Die Datentreuhand in der medizinischen Forschung – eine Untersuchung aus juristischer Perspektive

Von *Alissa Brauneck* und *Louisa Schmalhorst*

I. Einleitung

Patienten- und Gesundheitsdaten spielen in der medizinischen Forschung eine herausragende Rolle. Sie sind der Schlüssel zu akkuraten und effektiven Behandlungen und der Entwicklung neuer Medikamente.[1] Dabei gilt die Devise: Je mehr Daten, desto besser. Ziel ist die sogenannte personalisierte Medizin – eine medizinische Behandlung, die perfekt auf den einzelnen Patienten zugeschnitten ist. Zahlreiche Beispiele für eine solche Personalisierung bietet der Bereich der Onkologie: Weil Standardtherapien meist den Nachteil haben, dass sie nicht bei allen Patienten gleich gut wirken,[2] werden heute die Tumorzellen erst genetisch analysiert, bevor eine maßgeschneiderte Therapie erfolgt. Das verschafft den Erkrankten in vielen Fällen eine bessere Aussicht auf Heilung und eine längere Lebensdauer.[3] Was aus Sicht der Wissenschaft und zur Gesundheitsversorgung wünschenswert ist, lässt sich in der Praxis allerdings nicht leicht umsetzen: Bei Patienten- und Gesundheitsdaten handelt es sich in der Regel um personenbezogene Daten, die nur nach strengen datenschutzrechtlichen Voraussetzungen verarbeitet werden dürfen. Dieses strenge Regelungsregime zum Patientendatenschutz birgt allerdings die Gefahr, dass der für Fortschritte in der medizinischen Forschung notwendige Zugriff auf Daten erschwert wird, und reduziert somit die verfügbare Datenmenge. Das wiederum kann sich negativ auf den Behandlungserfolg und die Überlebensrate der Patienten auswirken. Dabei sind zwei Seiten zu berücksichtigen: Einerseits wollen Menschen ihre Gesundheitsdaten vor unberechtigten Zugriffen geschützt wissen. Andererseits wünschen sie sich ganz im Zeichen der Datensouveränität, frei über die eigenen Daten zu bestimmen. Studien hierzu haben belegt, dass viele Menschen grundsätzlich dazu bereit sind, die eigenen Daten der Gesundheitsforschung zur Verfügung zu stellen.[4] Der Gesetzgeber

[1] Vgl. *Bundesregierung*, Datenstrategie der Bundesregierung. Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Kabinettfassung, 27.01.2021, Datenstrategie der Bundesregierung, S. 1 (35).

[2] *Michael Manns,* Individualisierte Infektionsmedizin, https://www.helmholtz-hzi.de/de/wissen/wissensportal/keime-und-krankheiten/individualisierte-infektionsmedizin/ (17.10.22).

[3] *Manns,* Individualisierte Infektionsmedizin (Fn. 2).

[4] TZI Studie, 2021, https://www.bremen-digitalmedia.de/tzi-studie-hohe-bereitschaft-zur-spende-von-gesundheitsdaten/ (27.10.22); siehe zur Akzeptanz und Verbreitung der ePA auch *S. Deister*, in diesem Band, S. 41 f.

folgt diesem Trend an vielen Stellen, so etwa mit der elektronischen Patientenakte (ePA), bei der es bald schon möglich sein soll,[5] die eigenen – in der ePA gespeicherten – Daten für Forschungszwecke freigeben zu können;[6] nach aktuellen Bestrebungen über eine Widerspruchs- d. h. Opt-Out-Lösung.[7] Oder aber in dem geplanten Gesundheitsdatennutzungsgesetz (GDNG), das (ebenfalls) beabsichtigt, den Zugang zu Gesundheitsdaten für sekundäre (Forschungs-)Zwecke deutlich zu steigern.[8]

Die Nutzung von Daten in der medizinischen Forschung steht damit in einem gewissen Spannungsverhältnis. Forschungsinteressen sind mit der Patientensouveränität, insbesondere mit Datenschutz und Datensicherheit in Einklang zu bringen. Die Datentreuhand kann hier Abhilfe schaffen, indem sie als neutrale Intermediärin zwischen die datengebenden und datennutzenden Personen bzw. Einrichtungen tritt. Diskussionen um eine Datentreuhand in der medizinischen Forschung sind aktuell wie nie zuvor.[9] Davon zeugen der Koalitionsvertrag der aktuellen Bundesregierung[10] und etliche Strategien und Förderprojekte auf Bundes- aber auch auf europäischer Ebene.[11] Trotz dieses Hypes fehlt es an einer Definition und einem Regulierungsrahmen. Grund genug, das Phänomen der Datentreuhand aus juristischer Sicht näher zu untersuchen. In diesem Aufsatz sollen zunächst verschiedene Definitionsansätze vorgestellt werden. Diese Erkenntnisse werden im Anschluss durch konkrete Funktionen der Datentreuhand in der medizinischen Forschung ergänzt. Sodann wird die datenschutzrechtliche Verantwortung und Haftung der Datentreuhand untersucht. Es folgen Ausführungen zur rechtssicheren Datenverarbeitung in der medizinischen Forschung, wobei Privacy by Design i. S. d. Art. 25 Abs. 1 DSGVO im Fokus steht, und schließlich wird ein sogenanntes Schutzklassenkonzept als Lösungsweg präsentiert: Mithilfe dieses Konzepts lassen sich mögliche Risiken, die bei der Verarbeitung personenbezogener (Patienten-)Daten entstehen, mittels fünf verschiedener Privacy-Ebenen quantifizierbar machen und durch entsprechende Schutzmaßnahmen flankieren. Hierauf folgt eine Darstellung möglicher Maßnahmen, um Missbrauchsrisiken zu mitigieren. Der Beitrag schließt mit einem Fazit.

[5] Die ausreichen, um es der Kontrolle (und damit der moralischen Verantwortung) des Operateurs zu entheben. Zugleich sind diese Agentivität und Autonomie jedoch nicht in einem solchen Maß vorhanden, dass man dem Gerät den Status eines moralischen Agenten – und damit eines Verantwortungsträgers- zuweisen könnte.

[6] Insbesondere § 363 SGB V; vgl. *S. Rachut*, in diesem Band, S. 82.

[7] BR-Drs. 597/22, S. 2.

[8] *Bundestag*, Begründung zum Entwurf des GDNG, 30. 08. 2023, S. 84.

[9] Siehe bereits zu früheren Bemühungen um eine Datentreuhand, etwa in den 1980er Jahren: *Kurt Böhm/Gustav Wagner*, CR 1987, S. 621 (625).

[10] Koalitionsvertrag 2021 – 2025 zwischen SPD, Bündnis 90/Die Grünen und FDP, S. 1 (17).

[11] *Bundesregierung* (Fn. 1), S. 34.

II. Phänomen: Datentreuhand

Die Datentreuhand kann grundsätzlich eine natürliche, juristische, private oder öffentlich-rechtliche Person sein. Sie führt ihre Rolle entweder als Auftrag (unentgeltlich) oder Geschäftsbesorgung (entgeltlich) aus. Die §§ 662 ff. BGB beruhen auf dem Prinzip des persönlichen Vertrauens und sind daher gut geeignet, Treuhandverhältnisse im Innenverhältnis zu regeln.[12] Im Übrigen gibt es bereits verschiedene Definitionsansätze zur Datentreuhand. Nach dem Vorschlag der Bundesregierung in ihrer Datenstrategie kann eine Datentreuhandstelle „mit der Aufgabe betraut sein, einen standardisierten Zugang zu Daten für zugelassene Stellen zu entwickeln und umzusetzen. Zudem besitzen Datentreuhänder eine Beratungsfunktion gegenüber ihren Nutzerinnen und Nutzern und bietet je nach Spezialisierung verschiedene Dienste, wie zum Beispiel die Verwaltung von Daten im Sinne der Nutzerinnen und Nutzer. Datentreuhänder können aber auch datenschutzrechtliche Interessen und Gestaltungsrechte für Verbraucherinnen und Verbrauchern geltend machen".[13] Die Bundesregierung legt dabei weder die Rechtsnatur der Datentreuhand noch die Anforderungen, die an ihren Träger gestellt werden, fest.

Der am 23. 6. 2022 in Kraft getretene Data Governance Act (DGA) regelt seinem Wortlaut nach nicht unmittelbar Datentreuhandmodelle, dafür aber die ihr ähnlichen Anbieter von Datenvermittlungsdiensten. Dabei handelt es sich gemäß Art. 2 Nr. 11 DGA um Stellen, die „durch technische, rechtliche oder sonstige Mittel Geschäftsbeziehungen zwischen einer unbestimmten Anzahl von betroffenen Personen oder [Datengebenden] einerseits und [Datennutzenden] andererseits […] [herstellen], um die gemeinsame Datennutzung […] zu ermöglichen […]".[14] Die Ausgestaltungsmöglichkeiten solcher Datenvermittlungsdienste werden durch einen Negativkatalog in Art. 2 Nr. 11 lit. a) bis d) DGA begrenzt. Laut Erwägungsgrund 27 sollen durch Datenvermittlungsdienste freiwillige Verfahren zur gemeinsamen Datennutzung unterstützt und gefördert werden. Zudem sollen diese den Austausch von Daten erleichtern. Dabei verwenden sie die Daten der Datengebenden gemäß Art. 12 lit. a DGA nur, um sie Datennutzenden zur Verfügung zu stellen. Anbieter von Datenvermittlungsdiensten können gemäß Art. 12 lit. e DGA zusätzlich spezifische Werkzeuge und Dienste für die datengebenden Personen erbringen, zum Beispiel Daten speichern, pflegen, konvertieren, anonymisieren oder pseudonymisieren. Laut Erwägungsgrund 30 können sie sich auch – als besondere Kategorie von Datenvermittlungsdiensten – dafür einsetzen, „die Handlungsfähigkeit und die Kontrolle des Einzelnen in Bezug auf die ihn betreffenden [personenbezogenen] Daten [zu] verbessern

[12] *Gabriele Buchholtz/Alissa Brauneck/Louisa Schmalhorst*, Gelingensbedingungen der Datentreuhand – rechtliche und technische Aspekte, NVwZ 2023, S. 206 (208).

