vertrauensschutz für Gesundheitsdaten herzustellen, sollte die Union durch einen Regulierungsrahmen für ein Datentreuhandmodell Rechnung tragen [15] – und dadurch den Anstoß dafür liefern, langfristig europäische Datentreuhänder zu etablieren, die über die Grenzen der Mitgliedstaaten hinweg sowohl den digitalen Binnenmarkt als auch einen europäischen Raum der Forschung (vgl. Art 179 AEUV) mit Leben füllen. Ein Datentreuhänder tritt dann als unabhängige Instanz zwischen Datengeber und Datennutzer, um Daten sicher in einer Weise zu vermitteln, welche deren Vertraulichkeit und Integrität hinreichend wahrt. Seine Aufgabe ist es, Zugriffsrechte zu verwalten und als vertrauenswürdiger Makler sicherzustellen, dass die Vereinbarungen über zulässige Datennutzungen gewahrt bleiben. Ärzte und Krankenhäuser können ihren Patienten in diesem Modell rechtssicher die Möglichkeit eröffnen, Gesundheitsdaten an einen Datentreuhänder zu übermitteln und damit der Forschung zur Verfügung stellen, ohne sich selbst dem Risiko eines Datenschutzverstoßes auszusetzen.

Um sowohl das Vertrauen der Datengeber als auch der -nutzer zu rechtfertigen, sollte der Datentreuhänder offenlegen müssen, aus welchen Quellen er welche Daten erhält, an wen er diese Daten zu welchen Zwecken herausgeben möchte und welche Maßnahmen er zur Datensicherheit ergreift. Jede Übermittlung von Daten sollte er präzise und manipulationssicher dokumentieren müssen, damit Aufsichtsbehörden das Schicksal der Daten zuverlässig nachvollziehen können. Ein Datentreuhänder sollte nicht nur ein Zertifizierungs- oder Auditierungsverfahren durchlaufen, sondern auch während des laufenden Betriebs strengen Kontroll- und Berichtspflichten gegenüber einer Aufsichtsstelle unterliegen.

II. Forschungsbezogene Verarbeitungsbefugnisse der DSGVO

Wer personenbezogene Daten rechtmäßig verarbeiten will, ist dafür auf eine Rechtsgrundlage angewiesen. Für Gesundheitsdaten [16] legt die DSGVO die Messlatte besonders hoch: Der Unionsgesetzgeber stellt ihre Verarbeitung nicht allein unter den allgemeinen Zulassungsvorbehalt des Art. 6 DSGVO. Es unterwirft es vielmehr dem strengen Verarbeitungsverbot des Art. 9 Abs. 1 DSGVO. Der Verantwortliche kann es nur mithilfe einer ausdrücklichen Einwilligung (1.) oder unter den hohen Voraussetzungen eng gesteckter Erlaubnistatbestände (2.) überwinden.

---

[15] Zum Modell einer Vertrauensstelle im Recht der gesetzlichen Krankenversicherung: § 303a und § 303c SGB V i. V. m. der Datentransparenzverordnung. Vgl. auch *Deutscher Ethikrat* (o. Fußn. 17), S. 279. Zur Umsetzbarkeit eines solchen Modells im Kontext der elektronischen Patientenakte *Molavi/Kolain* (o. Fußn. 19), S. 63 ff.

[16] Den Gesundheitsbezug will der Unionsgesetzgeber im Grundsatz weit verstanden wissen. Vgl. Art. 4 Nr. 15, ErwGrd 35 S. 1.

1. Die Einwilligung als normatives Leitbild digitaler Souveränität

Die Einwilligung als unmittelbarer Ausdruck einer autonomen Willensbetätigung des Betroffenen soll in dem normativen Konzept der DSGVO eigentlich eine wichtige Rolle einnehmen, um die Verarbeitung von Daten zu legitimieren (vgl. Art. 9 Abs. 2 lit. a DSGVO).

