Teil II. Schlussbericht (2024) AP2/AP3
Datenschutzrechtliches Reallabor für eine Datentreuhand in der Netzwerkmedizin – TrustDNA / 16DTM108A / Berichtszeitraum: 01.01.2022 – 31.12.2024

Autoren: Noemi Aguirre Chan, Anna Lina Gummersbach, Marc Nestor, Fruzsina Molnár-Gábor

A. Einleitung

Dieser Bericht dient dazu, eine detaillierte Übersicht zum Abschluss der Bearbeitung von AP2 und AP3 im rechtswissenschaftlichen Teilprojekt des TrustDNA Verbundvorhabens im Berichtzeitraum vom 01.01.2022 bis 31.12.2024 zu liefern.

Im Bereich AP2 widmeten wir uns den Bedingungen einer Zurverfügungstellung von Gesundheitsdaten durch eine Datentreuhand in der Netzwerkmedizin und analysierten dazu die datenschutzrechtlichen Grundlagen (B.). Dies betraf die institutionelle und organisatorische Ausgestaltung von Datentreuhändern (I.), den Zusammenhang zwischen Aufgaben und Rollen (II.), die Vertrauenswürdigkeit von Datentreuhändern (III.), den Rechtsvergleich mit dem Vereinigten Königreich (IV.) und die datenschutzrechtliche Perspektive auf Datentreuhänder und Gesundheitsdateninfrastrukturen (V.). Die Entwicklung eines dynamischen Einwilligungskonzeptes (M2.a) (C.) und die Erstellung von Handreichungen und SOPs (M2.b) (D.) wurden unter Berücksichtigung relevanter, aktueller Entwicklungen im Bereich der nationalen und europäischen Gesetzgebung fertiggestellt. Ferner wurde eine Toolbox zu technischen und organisatorischen Maßnahmen (TOMs) (M3) erstellt / die Untersuchung zu technischen und organisatorischen Maßnahmen (TOMs) im rechtswissenschaftlichen Teilprojekt abgeschlossen (E.). Des Weiteren wird nachfolgend ein Überblick zum Austausch und projektbezogener Vorträge gegeben (F.). Abschließend werden die Publikationen aufgelistet (G.) und im Rahmen eines Ausblicks der voraussichtliche Nutzen der Ergebnisse dargestellt (H.). Der Schwerpunkt dieses Berichts liegt auf der Darstellung des Rechtsvergleichs mit dem Vereinigten Königreich, der datenschutzrechtlichen Perspektive der Datentreuhänder und des Einwilligungskonzepts.

Unterstützt wurden wir von zwei Honorarkräften und zwei studentischen Hilfskräften, die wesentlich zum Gelingen des rechtswissenschaftlichen Teilprojekts beigetragen haben.

Während der Durchführung des Teilprojekts wurde der für Datentreuhänder, insbesondere an der Schnittstelle zwischen Versorgung und Forschung, relevante rechtswissenschaftliche Stand (mit einem Fokus auf das Datenschutzrecht) national und auf europäischer Ebene in die Untersuchungen einbezogen. Siehe dazu entsprechende Hinweise.

B. Datenschutzrechtliche Grundlagen für einen Datentreuhänder in der Netzwerkmedizin

I. Institutionelle und organisatorische Ausgestaltung

Weder die Europäische Datenschutz-Grundverordnung (DSGVO)[1] noch der Data Governance Act (DGA)[2] geben zwingend eine öffentlich-rechtliche Ausgestaltung für Datenvermittlungsdienste oder datenaltruistische Organisationen vor, siehe ausdrücklich für Datenvermittlungsdienste Erwägungsgrund 27 DGA. Nach der Verordnung über den europäischen Gesundheitsdatenraum (EHDS-VO)[3] sind *Zugangsstellen für Gesundheitsdaten gemäß Art. 55 Abs. 1 S. 2 EHDS-VO öffentlich-rechtlicher Natur*.

Der DGA gibt keine bestimmte Rechtsform für Datenvermittlungsdienste vor. Damit besteht für *Datenvermittlungsdienste Rechtsformfreiheit*. Nach Art. 2 Nr. 16 und Art. 18 lit. a und c DGA handeln datenaltruistische Organisationen unentgeltlich und ohne Erwerbszweck, um Ziele von allgemeinem Interesse gemäß dem nationalen Recht wie die Gesundheitsversorgung zu verfolgen. Ziele von allgemeinem Interesse können in Deutschland von gemeinnützigen Organisationen verfolgt werden. Dies sind solche, die gemeinnützige Zwecke im Sinne des § 52 Abs. 1 Abgabenordnung (AO) verfolgen. Eine Eingrenzung von gemeinnützigen Organisationen auf eine bestimmte Rechtsform konnte hingegen nicht festgestellt werden. Somit kommen jegliche gemeinnützig agierenden Organisationen nach nationalem Recht wie beispielsweise eine Stiftung, ein Verein, eine gemeinnützige GmbH oder eine gemeinnützige AG als datenaltruistische Organisationen in Betracht. In der Praxis ist bei den gemeinnützigen Organisationen am häufigsten die Rechtsform der Stiftung anzutreffen, aus rechtlichen Gesichtspunkten besteht aber für *datenaltruistische Organisationen Rechtsformfreiheit, soweit gemeinnützige Zwecke* verfolgt werden.