[13] *Bundesregierung* (Fn. 1), S. 110.

[14] *Data Governance Acts (DGA)*, Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten Governance-Rechtsakt).

[und] Einzelpersonen bei der Ausübung ihrer Rechte gemäß der Verordnung (EU) 2016/679 [zu unterstützen]".

Unklar ist, ob die EU-Kommission mit den Anbietern von Datenvermittlungsdiensten auch die Datentreuhand erfassen wollte. Nach Auffassung einiger Stimmen im Schrifttum schließen DGA-Anbieter gemäß Art. 2 Nr. 11 DGA auch Datentreuhandmodelle mit ein.[15] Der DGA und der europäische Gesetzgeber treffen hierzu allerdings keine klare Aussage. Da sich die Datentreuhand und der Datenvermittlungsdienst bereits begrifflich stark voneinander unterscheiden, obwohl die Bezeichnungen *Datentreuhand* bzw. *data trust* bereits lange bekannt sind, spricht viel dafür, dass der Gesetzgeber mit dem *Datenvermittlungsdienst* – in Abgrenzung zur Datentreuhand – bewusst eine neue Figur hat schaffen wollen. Anbieter von Datenvermittlungsdiensten und Datentreuhand weisen zwar Überschneidungen auf, weil beide Figuren das Ziel haben, Daten zwischen mehreren Parteien zu mitteln. Datenvermittlungsdienste haben aber (unter anderem über den Negativkatalog in Art. 2 Nr. 11 DGA) enge Anwendungsgrenzen. Auch kann nach Erwägungsgrund 33 des DGAs der Datenvermittlungsdienst lediglich von einer juristischen Person erbracht werden.[16] In der Gesamtschau ist es diesen Diensten also unmöglich, derart weitreichende Funktionen zu erfüllen wie die Datentreuhand. Eine klare Trennung zwischen Datentreuhand und Datenvermittlungsdienst ist daher unumgänglich, um Interessenkonflikte zu vermeiden.[17] Der DGA schafft mit seiner Definition des Datenvermittlungsdiensts mithin keine abschließende definitorische Klarstellung für die Datentreuhand.[18]

In der medizinischen Forschung wird die Definition der Datentreuhand weitgehend auf ihre möglichen Funktionen gestützt: Danach ist die Datentreuhand eine Instanz, die „zwischen eine Forschungsdaten besitzende Stelle und den Forscher [tritt] und […] dadurch die Rechte der betroffenen Patienten und Probanden [absichert]".[19] Denkbar ist auch, dass sich die Datentreuhand unmittelbar mit Patient:innen und Proband:innenen in Verbindung setzt, ohne dass dazu eine weitere Stelle (etwa eine Arztpraxis, ein Krankenhaus oder ein Forschungslabor) dazwischen tritt. Ihr kann die Aufgabe zukommen, Daten, die ihr (von Patient:in/Proband:in, Krankenhaus,

[15] Ohne dies allerdings näher zu erläutern: *Louisa Specht-Riemenschneider/Aline Blankertz/Pascal Sierek/Ruben Schneider/Jakob Knapp/Theresa Henne*, Die Datentreuhand. Ein Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierungserfordernisse für Datentreuhandmodelle, MMR-Beil. 2021, S. 25 (32); *Benedikt Falkhofen*, Infrastrukturrecht des digitalen Raums. Data Governance, Data Act und Gaia X, EuZW 2021, S. 787 (790).

[16] Anders bei der Datentreuhand, siehe dazu II. Phänomen Datentreuhand.

[17] *Gunnar Stevens/Alexander Boden*, Warum wir parteiische Datentreuhänder brauchen, 2022, S. 1 (10), https://www.verbraucherforschung.nrw/sites/default/files/2022-02/zth-06-stevens-boden-warum-wir-parteiische-datentreuhaender-brauchen.pdf (08.09.2022).

[18] *Buchholtz/Brauneck/Schmalhorst* (Fn. 12), S. 207.

[19] *Klaus Pommerening/Johannes Drepper/Krister Helbing/Thomas Ganslandt*, Leitfaden zum Datenschutz in Medizinischen Forschungsprojekten: Generische Lösungen Der TMF 2.0., S. 1 (209).

Forschungseinrichtung, etc.) übermittelt werden, zu anonymisieren oder zu pseudonymisieren. Die Datentreuhand gibt dann ihrerseits Forschenden (und allgemein Zugriffsberechtigten) auf anonymisierte bzw. pseudonymisierte Daten Zugriff.[20] Teilweise wird vorgeschlagen, dass die Datentreuhand „idealerweise einer besonderen Geheimhaltungspflicht unterliegt, [wie] zum Beispiel ein Notar oder ein Arzt".[21] Die damit einhergehende gesetzliche Pflicht zur Verschwiegenheit könne zusätzlich das Vertrauen in die Datentreuhand stärken.[22] Unabhängig von einer solchen Geheimhaltungspflicht stellt sich die Frage, wie mit dem Zeugnisverweigerungsrecht von Ärzt:innen und anderen medizinischen Berufsgeheimnisträger:innen und dem Beschlagnahmeschutz bestimmter Daten und privilegierter Berufsgruppen gemäß § 53 Abs. 1 S. 1 Nr. 3 StPO im Zusammenhang mit Datentreuhandmodellen umzugehen ist.[23]

Aus den dargestellten Definitionsansätzen geht hervor, dass die Datentreuhand die Rolle einer Intermediärin[24] zur Mittlung von Daten zwischen mindestens zwei Parteien (Datengebenden und Datennutzenden) einnehmen soll. Je nach Einsatzbereich kann die Datentreuhand verschiedene Besonderheiten aufweisen, um ihre konkreten Aufgaben effektiv erfüllen zu können. In der medizinischen Forschung können Daten zwischen Patient:innen/Proband:innen und den Forschenden, Forschungseinrichtungen oder Krankenhäusern gemittelt werden.

III. Einsatz der Datentreuhand in der medizinischen Forschung

In der medizinischen Forschung existieren bereits verschiedene Beispiele für Datentreuhandstellen: So gibt es unter anderem Biodatenbanken, die zwischen dem Datengebenden und dem Datennutzenden die Pseudonymisierung vornehmen, bevor die Daten weitergeleitet werden, oder den Schlüssel zu den Pseudonymen aufbewahren.[25] Auch einige Universitäten lassen ihre Daten durch Datentreuhandstellen verwalten. So haben etwa die Technische Universität Dresden und die Universität

[20] *Pommerening/Drepper/Helbing/Ganslandt* (Fn. 19), S. 209.

[21] *Pommerening/Drepper/Helbing/Ganslandt* (Fn. 19), S. 209.

[22] *Pommerening/Drepper/Helbing/Ganslandt* (Fn. 19), S. 209.

[23] *Benedikt Buchner/Anna Haber/Horst Hahn/Harald Kusch/Fabian Prasser/Ulrich Sax/Carsten Schmidt*, Das Modell der Datentreuhand in der medizinischen Forschung, DuD 2021, S. 806 (807); s. etwa *Christian Dierks*, Rechtsgutachten zur elektronischen Datentreuhänderschaft (2008), www.tmf-ev.de/Themen/Projekte/V052_01_Datentreuhaenderdienst_I.aspx (25. 10. 2022).

[24] *Louisa Specht-Riemenschneider/Aline Blankertz*, Lösungsoption Datentreuhand: Datennutzbarkeit und Datenschutz zusammen denken, MMR 2021, S. 369 (370).

[25] *Verbraucherzentrale Bundesverband*, Neue Datenintermediäre. Anforderungen des vzbv an „Personal Information Management Systems" (PIMS) und Datentreuhänder, https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf, S. 1 (5); vgl. auch *Rat für Informationsinfrastrukturen*, Datentreuhänder: Potentiale, Erwartungen, Umsetzung, 2021, https://rfii.de/download/rfii-workshopbericht-datentreuhaender-potenziale-erwartungen-umsetzung-februar-2021/, S. 1 (4).

Greifswald die Verwaltung von Identitätsdaten und die Einwilligungen von Studienteilnehmenden an eine Datentreuhand delegiert.[26] Das WiSo-Forschungslabor der Universität Hamburg bietet zudem an, die Rolle einer Datentreuhand für Forschungsprojekte zu übernehmen: Es mittelt Daten zwischen Datengebenden und Datennutzenden und stellt dabei verschiedene Optionen, die betroffenen Daten zu anonymisieren, bereit.[27] Eine weitere Datentreuhandstelle sichert Corona-Daten im Auftrag der Bundesdruckerei.[28]

Die Aufgaben, die eine Datentreuhand in der medizinischen Forschung übernehmen könnte, sind vielfältig. Sie könnte beispielsweise dafür sorgen, dass die Datennutzenden auf Daten zugreifen und diese verarbeiten können. Zu diesem Zweck gibt die Datentreuhand dann in der Regel einheitliche Nutzungsparameter und Nutzungszwecke vor, denen die Datengebenden und Datennutzenden zustimmen. Individuell mit den Datengebenden ausgehandelte Nutzungsvereinbarungen sind aufgrund der großen Datenmenge, auf die die medizinische Forschung häufig angewiesen ist, eher unrealistisch. Vielmehr sollte es für verschiedene Datenkategorien standardisierte Bedingungen für Zugriff und Nutzung geben, die durch die Datentreuhand vorgegeben werden. Zudem soll die Datentreuhand die Aufgabe übernehmen, die Daten zu verwalten. Sie beurteilt dann unter anderem Nutzungsanfragen (lehnt diese ab oder nimmt sie an), dokumentiert Datenverarbeitungsprozesse und Datenschutzmaßnahmen und verwahrt die Einwilligung der Datengebenden, welche diese jederzeit gemäß Art. 7 Abs. 3 S. 1 DSGVO widerrufen können. Einmal der Forschung zur Verfügung gestellte Daten müssen im Falle eines Widerrufs zwar nicht im Nachhinein aus bereits ermittelten Forschungsergebnissen herausgerechnet werden. In der Zukunft dürfen sie aber nicht mehr für die Wissenschaft genutzt werden. Die Datentreuhand soll darüber hinaus Zugriffs- und Verarbeitungsberechtigungen verwalten, die Daten im Interesse von Datengebenden und Datennutzenden auffindbar machen und sie an letztere mitteln.