Die strukturellen Voraussetzungen, unter denen Gesundheitsbehandlungen erfolgen, engen den realen Anwendungsradius einer wirksamen Einwilligung jedoch substanziell ein: Das Beziehungsgefüge zwischen Arzt und Patient ist typischerweise durch ein strukturelles informatorisches Ungleichgewicht, nicht selten gar ein Abhängigkeitsverhältnis geprägt. Das kann die Freiwilligkeit der Einwilligung infrage stellen (Art. 7, ErwGr. 43 S. 1 DSGVO).[17] Auch eine unspezifische Pauschaleinwilligung, die der Arzt dem Patienten etwa als Teil der Behandlungsvereinbarung zur Unterschrift vorlegt, genügt den Anforderungen der DSGVO nicht. Vielmehr muss der Arzt – parallel zu den medizinischen Aufklärungspflichten – den Betroffenen umfassend über Zweck und Nutzen der Verarbeitung seiner personenbezogenen Daten in Kenntnis setzen.

Im Spannungsverhältnis zwischen zu weiten (und daher unzulässigen) und zu engen (und daher unpraktikablen) Verarbeitungszwecken erlaubt die DSGVO immerhin bereits die Einwilligung in „*bestimmte Bereiche wissenschaftlicher Forschung*“ (ErwGr 33 S. 2 DSGVO). De lege ferenda sollte der Unionsgesetzgeber diesen programmatischen Ansatz als „*Broad Consent*“-Zulässigkeitstatbestand festschreiben, d. h. den unbestimmten Begriff des „*bestimmte[n] Bereich[s] wissenschaftlicher Forschung*“ durch konkrete Beurteilungskriterien für ausgewählte Formen der wissenschaftlichen Datenerhebung operationalisierbar machen. Für solche Detailregelungen empfiehlt sich das Instrument nachgelagerter delegierter Rechtsakte (Art. 290 AEUV). Eine kontextspezifische Präzisierung könnte dem technischen Konzept einer *dynamischen Einwilligung* etwa in Gestalt einer sog. Einwilligungskaskade oder Meta-Einwilligung die legislatorische Grundlage bereiten.[18] Im Kontext der Medizinforschung wäre es Patienten, die ihre Gesundheitsdaten der Forschung zur Verfügung stellen wollen, dann einfacher möglich, z. B. über ein Datencockpit[19] gezielt in die Verarbeitung ihrer Daten für bestimmte Forschungsvorhaben einzuwilligen und nachzuvollziehen, was mit ihren Daten geschieht.

Technisch wird die elektronische Patientenakte insoweit neue Möglichkeiten eröffnen, Daten weiterzugeben. Regulatorisch weist der Entwurf des „Patientendaten-Schutz-Gesetz (PDSG)“ der Bundesregierung vom 27. April 2020[20] in diese Richtung: Der neu gefasste § 366 SGB V sieht ausdrücklich vor, dass Versicherte die Daten ihrer elektronischen Patientenakte als

---

[17] Eine weitere Grenze zieht zu Recht das sog. Kopplungsverbot klar (vgl. 7 Abs. 4 DSGVO): Der Arzt darf eine Behandlung nicht davon abhängig machen, dass der Betroffene in eine Datenverarbeitung einwilligt, die für die Behandlung nicht erforderlich ist – etwa eine Weitergabe der Patientendaten an die Forschung.
[18] Zu diesen Konzepten *Deutscher Ethikrat* (o. Fußn. 17), S. 183 ff. m. w. N.
[19] Ein Datencockpit vermittelt dem Einzelnen einen Überblick darüber, welche Daten gespeichert sind sowie auf welche Daten welche Instanz zu welchem Zeitpunkt zugegriffen hat.
[20] BT-Drs. 19/18793.

„Datenspende“ freiwillig der medizinischen wissenschaftlichen Forschung zur Verfügung stellen können.

Eine Achillesferse für den Einsatz der Einwilligung im praktischen Forschungskontext aber bleibt: Der Betroffene kann sie *jederzeit widerrufen* (Art. 7 Abs. 3 S. 1 DSGVO). Mit dieser Erklärung droht dann die Grundlage dafür wegzubrechen, dass der Verantwortliche (weiterhin) auf die Daten zugreifen darf. Bei größeren Investitionen in Datenanalysen mit zahlreichen Betroffenen macht das die Einwilligung als Instrument wenig praktikabel. Forscher sind daher im Zweifel besser beraten, bei umfassenden Auswertungen unmittelbar auf eine gesetzliche Verarbeitungsbefugnis zurückzugreifen.

2. Gesetzliche Verarbeitungsbefugnisse

Die Öffnungsklausel des Art. 9 Abs. 2 lit. j DSGVO ermöglicht es den Mitgliedstaaten in weitem Umfang, gesetzliche Verarbeitungsbefugnisse für „wissenschaftliche Forschungszwecke“ aus der Taufe zu heben. Diese legitimieren Forscher, Gesundheitsdaten (auch ohne die Einwilligung der Betroffenen) zu verarbeiten. Aller Betonung des hohen Schutzniveaus im Gesundheitsbereich zum Trotz räumt die DSGVO Forschungsinteressen dadurch umfassenden Vorrang gegenüber den datenschutzrechtlichen Interessen der Betroffenen ein.

a) Der Forschungsbegriff der DSGVO

Der Forschungsbegriff des Art. 9 Abs. 2 lit. j DSGVO ist im Lichte des Art. 13 GrCh weit zu verstehen. Er schließt auch Formen der privaten Forschung ein, die außerhalb des öffentlichen Interesses liegen.[21] Das lässt sich im Umkehrschluss aus dem Vergleich zu den anderen Privilegierungstatbeständen des Art. 9 Abs. 2 lit. j DSGVO herauslesen: Die Vorschrift nennt zwar das öffentliche Interesse als Tatbestandsmerkmal. Es bezieht sich semantisch jedoch ausschließlich auf die Privilegierung für Archivzwecke („*für im öffentlichen Interesse liegende Archivzwecke*“) – (bewusst) nicht auch auf „wissenschaftliche oder historische Forschungszwecke“.[22] Damit bringt der Unionsgesetzgeber stillschweigend zum Ausdruck: Forschung knüpft nicht an die Finanzierungsart an. Entsprechend nennt der Unionsgesetzgeber in seinen Erwägungsgründen neben der „*technologische[n] Entwicklung und […] Grundlagenforschung“* ausdrücklich auch *„die angewandte Forschung und die privat finanzierte Forschung*“ (ErwGrd 159 S. 2 DSGVO).

Die Schutzzone privater Forschung endet aber dort, wo der Einfluss des Auftragsgebers die Unabhängigkeit der Forschenden aushöhlt. Überlagert insbesondere die Anwendung bereits

---

[21] So aber *Jaspers/Schwartmann/Mühlenbeck,* in *Schwartmann/Jaspers/Thüsing/Kugelmann,* DSGVO/BDSG, 2018, Art. 9 DSGVO Rn. 197; *Wedde,* EU-Datenschutz-Grundverordnung, 2016, Art. 9, Rn. 133; *Weichert,* in *Kühling/Buchner,* DS-GVO/BDSG, 2. Aufl. (2018), Art. 9 DSGVO Rn. 122. Zu weitgehend auch *Schulz,* in *Gola,* DSGVO, 2. Aufl. (2018), Art. 9 DSGVO Rn. 43.
[22] *Albrecht/Jotzo* (o. Fußn. 16), Teil 4 Rn. 71.