Die Datentreuhand soll gegenüber den Datennutzenden gewährleisten, dass die Daten einem bestimmten Qualitätsstandard entsprechen (zum Beispiel durch aufwendige, teils mehrstufige Überprüfung der Datenaktualität[29]).[30] Das ist wichtig, zumal eine geringe Datenqualität einer der Hauptgründe ist, weshalb viele Institutionen derzeit noch nicht das notwendige Vertrauen haben, Daten von dritten Stellen zu

[26] *Technische Universität Dresden*, Unabhängige Treuhandstelle, https://tu-dresden.de/med/mf/forschung/services-fuer-forschende/unabhaengige-treuhandstelle (24.10.22); Universitätsmedizin Greifswald, https://www.medizin.uni-greifswald.de/de/forschung-lehre/core-units/treuhandstelle/ (24.10.22).

[27] *Universität Hamburg*, WiSo-Forschungslabor Datentreuhänderin, https://www.wiso.uni-hamburg.de/forschung/forschungslabor/services/datentreuhand.html.

[28] *Bundesdruckerei,* Treuhänder für Forschungsdaten/Patientendaten.Datentreuhänder CenTrust® der Bundesdruckerei, 2021 Microsoft PowerPoint – CenTrust@ZVEI_03112021_V02 (12. 10. 2022).

[29] *Pommerening/Drepper/Helbing/Ganslandt* (Fn. 19), S. 105, 185.

[30] *Bundesregierung* (Fn. 1), S. 34.

nutzen.[31] Zusätzlich kann die Datentreuhand weitere Aufgaben übernehmen und insbesondere Analysen für die Datennutzenden vornehmen und Daten aufbereiten, auswerten und miteinander verknüpfen.

Sowohl im Rahmen der Verwaltung als auch der Übermittlung von Daten muss die Datentreuhand sicherstellen, dass Datenschutz und -sicherheit im Sinne der Art. 24, 25 und 32 DSGVO und damit die Bestimmungen zu Privacy by Design (dazu unter V. 1.) eingehalten werden.[32] Dazu bietet es sich zum Beispiel an, Daten zu anonymisieren[33] und zu verschlüsseln[34] und Unbefugte durch Sicherheitsvorkehrungen davon abzuhalten, auf die Daten zuzugreifen.[35] Die datennutzenden Personen sollten grundsätzlich nicht auf Rohdaten zugreifen können. Ausnahmen bestehen dann, wenn die Daten durch die Verschlüsselung unbrauchbar werden oder es nicht möglich ist, sie zu pseudonymisieren. Darüber hinaus kann die Datentreuhand den Parteien ihre Expertise und technische Ausstattung zur Verfügung stellen,[36] um etwa Pseudonymisierungen oder Anonymisierungen durchzuführen oder entsprechende Beratungsdienste anzubieten. Der Bundesrat sieht zudem in seinem Beschluss zur Ausgestaltung des GDNG vor, dass die Datentreuhand Patient:innen dabei unterstützen soll, ihre Digitalkompetenz – also den richtigen „kenntnisreichen, kritischen, kreativen und widerstandsfähigen Umgang mit digitalen Medien“[37] – zu verbessern, um die „Akzeptanz und tatsächliche Nutzung von digitalen Angeboten“[38] zu fördern. Derartige Bestrebungen haben allerdings keinen Eingang in den am 30. 8. 2023 von der Bundesregierung vorgelegten Entwurf zum GDNG gefunden.

Insgesamt zeigt sich, dass der Einsatz einer Datentreuhand zahlreiche Vorteile bieten kann: Es lassen sich Daten von hoher Qualität erstellen sowie Datenschutz und -sicherheit verbessern. Das dient den Interessen der Forschenden ebenso wie

---

[31] *Sebastian Derwisch*, Data Monetization – Use Cases, Implementation and Added Value, 2019, Data Monetization – Use Cases, Implementation and Added Value, https://www.tableau.com/learn/whitepapers/barc-data-monetization-2019-summary, (12. 10. 2022).

[32] *Bundesregierung* (Fn. 1), S. 34; *Aline Blankertz/Louisa Specht*, Wie eine Regulierung für Datentreuhänder aussehen sollte, 2021, https://www.stiftung-nv.de/sites/default/files/regulierung_fuer_datentreuhaender.pdf, S. 1 (9).

[33] *Bundesregierung* (Fn. 1), S. 34.

[34] *Heiko Richter,* Europäisches Datenprivatrecht: Lehren aus dem Kommissionsvorschlag für eine „Verordnung über europäische Daten-Governance“, ZEuP 2021, S. 634 (642).

[35] *Richter* (Fn. 34), S. 642.

[36] *Bundesregierung* (Fn. 1), S. 34; GDV Die deutschen Versicherer, Positionspapier des Gesamtverbandes der Deutschen Versicherungswirtschaft. „Datenkranz beim automatisierten Fahren gemäß § 63a StVG – externe Speicherung bei einem Datentreuhänder“, 2018, https://www.gdv.de/resource/blob/36102/c9494add5b56ea558f59204a9f85e914/datentreuhaender-und-automatisiertes-fahren–download-data.pdf, S. 1 (5); vgl. auch *Jürgen Kühling*, Der datenschutzrechtliche Rahmen für Datentreuhänder. Chance für mehr Kommerzialisierungsfairness und Datensouveränität?, ZfDR 2021, S. 1 (11).

[37] *Bundesregierung*, Digitalisierung gestalten. Umsetzungsstrategie der Bundesregierung, 2021, S. 1 (39).

[38] BR-Drs. 597/22 (Fn. 7), S. 3.

denen der Patient:innen. Ein weiterer Vorteil ist, dass Datennutzende Kosten senken können,[39] indem sie nicht selbst Qualitätsdaten suchen und auswählen müssen,[40] sondern bereits auf überprüfte Daten Zugriff erhalten.[41] Weitere (finanzielle) Vorteile ergeben sich daraus, dass die Beteiligten nicht auf individuelle Verträge angewiesen sind, um Daten in ausreichender Menge zu erhalten. Kommuniziert und verhandelt wird ausschließlich mit der Datentreuhand, die zudem auch die technische Infrastruktur stellt.[42] Überdies kann es sinnvoll sein, mehr als eine Datentreuhand einzusetzen: So könnte dann etwa eine Datentreuhand damit beauftragt werden, Sicherheitsmaßnahmen durchzuführen, während die andere die verschlüsselten Daten weiter verarbeitet: Dann hat die Datentreuhand, die zum Beispiel Patient:innendaten verwaltet, aufbereitet und analysiert, selbst keinen Zugriff auf unmittelbar identifizierende Daten.[43] Die Forschenden erhalten nur diejenigen Daten, die sie tatsächlich für ihre Forschungstätigkeit benötigen.

IV. Datenschutzrechtliche Verantwortung und Haftung

Unmittelbar zusammenhängend mit der Frage, welche Aufgaben die Datentreuhand im Bereich der medizinischen Forschung übernehmen könnte muss geklärt werden, inwiefern die Datentreuhand im datenschutzrechtlichen Sinne verantwortlich ist und im Falle eines Schadens in Haftung genommen werden kann.

Datenschutzrechtlich verantwortlich ist nach Art. 4 Nr. 7 DSGVO diejenige Person, die „über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet". Übernehmen mehrere Personen diese Aufgabe, sind sie gemäß Art. 26 Abs. 1 DSGVO gemeinsam verantwortlich. Nach der Rechtsprechung des EuGH[44] ist im Zweifel dann von einer gemeinsamen Verantwortung auszugehen, wenn mehrere Akteure gemeinsam einen Beitrag zur Entscheidung über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten leisten, wobei nicht zwangsläufig von einer gleichwertigen Verantwortlichkeit der verschiedenen Akteure auszugehen ist. Auftragsverarbeiter nach Art. 4 Nr. 8 DSGVO sind hingegen Personen, die Daten nur im Auftrag einer anderen Person (des Verantwortlichen) verarbeiten und dabei deren Weisungen unterliegen (Art. 29 DSGVO)[45] und stellen damit lediglich einen „verlängerten Arm"[46] vom Auftraggeber dar.

[39] *Richter* (Fn. 34), S.643; vgl. Auch *Kühling* (Fn. 36), S. 24.

[40] Vgl. *Bundesregierung* (Fn. 1), S. 34; vgl. *Richter* (Fn. 34), S. 642.

[41] *Richter* (Fn. 34), S. 643; vgl. auch *Kühling* (Fn. 36), S. 24.

[42] Vgl. *Bundesregierung* (Fn. 1), S. 34; vgl. *Richter* (Fn. 34), S. 642.

[43] Vgl. *Pommerening/Drepper/Helbing/Ganslandt* (Fn. 19), S. 121.

[44] EuGH, Urt. v. 5.6.2018 – C-210/16, Rn. 31 ff.; Urt. v. 29.7.2019 – C-40/17, Rn. 75 ff.; *Petri*, EuZW 2018, S. 534 (536 f.).

[45] *Kühling* (Fn. 36), S. 15.

[46] *Winfried Veil*, Data Governance Act II: Datenmittler, 2021.

Inwieweit die Datentreuhand für die Verarbeitung von Daten verantwortlich ist, ist nicht abschließend geklärt und hängt von der konkreten Ausgestaltung sowie den von ihr übernommenen Aufgaben und Pflichten ab. Zum Vergleich: Der DGA sieht in Erwägungsgrund 35 vor, dass die Anbieter von Datenvermittlungsdiensten dazu verpflichtet sind, die Vorgaben der DSGVO einzuhalten. Dabei kann ihnen sowohl die Rolle des Verantwortlichen im Sinne von Art. 4 Nr. 7 DSGVO oder die des Auftragsverarbeiters im Sinne von Art. 4 Nr. 8 DSGVO zukommen (Erwägungsgrund 35 S. 2). Viel spricht dafür, diese flexible Handhabung, die sich an der tatsächlichen Praxis, das heißt, an den konkret erbrachten Aufgaben und Pflichten orientiert, auch auf die Datentreuhand zu übertragen.