erlangter Erkenntnisse das Bestreben, abstrakte Forschungsergebnisse zu erzielen, und schränken unternehmerische (Ziel-)Vorgaben die ungebundene Erkenntnissuche ein, sind das wichtige Kontraindikatoren.[23] Denn Wissenschaft zeichnet sich durch das Bemühen um einen übergreifenden Erkenntnisgewinn bei freier methodischer Vorgehensweise aus. Treten in einer Gesamtbetrachtung unternehmerische Vorgaben an die Stelle wissenschaftlicher Methodik, fehlt es an diesem Prozess planmäßiger Wahrheitssuche. Auf die Privilegierung der DSGVO kann sich daher nur berufen, wer eine übergeordnete wissenschaftliche Fragestellung und eine darauf ausgerichtete Methodik nachweisen kann, welche ihrerseits die Art und Weise der Datenerhebung und -auswertung vorprägt.[24] Das schließt die Produktentwicklung als Zweckkategorie nicht gänzlich aus. Sonst könnte private Forschung faktisch nie an der Privilegierung teilhaben. Eine rote Linie überschreitet der praxisnahe Medizinbereich aber jedenfalls dann, wenn die Produktentwicklung den Forschungszweck vollständig marginalisiert.

b) Ausfüllung des Spielraums im nationalen Recht

Auf nationaler Ebene hat der Bundesgesetzgeber den Regelungsspielraum des Art. 9 Abs. 2 lit. j DSGVO insbesondere in § 27 Abs. 1 BDSG ausgefüllt. Er gestattet (ebenso wie die parallelen Regelungen der Länder) die Verarbeitung von Gesundheitsdaten, soweit sie für wissenschaftliche Zwecke erforderlich ist und das Forschungsinteresse des Privatheitsinteresse des Betroffenen erheblich überwiegt.[25]

III. Privilegierungen der Forschung bei den Verarbeitungsgrundsätzen und Betroffenenrechten

Für Forschungszwecke erweitert die DSGVO nicht nur den Reigen der Verarbeitungsbefugnisse. Sie schränkt auch datenschutzrechtliche Grundsätze (1.) sowie die Betroffenenrechte (2.) ein. Damit greift sie zu einem der stärksten Privilegierungshebel, von denen sie in ihrem normativen Konzept Gebrauch macht.

1. Ausnahmen vom Gebot der Zweckbindung und der Speicherbegrenzung

Die wohl wichtigste Stärkung der Verarbeitung zu Forschungszwecken formt der Unionsgesetzgeber in Art. 5 Abs. 1 lit. b Hs. 2 DSGVO aus: Er lockert das *Zweckbindungsgebot.* Die forschungsbezogene Weiterverarbeitung stuft er kraft Gesetzes als mit dem Primärzweck vereinbar ein. Für sie ist keine *zusätzliche* Rechtsgrundlage erforderlich, solange

---

[23] Ähnlich auch *Roßnagel,* in *Simitis/Hornung/Spiecker gen. Döhmann,* DSGVO/BDSG, 2019, Art. 5 DSGVO Rn. 106.
[24] So im Ergebnis auch *Caspar,* in *Simitis/Hornung/Spiecker gen. Döhmann,* DSGVO/BDSG, 2019, Art. 89 DSGVO Rn. 16; *Weichert*, ZD 2020, 18 (19 f.); *Werkmeister/Schwaab*, CR 2019, 85 f.
[25] Wer an der Privilegierung teilhaben will, muss darüber hinaus *angemessene und spezifische Maßnahmen* zum Datenschutz in den Prozess der Datenverarbeitung implementieren (§ 27 Abs. 1 S. 2 BDSG). Die Vorgabe ergänzt und konkretisiert der Gesetzgeber in § 22 Abs. 2 S. 2 BDSG mit einem ausdifferenzierten Katalog technisch-organisatorischer Maßnahmen, die der Verantwortliche zu treffen hat, um den Datenschutz zu wahren.

Verantwortliche sich auf eine primäre Verarbeitungsbefugnis stützen können.[26] Wenn Medizinforscher etwa Patientendaten eines Krankenhauses wissenschaftlich auswerten möchten, dann genügt hierfür, dass die behandelnden Ärzte diese ursprünglich, sei es auf der Grundlage einer Einwilligung, sei es kraft einer gesetzlichen Befugnis, rechtmäßig erhoben hatten.

Die DSGVO lockert auch das Gebot der *Speicherbegrenzung*: Verantwortliche müssen personenbezogene Daten, die sie ausschließlich für wissenschaftliche Forschungszwecke verarbeiten, nicht unmittelbar nach Abschluss ihrer Auswertungen löschen, sondern dürfen diese länger speichern (Art. 5 Abs. 1 lit. e a. E. DSGVO).

a) Reichweite des Forschungsprivilegs

Die Privilegien, die das Unionsrecht der Forschung zugesteht, gelten nicht vorbehaltlos. Die DSGVO knüpft die Lockerung seines materiellen Schutzniveaus vielmehr stets an Sicherungsmechanismen: Inhalt und Umfang der Verarbeitungsbefugnis aus Art. 9 Abs. 2 lit. j DSGVO setzen einerseits „*angemessene und spezifische Maßnahmen*" des Verantwortlichen voraus, um den Datenschutz zu wahren. Andererseits verlangt Art. 89 Abs. 1 DSGVO – insbesondere für die Befreiung vom Zweckbindungsgebot und der Speicherbegrenzung – „*Garantien*", die einen angemessenen Privatheitsschutz sicherstellen. Nur wenn ein Verantwortlicher diese Kautelen einhält, kann er sich auf die gesetzliche Verarbeitungsbefugnis berufen, um personenbezogene Daten zu Forschungszwecken auch über die festgelegten Zwecke der primären Verarbeitung hinaus zu verarbeiten.

Art. 89 Abs. 1 DSGVO soll damit einen datenschutzrechtlichen Ausgleich für diejenigen herstellen, die sich damit abfinden müssen, dass ihre Daten Gegenstand einer gesetzlich zulässigen (Weiter-)Verarbeitung für Forschungszwecke sind. Dieser Intention wird die Vorschrift jedoch im Ergebnis nicht vollständig gerecht. Denn ihre Vorgabe, *„technische und organisatorische Maßnahmen [vorzusehen], mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird*", statuiert gegenüber der Generalklausel des Art. 25 Abs. 1 DSGVO (*Privacy by Design*) in ihrer nahezu wortlautgleichen Diktion keine greifbaren zusätzlichen Vorgaben, die das normative Anforderungsniveau inhaltlich ausfüllen. Die Funktion der Vorschrift erschöpft sich im Ergebnis vorrangig in einem programmatischen Bekenntnis: Sie schwört privilegierte Datenverarbeiter auf abstrakter Ebene auf ihre besondere Verantwortung für datenschutzfreundliche Technikgestaltung ein, schweigt sich jedoch gleichzeitig über konkrete Vorgaben für Forscher aus.

b) Konkretisierungsbedarf durch den Europäischen Datenschutzausschuss

Soll bei der forschungsbezogenen Datenauswertung ein einheitlich höheres Schutzniveau Einzug erhalten, führt an detaillierteren unionalen Vorgaben für ein konsequentes *Privacy by Design* kein Weg vorbei. *De lege ferenda* ist die Union daher aufgerufen, den Inhalt der

[26] A. A. wohl *Heberlein,* in *Ehmann/Selmayr,* DSGVO, 2. Aufl. (2018), Art. 6 DSGVO Rn. 17; ähnlich auch *Roßnagel* (o. Fußn. 34), Rn. 109 im Hinblick auf Art. 6 Abs. 4 lit. d DSGVO.

abstrakten Garantien des Art. 89 DSGVO in einer für den Rechtsanwender handhabbaren Weise zu konkretisieren.