Will man eine Verantwortlichkeit der Datentreuhand im Sinne von Art. 4 Nr. 7 DSGVO von vornherein ausschließen – zum Beispiel, um Haftungsrisiken zu reduzieren – bleiben zwei maßgebliche Aspekte zu bedenken. Erstens bleibt die Datentreuhand im Rahmen der von ihr übernommenen Aufgaben grundsätzlich immer verantwortlich und kann sich insoweit auch einer eventuellen Haftung nicht entziehen.[47] Und zweitens hängen Verantwortung und Vertrauen eng miteinander zusammen: Damit das Vertrauen der Datengebenden gewonnen werden kann und sich neue Konstrukte wie die Datentreuhand überhaupt erfolgreich etablieren lassen, kommt es insbesondere auch darauf an, wie sich diese zu Fragen der Verantwortung und damit letztlich zur Haftung im Falle einer Rechtsverletzung verhält. Setzt die Datentreuhand eigenverantwortlich ihr „überlegene[s] Wissen“[48] ein, spricht Vieles gegen die Rolle eines (reinen) Auftragsverarbeiters.[49] Wer welche Aufgaben und Pflichten übernimmt, sollten alle Beteiligten vor der Datenverarbeitung regeln, um damit die Frage der Verantwortlichkeit zu klären.

Zentral ist ferner die Frage nach der Haftung für datenschutzrechtliche Verstöße. Mit Inkrafttreten der DSGVO hat der EU-Gesetzgeber den Bußgeldrahmen deutlich – für besonders gravierende Verstöße etwa auf Geldbußen von bis zu 20 Millionen Euro, Art. 83 Abs. 5 DSGVO – erhöht. Da die Datentreuhand Daten regelmäßig zwischen vielen verschiedenen Betroffenen und Verantwortlichen mitteln soll, potenziert sich ihr Haftungsrisiko.[50] Werden zusätzlich sensible Daten verarbeitet, so fällt der Schaden, der bei der Verletzung dieser Daten entsteht, und damit auch die Haftung noch einmal höher aus. Eine Datentreuhand etwa in der medizinischen Forschung ist folglich erheblichen Haftungsrisiken ausgesetzt. Verstößt eine Verarbeitung personenbezogener Daten gegen Datenschutzrecht, so können die Betroffenen gegenüber dem/den Verantwortlichen Schadensersatz geltend machen, sofern der entstandene Schaden zurechenbar und eine Exkulpation ausgeschlossen ist

[47] Vgl. *Johannes Buchheim/Steffen Augsberg/Petra Gehring*, Transaktionsbasierte Datentreuhand, JZ 2022, S. 1139 (1146).

[48] Vgl. *Kühling* (Fn. 36), S. 16.

[49] Vgl. *Kühling* (Fn. 36), S. 16.

[50] *Jürgen Kühling/Florian Sackmann/Hilmar Schneider,* Datenschutzrechtliche Dimensionen Datentreuhänder: Kurzexpertise, 2020, S. 1 (28).

(Art. 82 Abs. 1, 2 und 3 DSGVO).[51] Grund für die Haftung können sowohl Verstöße gegen Informationsrechte von Patient:innen oder Proband:innen und Verarbeitungen ohne wirksame Einwilligungen sein, oder auch der Verlust von Forschungsdaten. Der Schadensersatzanspruch besteht nach dem Wortlaut des Art. 82 Abs. 1 DSGVO sowohl im Hinblick auf die materiellen als auch die immateriellen Schäden. Dabei handelt es sich um eine Regelung im Sinne des § 253 Abs. 1 BGB.[52] Der Schadensbegriff ist mithin weit auszulegen. Immaterielle Schäden sind aber wohl noch nicht anzunehmen, wenn die Verantwortlichen bloß gegen Ordnungsvorschriften (zum Beispiel Formalia) verstoßen.[53]

Für die Datentreuhand ist an dieser Stelle gemäß Erwägungsgrund 146 S. 1 DSGVO relevant, dass sie sowohl als Auftragsverarbeiterin als auch als (gemeinsam) Verantwortliche potenziell Adressatin von Haftungsansprüchen werden kann. Im Fall einer gemeinsamen Verantwortlichkeit haftet sie gesamtschuldnerisch für den verursachten Schaden und kann im Innenverhältnis nach Art. 82 Abs. 5 DSGVO unter Umständen Regressansprüche geltend machen. Die Datentreuhand kann sich der Haftung nur entziehen, wenn sie nachweisen kann, dass sie die Datenschutzvorschriften eingehalten hat.[54]

Datenschutzrechtlich Verantwortliche sind auch zivilrechtlich verantwortlich.[55] Im Rahmen dieser zivilrechtlichen Haftung kann ein geltend gemachter Schadensersatz sogar noch höher als die „öffentlich-rechtliche Bußgeldhaftung" nach der DSGVO ausfallen.[56] Immaterielle Schäden, etwa wenn Daten verloren gehen, sind dabei nicht immer leicht zu bestimmen. Der BGH hat dazu im Jahr 2008 entschieden,[57] dass die verantwortliche Person grundsätzlich Naturalrestitution in Form der Datenwiederherstellung nach § 249 BGB schuldet, jedoch nur, wenn die Daten an anderer Stelle (zum Beispiel ausgedruckt) noch existieren. Müssten sie dagegen neu geschaffen werden, handle es sich nicht um eine Wiederherstellung im Sinne der Norm. Dann besteht nur ein Anspruch auf Wertersatz nach § 251 Abs. 1 BGB. Werden keine Sicherungskopien angefertigt, kann es zu einem Mitverschulden derjenigen Person kommen, die eine andere angewiesen hat, ihre Daten zu verarbeiten. Der genaue Schaden kann im Einzelfall nach § 287 ZPO ermittelt werden. Grundlage, um den Wert der Daten zu bestimmen, sind die tatsächlichen Kosten für die Rekonstruktion, die wahrscheinlichen Kosten für die Rekonstruktion (bestimmen sich danach, welcher Aufwand in der Vergangenheit betrieben wurde), sowie Kosten, die aus der Störung von Betriebsabläufen wegen der gelöschten Daten folgen.

[51] *Stefan Korch*, Schadensersatz für Datenschutzverstöße, NJW 2021, S. 978 (979).
[52] *Kühling* (Fn. 36), S. 18.
[53] *Kühling* (Fn. 36), S. 18 f.
[54] *Kühling* (Fn. 36), S. 19.
[55] *Kühling* (Fn. 36), S. 18.
[56] *Kühling* (Fn. 36), S. 18.
[57] BGH, VI ZR 173/07.

Im Ergebnis sieht sich die Datentreuhand einem nicht zu unterschätzenden Haftungsrisiko ausgesetzt, das von dieser mit einer Haftpflichtversicherung weitestgehend mitigiert werden sollte. Dieses Risiko folgt nicht nur aus den hohen Bußgeldern und Schadensersatzsummen, sondern in besonderem Maße auch daraus, dass es im Einzelfall eine Abwägungsfrage bleibt, ob ausreichende Schutzmaßnahmen im Sinne der Art. 24, 25 und 32 DSGVO ergriffen wurden, oder die verantwortliche Person für eine Datenschutzverletzung und damit einem Schaden einstehen muss.

V. Privacy by Design und rechtssichere Datenverarbeitung in der medizinischen Forschung

Unmittelbar daran anknüpfend gilt es nun zu klären, welche Anforderungen an eine Datentreuhand mit Blick auf die Gewährleistung von Datenschutz und Datensicherheit (in der medizinischen Forschung) generell zu stellen sind, und wie diese rechtssicher von den Beteiligten festgestellt und umgesetzt werden können.

1. Privacy by Design

Sowohl in den Fällen, in denen die Datentreuhand Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO ist als auch in solchen, in denen sie Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO ist, muss sie sicherstellen, dass Datenschutz und -sicherheit nach der DSGVO eingehalten werden. *Privacy by Design* – Datenschutz durch Technikgestaltung – ist ein in Art. 25 Abs. 1 DSGVO verankertes Prinzip, nach dem die Verantwortlichen und Auftragsverarbeiter bei der Verarbeitung von personenbezogenen Daten, „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für Rechte und Freiheiten natürlicher Personen […] geeignete technische und organisatorische Maßnahmen“ ergreifen müssen, um die Datenschutzgrundsätze nach Art. 5 DSGVO wirksam umzusetzen.[58]

Im Kontext medizinischer Forschung sind diese Risiken aufgrund der sensiblen Daten besonders hoch. Die Datentreuhand wird daher in der Regel dazu verpflichtet sein, ein besonders hohes Schutzniveau zu gewährleisten: In diesem Bereich werden regelmäßig personenbezogene Daten besonderer Kategorien im Sinne des Art. 9 Abs. 1 DSGVO verarbeitet. Davon sind unter anderem genetische, biometrische und Gesundheitsdaten umfasst. Nach Art. 9 Abs. 1 DSGVO genießen diese Daten einen besonderen Schutz, und eine Verarbeitung ist dem Grundsatz nach untersagt. Daten dürfen nur in Ausnahmefällen nach Art. 9 Abs. 2 DSGVO verarbeitet werden; den wichtigsten Fall stellt Art. 9 Abs. 2 lit. a DSGVO dar, der die Verarbeitung von personenbezogenen Daten besonderer Kategorien dann erlaubt, wenn die Betroffenen ausdrücklich eingewilligt haben. Grund hierfür ist, dass diese Daten besonders

[58] Vgl. *Buchholtz/Brauneck/Schmalhorst* (Fn. 12), S. 209.