Vor allem der Europäische Datenschutzausschuss („EDSA“) steht in der Verantwortung, zeitnah seine Befugnisse zu nutzen, um die rechtlichen Anforderungen mit Hilfe bereichsspezifischer Mechanismen zu konkretisieren. Sein Aufgabenkatalog umfasst ausdrücklich, Leitlinien bereitzustellen, um eine einheitliche Anwendung der Verordnung sicherzustellen (Art. 68 Abs. 1 S. 2 lit. e DSGVO). Vermittelt über akkreditierte Stellen kann er nicht nur datenschutzspezifische Zertifizierungsverfahren, sondern auch Datenschutzsiegel und -prüfzeichen aus der Taufe heben. Der Ausschuss könnte im Kohärenzverfahren insbesondere einen Prüfkatalog für die technisch-organisatorische Absicherung des Datenschutzes in der Forschung schaffen, der auch die legitimen Interessen der Forscher berücksichtigt (vgl. Art 63 DSGVO). Zudem sollte der EDSA seiner Aufgabe aus Art. 40 Abs. 1 DSGVO nachkommen, die im Forschungskontext relevanten Verbände der Medizinforschung dabei zu unterstützen, Verhaltensregeln auszuarbeiten.

Vollständig auflösen kann der EDSA die bestehende Regelungsunschärfe jedoch nicht aus eigener Machtvollkommenheit. Denn er kann die DSGVO zwar *konkretisieren*, ihren Aussagegehalt aber nicht mit normativer Kraft *korrigieren*. Dafür erteilt ihm Art. 70 DSGVO nicht das Mandat. Perspektivisch wird sich die Hoffnung auf mehr Rechtssicherheit ohne kontextspezifische Regulierung mit einem erhöhten Maß an legislatorischen Detailregelungen kaum einlösen lassen. Insbesondere delegierte Rechtsakte sind insoweit ein probates Mittel, um Vorgaben zu präzisieren, ohne Gefahr zu laufen, die DSGVO als rechtlichen Rahmen mit Detailregelungen zu überfrachten.

2. Einschränkung der Betroffenenrechte zugunsten wissenschaftlicher Forschung

Dass die DSGVO auf Konkretisierung angewiesen ist und Interessenkonflikte nur unzureichend auflöst, zeigt sich nicht nur am Beispiel des Art. 89 DSGVO, sondern auch bei den Betroffenenrechten (Art. 14 ff. DSGVO).

Die Verordnung schränkt diese zugunsten wissenschaftlicher Forschungszwecke nachhaltig ein.[27] So entfällt der Anspruch auf Löschung bspw., wenn diese die wissenschaftlichen Forschungszwecke unmöglich macht oder ernsthaft beeinträchtigt (Art. 17 Abs. 3 lit. d DSGVO). Gleiches gilt für das Recht, der forschungsbezogenen Verarbeitung personenbezogener Daten aufgrund besonderer persönlicher Umstände zu widersprechen: Ist die Datenverarbeitung für Forschungszwecke erforderlich, die im öffentlichen Interesse liegen, schließt die Union das Widerspruchsrecht aus (Art. 21 Abs. 6 Hs. 2 DSGVO). Damit versucht die DSGVO der spannungsgeladenen Konfliktsituation zwischen Individual- und Gemeinwohlinteresse bei Forschungszwecken Tribut zu zollen. Dieser gesetzgeberischen Entscheidung für den Vorrang

[27] Darüber hinaus ermöglichen es die Öffnungsklauseln des Art. 23, Art. 85 Abs. 2 und Art. 89 Abs. 2 DSGVO den Mitgliedstaaten, die Betroffenenrechte weitergehend zurückzuschneiden.

der Forschungsinteressen liegt ein Dilemma zugrunde, das strukturelle Ähnlichkeit mit der erzwungenen Blutspende bei einem Träger einer seltenen Blutgruppe aufweist. Ebenso wie sich der behandelnde Arzt fragen muss, inwieweit er in die körperliche Integrität eines Patienten eingreifen darf, um das Leben eines anderen zu retten, steht der Gesetzgeber vor der Frage, innerhalb welcher Grenzen er dem Betroffenen im überwiegenden Gemeinwohlinteresse einen sensiblen Eingriff in sein informationelles Selbstbestimmungsrecht zumuten darf.