sensitive Informationen über die betroffenen Personen preisgeben. Führt eine Datentreuhand eine beachtliche Menge Daten – insbesondere sensibler Daten – zusammen, schafft sie dadurch ein weiteres Risiko für die datengebenden Patient:innen: Werden Daten über eine einzelne Person verknüpft und rekombiniert, können daraus ohne Einwilligung der datengebenden Person zusätzliche, sensible Informationen geschaffen werden. Schon mit wenigen Datenpunkten, die etwa über Sport- und Freizeitapplikationen wie Fitnessarmbänder gesammelt werden, kann zum Beispiel ein Risiko für bestimmte Krankheiten oder Störungen (wie eine Corona- oder Herzerkrankung oder ein Diabetesrisiko) erkannt werden.[59] Je mehr Daten (aus verschiedenen Quellen) zusammengeführt werden, desto mehr steigt das Risiko für solche ungewollten Diagnosen.[60]

Art. 9 Abs. 2 DSGVO enthält zehn Ausnahmetatbestände vom grundsätzlichen Verarbeitungsverbot in Art. 9 Abs. 1 DSGVO, die teils sehr hohe Anforderungen an Datenschutz und -sicherheit stellen. Von besonderem Interesse ist im Kontext der medizinischen Forschung neben der Verarbeitung aufgrund einer Einwilligung (Art. 9 Abs. 2 lit. a DSGVO) insbesondere Art. 9 Abs. 2 lit. j DSGVO: Danach dürfen Daten in Ausnahmefällen zu Forschungszwecken verarbeitet werden. Die Datentreuhand muss dabei angemessene und spezifische Maßnahmen einsetzen, um die Grundrechte und Interessen der Datengebenden zu wahren. *Angemessene und spezifische Maßnahmen* sind allerdings ein abstrakter Begriff, der konkretisiert werden muss. Ob eine Maßnahme im Sinne des Art. 9 Abs. 2 lit. j DSGVO angemessen ist, hängt unter anderen vom „Verarbeitungskontext, Verarbeitungsverfahren und -techniken und der kontextspezifischen Schutzbedürftigkeit der betroffenen Person" ab.[61] Diese Anforderung präzisiert Art. 89 Abs. 1 DSGVO,[62] wonach technische und organisatorische Maßnahmen (zum Beispiel Pseudonymisierung) die Rechte und Freiheiten (insbesondere den Grundsatz der Datenminimierung in Art. 5 Abs. 1 lit. c DSGVO) absichern sollen. §§ 27 Abs. 1, 22 Abs. 2 BDSG[63] konkretisieren

[59] *Martin Risch/Kirsten Grossmann/Stefanie Aeschbacher/Ornella Weideli/Marc Kovac/Fiona Pereira/Nadia Wohlwend/Corina Risch/Dorothea Hillmann/Thomas Lung/Harald Renz/Raphael Twerenbold/Martina Rothenbühler/Daniel Leibovitz/Vladimir Kovacevic/Andjela Markovic/Paul Klaver/Timo Brakenhoff/Billy Franks/Marianna Mitratza/George Downward/Ariel Dowling/Santiago Montes/Diederick Grobbee/Maureen Cronin/David Conen/Brianna Go odale/Lorenz Risch,* Investigation of the use of a sensor bracelet for the presymptomatic detection of changes in physiological parameters related to COVID-19: an interim analysis of a prospective cohort study (COVI-GAPP), 2022; *Jyoti Soni/Ujma Ansari/Dipesh Sharma/Sunita Soni*, Predictive Data Mining for Medical Diagnosis: An Overview of Heart Disease Prediction, International Journal of Computer Applications, 2011, S. 44; *Gabriele Buchholtz/Alissa Brauneck/Louisa Schmalhorst,* Was ist eigentlich … eine Datentreuhand, JuS 2023, 414, S. 415.

[60] *Buchholtz/Brauneck/Schmalhorst* (Fn. 59), S. 415.

[61] *Marion Albers/Raoul-Darius Veit*, Art. 9 DS-GVO, in: BeckOK DatenschutzR, Rn. 86, 103, 105 f.

[62] *Albers/Veit* (Fn. 61), Rn. 103.

[63] *Gernot Sydow*, in: Sydow/Marsch, DS-GVO-BDSG, 3. Auflage 2022, Rn. 55, 56, 58: Auch nach Inkrafttreten der DSGVO bleibt das BDSG weiterhin als „Begleit- und Durch-

den Begriff über Beispiele im nationalen Recht weiter. Sie nennen unter anderem die Möglichkeit, den Zugang zu den Daten zu beschränken und die etablierten Maßnahmen regelmäßig zu überprüfen.

Auch wenn die Pseudonymisierung von Daten eine effektive Maßnahme im Sinne von Art. 9 Abs. 2 lit. j i.V.m. Art. 89 Abs. 1 DSGVO sein kann, um Daten zu schützen, muss beachtet werden, dass pseudonyme Daten noch immer personenbezogen im Sinne der DSGVO sind. Solange ein „Schlüssel" existiert, können die datengebenden Personen weiterhin identifiziert werden, und ihre Daten bedürfen daher zusätzlicher Schutzmaßnahmen. Das ist insbesondere für die medizinische Forschung relevant, da sich etwa genetische Daten nicht anonymisieren und nur unter bestimmten Umständen[64] pseudonymisieren lassen: sie sind ihrer Natur nach hoch identifizierend.[65] In Fällen also, in denen (lediglich) pseudonymisierte bzw. sogar Rohdaten verarbeitet werden sollen, sind Sicherheitsmaßnahmen in der Regel nur dann angemessen im Sinne des Art. 32 DSGVO, wenn zusätzliche Vorkehrungen getroffen werden. Dazu gehört beispielsweise, Beteiligte zu sensibilisieren (vgl. § 22 Abs. 2 Nr. 3 BDSG), technische Maßnahmen wie Verschlüsselungen (Encryption) und Differential Privacy (eine Technik, die Daten unscharf bzw. ungenau macht, sodass die Identifikation erschwert wird) zu etablieren, und Authentifizierungsdienste einzurichten. Insofern kommt es sowohl bei der Etablierung als auch bei der Regulierung der Datentreuhand immer darauf an, die technischen Aspekte mitzudenken, durch die sich derartige Schutzmaßnahmen überhaupt erst umsetzen lassen.[66]

Um die Anforderungen von Privacy by Design gemäß Art. 25 Abs. 1 DSGVO zu erfüllen, ist die Datentreuhand im Rahmen einer Datenverarbeitung auch verpflichtet, die Grundsätze nach Art. 5 DSGVO einzuhalten: Dazu gehören insbesondere der Datenminimierungs- (Art. 5 Abs. 1 lit. c DSGVO) und der Richtigkeitsgrundsatz (Art. 5 Abs. 1 lit. d DSGVO). Letzterer kann es notwendig machen, die Identität von Patienten:innen und Proband:innen zu überprüfen.[67] Es ist ihnen nicht nur verboten, Daten zu verarbeiten, die grundlegend falsch sind, sondern teils auch solche, die bloß unvollständig sind.[68] Was aus datenschutzrechtlicher Perspektive notwendig ist, um unrichtige Daten zu identifizieren und zu korrigieren, ist vom Einzelfall abhängig. Die Datentreuhand muss jedenfalls dann gewährleisten, dass Daten überprüft

führungsgesetz[]" relevant und trifft eine Reihe abweichender Regelungen. Dies ermöglichen die Öffnungsklauseln in der DSGVO sogar bezüglich hochsensibler Daten (vgl. Art. 9 Abs. 2 lit. a, b, j, Abs. 4 DSGVO).

[64] *GMDS*, Arbeitshilfe zur Pseudonymisierung/Anonymisierung, 2018, S. 15, https://gesundheitsdatenschutz.org/download/Pseudonymisierung-Anonymisierung.pdf.

[65] *Colin Mitchel/Johan Ordish/Emma Johnson/Tanya Bridgen/Alison Hall,* The GDPR and genomic data. The impact of the GDPR and DPA 2018 on genomic healthcare and research, 2020, S. 36.

[66] So etwa bei *Buchholtz/Brauneck/Schmalhorst* (Fn. 12), S. 209 ff.

[67] *Pommerening/Drepper/Helbing/Ganslandt* (Fn. 19), S. 106, 178.

[68] *Alexander Roßnagel,* in: Sinitis/Hornung/Spieker gen. Döhmann, Datenschutzrecht, 2019, Rn. 139.

werden, wenn ihr Informationen vorliegen, dass diese potentiell unrichtig sind.[69] Aufgrund des Transparenzgrundsatzes (Art. 5 Abs. 1 lit. a DSGVO), der darauf beruhenden Informationspflichten des Verarbeitenden (Art. 12 ff. DSGVO) und des Rechenschaftsgrundsatzes (Art. 5 Abs. 2 DSGVO), ist es darüber hinaus notwendig, dass die Datentreuhand alle Verarbeitungsschritte, Zugriffsrechte sowie technische und organisatorische Maßnahme überwacht und protokolliert. Die Datentreuhand muss zudem verhindern, dass unbefugte Personen auf die Daten zugreifen, und eine angemessene Datensicherheit gewährleisten (Art. 5 Abs. 1 lit. f DSGVO).

Die Datentreuhand im medizinischen Sektor muss im Ergebnis also hohen Ansprüchen gerecht werden. Zu datenschutzrechtlichen Standardproblemen gehören neben unberechtigten Datenverarbeitungen (Datenlecks, Hackerangriffe, interne Missbräuche) auch die zusätzlichen Anforderungen, die Art. 45 und 46 DSGVO an Datentransfers in Staaten außerhalb der EU den Verantwortlichen und Auftragsverarbeitenden aufgeben. Danach muss die Europäische Kommission entweder feststellen, dass der Drittstaat bzw. die involvierten Organisationen ein angemessenes Schutzniveau bieten (Art. 45 Abs. 1 DSGVO), oder die Verantwortlichen oder Auftragsverarbeitenden müssen geeignete datenschutzrechtliche Garantien gegeben haben (Art. 46 Abs. 1 DSGVO). Für die medizinische Forschung gerade zu seltenen Krankheiten sind internationale Datenverarbeitungen aber hoch relevant,[70] um Zugriff auf ausreichend große Datensätze zu haben, um aussagekräftige Ergebnisse zu erzeugen. Allein im Jahr 2019 arbeiteten Forscher aus der EU und das US National Cancer Institute gemeinsam an etwa 5.000 Projekten zur Krebsforschung.[71]

2. Vorschlag: Schutzklassen bestimmen und Risiken quantifizierbar machen

Die geschilderten Herausforderungen werfen die Frage auf, welche konkreten Maßnahmen getroffen werden müssen, um dem hohen Schutzniveau gerade in der medizinischen Forschung gerecht zu werden. Art. 25 Abs. 1 DSGVO sieht vor, dass sich die technischen und organisatorischen Maßnahmen der Verantwortlichen und der Auftragsverarbeiter an dem Umfang, den Umständen und dem Zweck der Verarbeitung sowie der „unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen" orientieren müssen. Durch diese Maßnahmen soll ein „angemessenes Schutzniveau" im Sinne des Art. 32 Abs. 1 DSGVO gewährleistet werden. Diese

[69] *Peter Schantz,* in: Wolff/Brink BeckOK Datenschutzrecht, 2021, Rn. 29.

[70] *Heidi Bentzen/Rosa Castro/Robin Fears/George Griffin/Volker ter Meulen/Giske Ursin*, Remove obstacles to sharing health data with researchers outside of the European Union, Nature Medicine, 2021, S. 1329 (1329 – 1330).

[71] The ALLEA, EASAC and FEAM joint initiative on resolving the barriers of transferring public sector data outside the EU/EEA, International Sharing of Personal Health Data for Research, 2021, 32, https://www.feam.eu/wp-content/uploads/International-Health-Data-Transfer_2021_web.pdf (25. 10. 2022).

Pflicht trifft auch die Datentreuhand; entweder in der Rolle als Verantwortliche oder als Auftragsverarbeiterin. Stellt sie dieses Schutzniveau nicht sicher, haftet sie nach den oben dargestellten Maßstäben. Um zu bestimmen, was im Einzelfall angemessene Maßnahmen sind, soll hier ein Schutzklassenkonzept vorgeschlagen werden. Mit diesem Konzept lassen sich Daten in verschiedene Risikogruppen einordnen. Gleichzeitig zeigt es jeweils auf, welche Maßnahmen ergriffen werden müssen, um die Daten datenschutzkonform zu verarbeiten. Wie hoch das Risiko für bestimmte Daten einzuschätzen ist, hängt davon ab, wie sensibel die Informationen über eine natürliche Person sind, die durch die Daten ermittelt werden können, und wie groß die Gefahr ist, dass es tatsächlich zu einer unbeabsichtigten Offenlegung dieser Daten kommt.

Orientierung für ein solches Konzept können hier Schutzklassen bieten, zu denen im Bereich datenschutzrechtlicher Zertifizierungen bereits umfangreiche Konzepte vorliegen.[72] An diese angelehnt, wird hier ein Vorschlag unterbreitet, der zwischen fünf Schutzklassen unterscheidet: Klasse 0 umfasst Daten, die nicht besonders geschützt werden müssen, und Klasse 3+ Daten, für die nicht pauschal angemessene Sicherheitsmaßnahmen genannt werden können, weil aus deren Verarbeitung Gefahren für das körperliche Wohlbefinden der datengebenden Person folgen.

Im ersten Schritt werden die Daten und Verarbeitungsprozesse nach ihrer Art beurteilt und dem jeweiligen Risiko für die datengebenden Personen entsprechend in Klassen eingeordnet.

Schutzklasse	Beschreibung
0: Daten ohne Schutzbedarf	Datenverarbeitungsvorgänge, die keine Aussagen über schützenswerte persönliche Verhältnisse natürlicher Personen enthalten, erzeugen, unterstützen oder ermöglichen. Auf solche Daten (nicht-personenbezogene Daten) ist die DSGVO nicht anwendbar.
1: Daten mit niedrigem Schutzbedarf	Datenverarbeitungsvorgänge, die Aussagen über die persönlichen Verhältnisse der betroffenen Person aufgrund der enthaltenen Daten und der konkreten Erhebung, Verarbeitung oder Nutzung dieser Daten enthalten, erzeugen, unterstützen oder ermöglichen. Hierunter können z. B. Informationen über Wohnort, Augenfarbe oder Alter fallen.
2: Daten mit mittlerem Schutzbedarf	Datenverarbeitungsvorgänge, die aufgrund der verwendeten Daten oder der konkreten Erhebung, Verarbeitung oder Nutzung dieser Daten eine Aussagekraft über die Persönlichkeit oder die Verhältnisse einer Person (Betroffener) haben, unterstützen oder bewirken können. Die unbefugte Verarbeitung oder Nutzung solcher Daten kann zu einem Nachteil für die betroffene Person führen (Beeinträchtigung von Rechtsgütern). Hierunter können z. B. Daten fallen, die Rückschlüsse auf politische Anschauungen oder finanzielle Umstände einer Person zulassen.

[72] *Kompetenzzentrum Trusted Cloud*, Arbeitspapier – Schutzklassen in der Datenschutz-Zertifizierung 2015, https://www.rechtsinformatik.saarland/images/pdf/tc-de/09_Arbeitspapier_Schutzklassen-in-der-Datenschutz-Zertifizierung.pdf (16. 10. 2022); *LfD Niedersachen*, Schutzstufenkonzept 2018, https://lfd.niedersachsen.de/startseite/themen/technik_und_organisation/schutzstufen/schutzstufen-56140.html (26.10.22).

Schutzklasse	Beschreibung
3: Daten mit hohem Schutzbedarf	Datenverarbeitungsvorgänge, die aufgrund der verwendeten Daten oder der konkreten Erhebung, Verarbeitung oder Nutzung dieser Daten eine erhebliche Aussagekraft über die Persönlichkeit oder die Verhältnisse einer Person (Betroffener) haben, unterstützen oder zur Folge haben können. Die unbefugte Erhebung, Verarbeitung oder Nutzung dieser Daten kann zu schwerwiegenden Nachteilen für die betroffene Person führen. Hierunter können z. B. Daten über die psychische Gesundheit einer Person fallen.
3+: Daten mit sehr hohem Schutzbedarf	Datenverarbeitungsvorgänge, die aufgrund der verwendeten Daten oder der konkreten Erhebung, Verarbeitung oder Nutzung dieser Daten eine erhebliche Aussagekraft über die Persönlichkeit oder die Verhältnisse einer Person (Betroffener) haben, unterstützen oder zur Folge haben können. Die unbefugte Erhebung, Verarbeitung oder Nutzung solcher Daten kann zu einer erheblichen Beeinträchtigung des Lebens, der Gesundheit oder der Freiheit der betroffenen Person führen. Hierunter können z. B. Daten fallen, die V-Leute identifizieren.

Das Risiko für die Daten wird aber auch durch die Verarbeitungsumstände beeinflusst. Diese müssen im zweiten Schritt berücksichtigt werden. Werden beispielsweise nicht zwangsläufig identifizierende Daten einer Person wie Alter, Krankheit und Geschlecht zusammengeführt, erhöht sich das Risiko einer Identifizierung und damit auch die Schutzklasse. Das ist insbesondere der Fall, wenn einzelne Datenpunkte von der Norm abweichen, wie beispielsweise ein ungewöhnlich hohes Alter in Kombination mit einer seltenen Krankheit. Umgekehrt kann eine besonders risikolose Verarbeitung dazu führen, dass die Schutzklasse gesenkt wird. Das ist zum Beispiel anzunehmen, wenn eine Studie mit einer so großen Menge homogener Daten arbeitet, bei denen die Daten auf so viele verschiedene Personen zutreffen könnten, dass keine einzelne Person identifiziert werden kann. Um die jeweils einschlägige Schutzklasse auf Grundlage des den Daten inhärenten Risikos und der Verarbeitungsumstände im Einzelfall ermitteln zu können, soll ein Fragenkatalog alle Daten verarbeitenden Personen unterstützen.

Auch die Datentreuhand könnte dieses Schutzklassenkonzept nutzen, um auf der einen Seite zu bestimmen, welche organisatorischen und technischen Maßnahmen sie selbst treffen muss, um Daten innerhalb ihrer Aufgabenbereiche datenschutzkonform zu verarbeiten. Auf der anderen Seite ist es angesichts der hohen Haftungsrisiken, denen eine Datentreuhand ausgesetzt sein kann, von besonderem Interesse, dass offizielle Leitfäden wie etwa die hier dargestellten Schutzklassen etabliert werden, um eine verlässliche Orientierung zu bieten.

VI. Datenzugang: Datenaltruismus oder Verpflichtung zur Datenteilung

Wenn geklärt ist, nach welchen datenschutzrechtlichen Vorgaben und innerhalb welchen Rahmens die Datentreuhand Daten verwalten können soll, muss weiter überlegt werden, woher schließlich die Daten kommen sollen, d. h. nach welchen Re-

geln die Datentreuhand ihr Treugut erlangen sollte. Eine Datentreuhand kann die Daten entweder aufgrund altruistischer – das heißt freiwilliger und uneigennütziger – Entscheidungen der datengebenden Personen oder von Gesetzes wegen erhalten. Auf diese Art des Datenteilens setzt unter anderem auch der DGA. Ein altruistischer Ansatz erhält den datengebenden Personen eine weitgehende Kontrolle über ihre Daten. Die Datentreuhand könnte als Verwalterin eines Datenpools agieren, in den Personen freiwillig ihre Daten einspeisen und auf den Datennutzende zu festgelegten Zwecken zugreifen dürfen. Ein Schwerpunkt der Datentreuhand-Tätigkeit liegt in diesem Fall im Einwilligungsmanagement und darin, zu gewährleisten, dass die Daten nur den festgelegten Zwecken nach durch berechtigte Personen verarbeitet werden.