Der Unionsgesetzgeber hat zwar darauf verzichtet, das forschungsbezogene Widerspruchsrecht der DSGVO explizit mit einem Menschenwürdevorbehalt als Brandmauer gegen ausufernde Datenauswertungen von Forschern, die sich auf das Gemeinwohl berufen, auszustatten. Die Grundrechte der GRCh ziehen utilitaristisch motivierten Datenverarbeitungen gleichwohl eine absolute Grenze: Greift eine Datenverarbeitung in die Menschenwürde (Art. 1 GRCh) ein, setzt sich diese nicht abwägungsfähige Grundrechtsposition des Betroffenen gegen das Forschungsinteresse durch. Die Grenze zum Eingriff ist dann überschritten, wenn die Datenverarbeitung den Betroffenen ohne Rücksicht auf seine Interessen zum bloßen Objekt staatlichen Handelns herabwürdigt. Konkretisierende Maßstäbe für diese Grenzziehung tun angesichts des stetig wachsenden Analysepotenzials personenbezogener Daten allerdings not. Dazu bleibt der Unionsgesetzgeber weiterhin aufgerufen.

IV. Schärfung des risikobasierten Ansatzes

Während auf der einen Seite die gelebte Praxis in Wartezimmern die Ideale des Datenschutzes schnell zu einem leeren Formalismus verkommen lässt, stellt sich angesichts des Datenhungers der großen Internetkonzerne bei vielen Patienten auf der anderen Seite ein Gefühl der Ohnmacht ein, wenn ihre Daten in opake Softwareanwendungen oder umfassende Forschungsanalysen einfließen (sollen). Dieser Befund findet seine Ursache nicht zuletzt im „One-Size-Fits-All"-Anspruch der DSGVO: Sie schlägt verschiedene Verarbeitungskontexte mit gänzlich unterschiedlichem Gefährdungspotenzial über einen Leisten. Die dörfliche Hausarztpraxis, die Blutproben an ein Labor übersendet, unterliegt grundsätzlich dem gleichen datenschutzrechtlichen Regime wie ein großes Universitätsklinikum, das tausende Patientendaten aus unterschiedlichen Quellen sammelt und mittels Deep Learning auswertet. Die Folge: Das rechtliche Zulässigkeitsregime spiegelt die besonderen divergierenden Risiken der spezifischen Verarbeitungskontexte nicht hinreichend wider.

Langfristig ist eine Neuorientierung des Datenschutzrechts unumgänglich: Um die Interessen des Einzelnen im digitalen Zeitalter angemessen berücksichtigen zu können, sollte es sich nicht bloß an Datenkategorien und Verarbeitungszwecken ausrichten, sondern stärker das Bedrohungspotenzial spezifischer Verarbeitungskontexte in den Blick nehmen. [28] Die

[28] In diese Richtung auch *Purtova*, Law, Innovation and Technology 10 (2018), 40, 79 f. Vgl. auch *Veil*, NVwZ 2018, 686 (692 ff.).

Verantwortung dafür, passgenaue Maßnahmen zu ergreifen, stülpt die DSGVO indessen *de lege lata* den jeweiligen Verarbeitern über. Sie hält keine konkreten Abwägungskriterien vor, die ebenso greifbar wie praktikabel sind. Diese Lücke gilt es zu schließen. Gesetzgeberisches Ziel sollte daher sein kontextspezifische Verarbeitungsregeln zu etablieren, die zielgenau auf konkrete Gefahrenszenarien reagieren und im Wege der praktischen Konkordanz die Interessen von Betroffenen und Forschern durch rechtssichere Vorgaben ausgleichen.