Aus der Perspektive der Forschenden sind jedoch zwingende oder jedenfalls Opt-Out-Konzepte vorzuziehen, die ihnen – anders als eine altruistisch gespeiste Datenbank, die auf die Bereitschaft und Initiative von Personen, ihre Daten freizugeben, angewiesen ist – einen langfristigen Zugriff auf geeignete Daten in ausreichender Menge sichern.[73] Für die Forschung sind zudem gerade auch Sekundärnutzungen von Daten (zum Beispiel aus der ePA) von Interesse;[74] Einzelheiten und Umfang von Sekundärnutzungen sind jedoch von der ursprünglichen Einwilligung häufig noch nicht umfasst, sodass Forschende eine neue Einwilligung einholen müssten, um die Daten verarbeiten zu dürfen. Aus diesen Gründen werden Ansätze, die von dem Erfordernis einer Einwilligung zur Datenfreigabe absehen, vermehrt verfolgt. Auch die Politik hat diesen Bedarf erkannt. Sowohl der Beschluss des Bundesrats zum GDNG[75], als auch der GDNG-Entwurf der Bundesregierung zielen darauf ab, (Gesundheits-)Daten – unter anderem durch Einsatz eines Opt-Out-Verfahrens bei der ePA[76] – besser wissenschaftlich nutzbar zu machen.[77] Gleiches gilt für die geplante Verordnung des Europäischen Parlaments und des Rates über den europäischen Raum für Gesundheitsdaten (European Health Data Space, EHDS),[78] wonach eine sekundäre Nutzung von Gesundheitsdaten auch unabhängig von der Einwilligung

[73] S. hierzu *Julian Olk,* Der Industrieverband drängt auf Datenspende – Hindernis Datenschutzgrundverordnung, Handelsblatt, 2019, https://www.handelsblatt.com/politik/deutschland/gesundheitspolitik-industrieverband-draengt-auf-datenspende-hindernis-datenschutz-grundverordnung/25363570.html (28. 10. 2022); s. hierzu ärzteblatt, Hecken plädiert für verpflichtende Datenspende, 2018, https://www.aerzteblatt.de/nachrichten/99900/Hecken-plaediert-fuer-verpflichtende-Datenspende (28. 10. 2022).

[74] *Martin Jungkunz/Anja Köngeter/Eva Winkler/Katja Mehlis/Christoph Schickhardt*, in: Jungkunz/Köngeter/Winkler/Mehlis/Schickhardt, Sekundärnutzung klinischer Daten in datensammelnden, nicht-interventionellen Forschungs- oder Lernaktivitäten – Begriff, Studientypen und ethische Herausforderungen, 2021, S. 71 (78).

[75] BR-Drs. 597/22, S. 1 (2).

[76] BR-Drs. 597/22 (Fn. 75), S. 2; siehe hierzu auch *Deister* (Fn. 4), S. 12.

[77] BR-Drs. 597/22 (Fn. 75), S. 2; *Bundestag* (Fn. 8), S. 84; vgl. Wissenschaftsrat, Digitalisierung und Datennutzung für Gesundheitsforschung und Versorgung. Positionen und Empfehlungen, S. 63, https://www.wissenschaftsrat.de/download/2022/9825-22.pdf?__blob=publicationFile&v=11 (3. 5. 2023).

[78] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den europäischen Raum für Gesundheitsdaten, COM(2022) 197 final vom 3. 5. 2022.

der Betroffenen, und ohne dass die Betroffenen über die Datenverarbeitung unterrichtet werden,[79] gestattet sein soll (im Detail geregelt in den Art. 33 ff. des EHDS-Verordnungsentwurfs).[80] Danach müssten zum Beispiel Daten aus der ePA verpflichtend zur Verfügung gestellt werden. Eine Schlüsselposition nimmt nach dem GDNG-Entwurf und auch nach dem EHDS-Verordnungsvorschlag das Forschungsdatenzentrum (FDZ) ein. Gemäß § 363 SGB V verarbeitet das FDZ die Daten aus der ePA, die zu Forschungszwecken freigegeben wurden: Insbesondere verwaltet es gemäß § 303d Abs. 1 SGB V die Daten und gewährt Datennutzenden zu Forschungszwecken Zugriff auf die Daten; damit erfüllt das FDZ nach dem hier vertretenen Verständnis die Rolle einer Datentreuhand.

Diese Entwicklungen zugunsten der medizinischen Forschung bringen allerdings erhebliche Risiken für die Patientensouveränität mit sich. Das gilt zumindest für den Fall, dass diese ihre Daten gerade nicht für eine sekundäre Nutzung freigeben wollen. Schon ein Opt-Out-Verfahren wie es der Beschluss des Bundesrates und der GDNG-Entwurf der Bundesregierung vorsehen, lässt den Datengebenden zwar noch die Option, einer Datenverarbeitung zu widersprechen, macht aber den Eingriff in die Patientensouveränität zum Status Quo. Umstritten ist in diesem Zusammenhang vor allem auch die Regelung im EHDS-Verordnungsentwurf, durch die eine sekundäre Nutzung von Gesundheitsdaten sogar kommerziellen Nutzer:innen auch ohne Einwilligung der Betroffenen ermöglicht wird (Art. 33 Abs. 5 EHDS-Verordnungsentwurf).[81] Dies kann sich insbesondere auf Patient:innen mit seltenen Krankheiten und in der Folge stark identifizierenden Gesundheitsdaten negativ auswirken.[82] Das Europäische Parlament plant daher Sekundärnutzungen dahingehend zu limitieren, dass diese dem allgemeinen Interesse der Gesellschaft („general interest of the society“) dienen müssen.[83] Um Patientensouveränität weitgehend gewährleisten zu können, sollte daher in jedem Fall die Möglichkeit eines Widerspruchs erhalten bleiben.

[79] Stellungnahme der Kassenärztlichen Bundesvereinigung zum europäischen Gesundheitsdatenraum vom 16. 12. 2022, S. 8.

[80] Im Hinblick auf diese Regelung wurde der EHDS-Verordnungsentwurf vom 3. 5. 2022 stark kritisiert, sodass schließlich am 13. 12. 2023 mehrheitlich ein entsprechender Änderungsantrag vom 7. 12. 2023 angenommen wurde, wonach „natürlichen Personen ein Widerspruchsrecht gegen die Registrierung ihrer personenbezogenen Daten in einem EHR-System [(electronic health records)]“ eingeräumt wird, Änderungsantrag vom 7. 12. 2023, https://www.europarl.europa.eu/RegData/seance_pleniere/textes_deposes/prop_resolution/2023/0395/amendements/P9_AMA(2023)0395(555-555)_DE.pdf (22. 1. 2024).

[81] *Michael Denga*, EuZW 2023, S. 25 (30).

[82] *Denga* (Fn. 80), S. 30.

[83] „In particular, the secondary use of health data for research and development purposes should contribute to a benefit to society in the form of new medicines, medical devices, health care products and services at affordable and fair prices for Union citizens, as well as enhancing access to and the availability of such products and services in all Member States“, Europäisches Parlament, DRAFT COMPROMISE AMENDMENTS, 2022/0140(COD) 24. 11. 2023, S. 20 (Rn. 41).

VII. Flankierende Maßnahmen – Kontrolle und Zertifizierung

Neue Konstrukte wie die Datentreuhand lassen sich nur dann erfolgreich etablieren, wenn ihnen das notwendige Vertrauen von den Datengebenden und Datennutzenden entgegengebracht wird. Dies ist umso wichtiger, wenn die Datentreuhand im Kontext der medizinischen Forschung hochsensible Gesundheitsdaten verarbeiten soll. Für die datengebenden Personen kommt es dabei insbesondere darauf an, dass die Datentreuhand ihre Interessen und Rechte hinreichend wahrnimmt bzw. schützt. Aber auch Datennutzende (etwa Forschende) müssen sich auf die Integrität der Datentreuhand verlassen können. Um also alle Beteiligten vor einem missbräuchlichen Verhalten der Datentreuhand weitgehend zu schützen, gibt es verschiedene Stellschrauben.

1. Aufsicht

Der Staat kann die Datentreuhand unter seine Aufsicht stellen[84] und ihre Entscheidungen überprüfen. Zunächst ist die Datenschutzaufsichtsbehörde dafür zuständig, sicherzustellen, dass der Datenschutz eingehalten wird (vgl. Art. 58 DSGVO).[85] Ihre Aufgaben sollten aber angelehnt an Stiftungsaufsichten erweitert werden oder es sollte eine datentreuhandspezifische Aufsicht eingeführt werden: Bei der Datentreuhand hätte die Aufsichtsbehörde zu prüfen, ob diese nicht vom festgelegten Zweck abweicht und ihre Vertrauensposition nicht missbraucht.[86] Eine Datentreuhand sollte von dieser Aufsicht nur ausgenommen sein, wenn sie lediglich zu persönlichen und familiären Zwecken tätig wird.[87] Aufgabe der Aufsichtsbehörde soll nicht nur sein, Fehlentscheidungen entgegenzuwirken, sondern auch die Vertrauenswürdigkeit der Datentreuhand selbst zu überprüfen: Hat sich eine Datentreuhand einer bestimmten Straftat schuldig gemacht, aufgrund derer ihr die notwendige Zuverlässigkeit fehlt (zum Beispiel Betrugsdelikte), kann die Behörde ihr (nach dem Vorbild des Vereinigten Königreichs[88]) verbieten, als Datentreuhand tätig zu sein.

[84] Vgl. *Richard Nolan*, „The execution of Trust shall be under the control of the court": A Maxim in Modern Times, 2016, S. 469 (470–474); vgl. *Birgit Weitemeyer*, § 80 BGB, in: MükoBGB, 2021, § 80 Rn. 68; *Buchholtz/Brauneck/Schmalhorst* (Fn. 18), S. 208.

[85] Vgl. *Cornelia Kibler,* Datenschutzaufsichtsbehörden und ihre Stellung im europäischen Verwaltungsraum, NVwZ 2021, S. 1676 (1676 f.).

[86] *Weitemeyer* (Fn. 83), Rn. 51.

[87] S. hierzu Familienstiftungen: *Weitemeyer* (Fn. 83), Rn. 180.

[88] Vgl. *Charity Commission for England and Wales*, Trustee board: people and skills, aktualisiert 2014, https://www.gov.uk/guidance/trustee-board-people-and-skills, (08. 09. 2022); *Buchholtz/Brauneck/Schmalhorst* (Fn. 12), S. 208.

2. Zertifizierung und Akkreditierung

Eine Datentreuhand könnte durch den Staat oder über privat handelnde, akkreditierte[89] Organisationen[90] verpflichtend für die Verwaltung und Verarbeitung sensibler Daten zertifiziert werden, um das Vertrauen der Datengebenden und Datennutzenden zu steigern.[91] Bisher gibt es in Deutschland allerdings noch keine Stellen, die Datentreuhandmodelle zertifizieren können. Wenngleich das Bundesministerium für Bildung und Forschung ein Zulassungs- oder Akkreditierungsverfahren anstrebt,[92] liegt für die Ausgestaltung von Akkreditierungsstellen und Zulassungsvoraussetzungen noch kein Konzept vor. Die Zertifizierung stellt allerdings ein sinnvolles Instrument dar, um die Einhaltung bestimmter Standards sicherzustellen: So kann belegt werden, dass die Datentreuhand über organisatorische und technische Maßnahmen verfügt, um sicherzustellen, dass Datenschutzstandards und -normen eingehalten und Missbrauch entgegengewirkt wird.[93] Darüber hinaus könnten auch die IT-Sicherheit[94] oder das Vorhandensein von sicheren Datenzugriffsverfahren sowie hinreichende Rechenschaftspflichten der Datentreuhand Gegenstand der Zertifizierung sein.[95] Die Zertifizierung schafft zudem Transparenz gegenüber den datengebenden Personen hinsichtlich verbleibender Risiken.[96] Regelmäßige Rezertifizierungen sind wichtig, um sicherzustellen, dass die Maßnahmen an die sich schnell ändernden technischen Möglichkeiten angepasst werden.

3. Finanzierungsmöglichkeiten

Ein nachhaltiges Finanzierungsmodell ist notwendig, um die Etablierung von Treuhandverhältnissen zu fördern. Wie dieses ausgestaltet ist, kann sich auf das Vertrauen der Datengebenden auswirken. Teilweise wird gefordert, dass die Datentreuhand die Daten selbst nicht monetarisieren darf, um keinen Anreiz dafür zu schaffen,

---

[89] Akkreditierungen können durch die Deutsche Akkreditierungsstelle GmbH erfolgen, https://www.dakks.de/de/home.html (24. 05. 2023).

[90] *Oxfords Insights,* Report. Data Trust Certification, 2019, S. 1 (7 f.).

[91] *Richter* (Fn. 34), S. 643; *Buchholtz/Brauneck/Schmalhorst* (Fn. 12), S. 208; Rat für Informationsinfrastrukturen, Datentreuhänder: Potentiale, Erwartungen, Umsetzung, https://rfii.de/download/rfii-workshopbericht-datentreuhaender-potenziale-erwartungen-umsetzung-februar-2021/ (26. 10. 2022), S. 1 (4).

[92] Vgl. *Bundesministerium für Bildung und Forschung,* Bekanntmachung, 2021, https://www.bmbf.de/bmbf/shareddocs/bekanntmachungen/de/2021/01/3292_bekanntmachung.html (24. 05. 2023).

[93] *Blankertz/Specht* (Fn. 32), S. 3.

[94] *Blankertz/Specht* (Fn. 32), S. 27.

[95] *Sabrina Martin/Walter Pasquarelli*, „Exploring Data Trust Certifications", Oxford Insights, 2019, S. 1 (6).

[96] *Blankertz/Specht* (Fn. 32), S. 5.

möglichst häufig (und auch unrechtmäßig) Daten zu mitteln.[97] Ein besonders hohes Missbrauchspotential besteht dann, wenn die Vergütung der Datentreuhand unmittelbar an die Menge der Daten, die sie mittelt, oder die Anzahl der Zugriffe, die sie erlaubt, geknüpft ist.[98] Die Monetarisierung sollte jedoch nicht gänzlich ausgeschlossen sein, um eine möglichst schnelle und flächendeckende Etablierung der Datentreuhand zu fördern:[99] Ohne Monetarisierung der Daten blieben nur die Möglichkeiten, Datentreuhandmodelle über den Staat,[100] durch Spenden oder über Nebentätigkeiten[101] wie Informations-, Beratungs-, oder Zertifizierungsdienste zu finanzieren. Fraglich ist dabei allerdings, ob die Datentreuhand dadurch über ausreichende Mittel verfügt, um sowohl laufende Kosten, als auch Investitionen in ihre Fortentwicklung decken zu können. Im Interesse der Forschung sollten den Kosten der Datennutzung aber Grenzen gesetzt werden. Dies lässt sich entweder durch eine gesetzliche Deckelung der Kosten oder staatliche Subventionen für Forschende erreichen.[102]

VIII. Fazit und Ausblick

Die Datentreuhand kann dabei helfen, dem aufgezeigten Spannungsverhältnis zwischen Forschungsinteressen einerseits und Patientensouveränität andererseits effektiv zu begegnen. Damit dies gelingen kann, ist auch der Gesetzgeber gefragt. Insbesondere sollte sich der Gesetzgeber aus Gründen der Rechtssicherheit um eine allgemein anerkannte Definition und eine rechtliche Einordnung der Datentreuhand bemühen. Zu hohe Hürden machen Datenaltruismus – als eine wichtige Form des Datenteilens – unattraktiv.[103]

Generell lässt sich die Datentreuhand nur dann erfolgreich etablieren, wenn sie eine berechtigte Vertrauensposition einnimmt. Dazu müssen, bevor es zu einer Verarbeitung von Daten durch die Datentreuhand kommt, Fragen der Verantwortlichkeit und den damit einhergehenden Haftungsrisiken geklärt werden. Eine entscheidende Rolle dabei können staatliche Maßnahmen spielen, die darauf gerichtet sind, das Missbrauchsrisiko zu senken: namentlich Zertifizierung, Akkreditierung und Auf-

[97] Vgl. *Aline Blankertz/Louisa Specht-Riemenschneider*, Neue Modelle ermöglichen. Regulierung für Datentreuhänder, böll-brief, 2021, S. 1 (8).

[98] Vgl. *Blankertz/Specht-Riemenschneider* (Fn. 96), S. 8.

[99] Vgl. *Blankertz/Specht-Riemenschneider* (Fn. 96), S. 8 f.; Für ein Verbot siehe nur: *Hans-Günter Lind/Hanns Suckfüll*, Initiative zu einer deutschen Daten-Treuhand (DEDATE) als Ultima Ratio der Persönlichen Digitalen Datenwirtschaft (PDD), S. 1 (16 f.).

[100] Vgl. *Blankertz/Specht-Riemenschneider* (Fn. 96), S. 7.

[101] Vgl. *Blankertz/Specht-Riemenschneider* (Fn. 96), S. 8.

[102] Vgl. auch: Statistische Ämter des Bundes und der Länder, Entgelt für die Datennutzung, https://www.forschungsdatenzentrum.de/de/entgelte (23. 05. 2023).

[103] *Winfried Veil,* Datenaltruismus: Wie die EU-Kommission eine gute Idee versemmelt, 2020, https://www.cr-online.de/blog/2020/12/01/datenaltruismus-wie-die-eu-kommission-eine-gute-idee-versemmelt/ (23. 05. 2023).

sicht durch Behörden. Um einen transparenten Umgang mit Haftungsrisiken möglich zu machen, sollte auf geeignete Konzepte, wie etwa das hier vorgeschlagene Schutzklassenkonzept zurückgegriffen werden. Davon könnten sowohl die Datentreuhand als auch die Datennutzenden profitieren. Schlussendlich ist es wichtig, dass von der Datentreuhand „echte Verbesserungen für die Privatsphäre der Nutzer“[104] und mithin für die Patientensouveränität ausgehen. Bei allen Bestrebungen ist eine interdisziplinäre Zusammenarbeit zwischen Recht und Technik zentral. Nur wenn diese beiden Disziplinen im Sinne von Privacy by Design bei der Entwicklung und Erprobung von Datentreuhandmodellen sinnvoll zusammenarbeiten, lassen sich zukunftsfähige Konzepte entwickeln.

Literatur

Blankertz, Aline/*Specht-Riemenschneider*, Louisa: Neue Modelle ermöglichen. Regulierung für Datentreuhänder, böll-brief, 2021.

Blankertz, Aline/*Specht-Riemenschneider*, Louisa: Wie eine Regulierung für Datentreuhänder aussehen sollte, 2021, https://www.stiftung-nv.de/sites/default/files/regulierung_fuer_datentreuhaender.pdf.

Buchholtz, Gabriele/*Brauneck*, Alissa/*Schmalhorst*, Louisa: Gelingensbedingungen der Datentreuhand – rechtliche und technische Aspekte, NVwZ 2023, S. 206.

Bundesregierung: Datenstrategie der Bundesregierung. Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Kabinettfassung, 27.01.2021, https://www.bundesregierung.de/resource/blob/992814/1845634/f073096a398e59573c7526feaadd43c4/datenstrategie-der-bundesregierung-download-bpa-data.pdf.

Kompetenzzentrum Trsuted Cloud: Arbeitspapier – Schutzklassen in der DatenschutzZertifizierung 2015, https://www.rechtsinformatik.saarland/images/pdf/tc-de/09_Arbeitspapier_Schutzklassen-in-der-Datenschutz-Zertifizierung.pdf.

Kühling, Jürgen: Der datenschutzrechtliche Rahmen für Datentreuhänder. Chance für mehr Kommerzialisierungsfairness und Datensouveränität?, ZfDR 2021, S. 1.

LfD Niedersachsen: Schutzstufenkonzept 2018, https://lfd.niedersachsen.de/startseite/themen/technik_und_organisation/schutzstufen/schutzstufen-56140.html.

Pommerening, Klaus/*Drepper*, Johannes/*Helbing*, Krister/*Ganslandt*, Thomas: Leitfaden zum Datenschutz in Medizinischen Forschungsprojekten: Generische Lösungen Der TMF 2.0., S. 1.

Richter, Heiko: Europäisches Datenprivatrecht: Lehren aus dem Kommissionsvorschlag für eine „Verordnung über europäische Daten-Governance“, ZEuP 2021, S. 634.

Weitemeyer, Birgit: § 80 BGB, in: MükoBGB, 2021, § 80.

[104] *Kühling/Sackmann/Schneider* (Fn. 50), S. 1 (26 f.).