Im Fall des DVG können bspw. Regelungen sinnvoll sein, um Betroffene, die – trotz der bereits umfassenden Vorkehrungen – ein erhöhtes Re-Identifikationsrisiko trifft, gezielt vor besonderen Gefahren für ihr informationelles Selbstbestimmungsrecht zu schützen, bspw. eine Auswertung nur unter der Voraussetzung klar benannter technischer Schutzvorkehrungen zuzulassen. Als mögliche Maßnahmen sind insbesondere nicht nur konkrete erhöhte Anforderungen an die Verschlüsselung der Daten denkbar, sondern auch umfassende Protokollierungspflichten über Datenzugriffe.

V. Fazit und Ausblick

Die DSGVO ist mit dem Anspruch angetreten, das unionale Datenschutzniveau auf eine neue Stufe zu heben. Im Hinblick auf den Datenschutz in der Medizinforschung ist ihr das nur teilweise gelungen. Der weite Begriff des Personenbezugs sichert dem Datenschutzregime zwar einen umfassenden Anwendungsbereich – denn Patienten- und Fitnessdaten sind aufgrund ihrer Individualität im Zweifel immer personenbezogen. Damit korrespondiert allerdings nicht notwendig auch ein höheres Schutzniveau für die Betroffenen und ihre Interessen. Die DSGVO priorisiert Forschungszwecke vielmehr umfänglich – sowohl im Hinblick auf Verarbeitungsbefugnisse als auch Verarbeitungsgrundsätze. Insbesondere lockert der Unionsgesetzgeber die Zweckbindung sowie das Gebot der Speicherbegrenzung und verbürgt die Betroffenenrechte im Forschungskontext auf der Grundlage zahlreicher Öffnungsklauseln nur in eingeschränkter Form. Forscher können daher Gesundheitsdaten auch ohne Einwilligung der Betroffenen umfänglich auswerten.

Dem besonderen Bedürfnis nach einem wirksamen Vertrauensschutz für Patienten sollten *de lege ferenda* ein Regulierungsrahmen für ein Datentreuhandmodell sowie eine rechtliche Anonymisierung den Weg ebnen: Verantwortliche, die umfassende Vorkehrungen treffen, um eine (Re-)Identifikation der Betroffenen zu vermeiden, befreit das Gesetz dann in festgelegten Verarbeitungskontexten aus dem Klammergriff datenschutzrechtlicher Anforderungen; wer als Nutzer den Personenbezug gleichwohl herstellt, sieht sich dann im Gegenzug hohen Sanktionsdrohungen ausgesetzt.

Weitsichtiger als nationale Regelungen, die mitunter in einer datenschutzrechtlichen Kleinstaaterei münden, sind dabei einheitliche Vorgaben auf Unionsebene, welche die Vision eines EU-weiten Gesundheitsdatenraums verwirklichen. Gegenwärtig läuft die Entwicklung aber unter umgekehrten Vorzeichen: Die hohe Zahl an Öffnungsklauseln in der DSGVO fragmentiert das europäische Gesundheitsdatenschutzrecht. Langfristig wird daher kein Weg daran vorbeiführen, den mitgliedstaatlichen Regelungsspielraum zurückzuschneiden.

Materiell ist der EU-Gesundheitsdatenschutz der Zukunft dazu aufgerufen, das Innovationspotenzial eines digitalisierten Gesundheitswesens und die Interessen der Betroffenen durch tertiärrechtlich konkretisierte und dadurch rechtssichere, praktisch handhabbare Privacy-by-Design-Lösungen miteinander zu versöhnen. Medizinische Forschung und Datenschutz müssen dabei kein Widerspruch in sich sein. Denn erst das Vertrauen der Patienten in selbstbestimmungsgerechte Gesundheitsdatenverarbeitung liefert den Nährboden für eine reiche Datenlese der Big-Data-Forschung. Dieses Vertrauen ist auf verlässliche rechtliche Regeln angewiesen. Nur dann kann die Dystopie eines gläsernen Patienten der Vision digitaler Patientensouveränität weichen.