II. Zusammenhang zwischen Aufgaben und Rollen einer Datentreuhand

Die für Datentreuhänder ins Auge gefassten *Aufgaben* sind so vielfältig wie die Bereiche, in denen sie eingesetzt werden können. Im TrustDNA Vorhaben sollen Datentreuhänder in der Netzwerkmedizin an der Schnittstelle zwischen Versorgung und Forschung eingesetzt werden. In der vorliegenden Untersuchung wurden deshalb die Kriterien zur Bestimmung der Rolle(n) einer Datentreuhand exemplarisch auf drei nichtabschließende Aufgabenbereiche angewendet, deren Zusammenstellung sich daran orientiert, wer bei der Erfüllung der jeweiligen Aufgaben neben einer Datentreuhand im medizinischen Kontext involviert ist. Ausgegangen wird grundsätzlich von drei weiteren Akteuren in diesem Zusammenhang: den Patient:innen als betroffene Personen, den Datengebern, die nicht betroffene Personen sind (z.B. Krankenhäuser, Ärzte) als Verantwortliche und den Datennutzern (z.B. forschende Unternehmen und Forschungseinrichtungen) als Verantwortliche. Die drei exemplarischen Aufgabenbereiche sind: (1) Partizipierendes Verfahren, Einwilligungsmanagement und Geltendmachung von Betroffenenrechten, (2) Pseudonymisierung und Anonymisierung sowie (3) Datenübermittlung bzw. Bereitstellung von Daten in sicherer Verarbeitungsumgebung.

Grundsätzlich wurde festgestellt, dass die für den jeweiligen Aufgabenbereich in Betracht kommenden Rollen zunehmen, je mehr Akteure an der Durchführung einer Aufgabe beteiligt sind und sich parallel dazu auch die Rechtsunsicherheit erhöht (siehe Abbildung 1). Für den medizinischen Kontext ergeben sich daraus bestimmte datenschutzrechtliche Konsequenzen, die in der Untersuchung zur Vertrauenswürdigkeit von Datentreuhändern (II.) aufgegriffen

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. 2016 L 119, 1), im Folgenden DSGVO.

[2] 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) (ABl. 2022 L 152, 1), im Folgenden DGA.

[3] Verordnung (EU) 2025/327 des Europäischen Parlaments und des Rates vom 11. Februar 2025 über den europäischen Gesundheitsdatenraum sowie zur Änderung der Richtlinie 2011/24/EU und der Verordnung (EU) 2024/2847 (ABl. 2025 L 96, 1), im Folgenden EHDS-VO.

wurden.

Involvierte Akteure	Betroffene Person Datentreuhand	Betroffene Person Datengeber Datentreuhand	Betroffene Person Datengeber Datentreuhand Datennutzer
Aufgabenbereich	Partizipierendes Verfahren, Einwilligungsmanagement, Geltendmachung von Betroffenenrechten	Pseudonymisierung, Anonymisierung	Übermittlung / Bereitstellung von Daten
Rolle(n)	Verantwortlicher	Allein / gemeinsam Verantwortlicher, Auftragsverarbeiter	Allein / gemeinsam Verantwortlicher, Auftragsverarbeiter
Konsequenzen	(Abstrakt) vorhersehbar	Je nach Einzelfall / ungewiss	Je nach Einzelfall / ungewiss

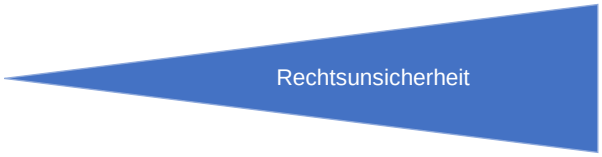

Abbildung 1: Zusammenhang zwischen Aufgaben und Rollen einer Datentreuhand (Darstellung von Anna Lina Gummersbach)

III. Vertrauenswürdigkeit von Datentreuhändern

Die Untersuchung der Vertrauenswürdigkeit von Datentreuhändern in der Netzwerkmedizin wurde im Berichtzeitraum abgeschlossen. Die Ergebnisse dieser Untersuchung wurden in Form eines Aufsatzes werden zur Veröffentlichung eingereicht.

Die dabei im Rahmen der Untersuchung des für Datentreuhänder in der Netzwerkmedizin relevanten europäischen Regelungsrahmens gewonnenen Erkenntnisse bestätigen die Ergebnisse der Begleitforschung insoweit, als dass Rechtsunsicherheit in Bezug auf das Datenschutzrecht für Datentreuhänder als Rechtsanwender als Herausforderung besteht. Ferner sind nur wenige Standards und keine für Datentreuhänder spezifischen Zertifizierungen vorhanden. Wie diesen Herausforderungen aus Sicht einer anvisierten Datentreuhand in der Netzwerkmedizin begegnet werden kann, war ebenfalls Teil unserer Untersuchung.

Weitere hervorzuhebende Erkenntnisse der Untersuchung sind die Identifikation der im DGA normierten Datenvermittlungsdienste und datenaltruistischen Organisationen, sowie die im EHDS-VO vorgesehenen Zugangsstellen für Gesundheitsdaten als mögliche Datentreuhandformen.

Zum Zwecke der Untersuchung definieren wir Datentreuhänder in der Netzwerkmedizin als einen Akteur, der die datenschutzkonforme Teilung[4] personenbezogener Daten zwischen

[4] Im Englischen „data sharing“.

Dateninhaber[5] bzw. betroffener Person auf der einen und Datennutzer[6] auf der anderen Seite ermöglicht oder fördert.

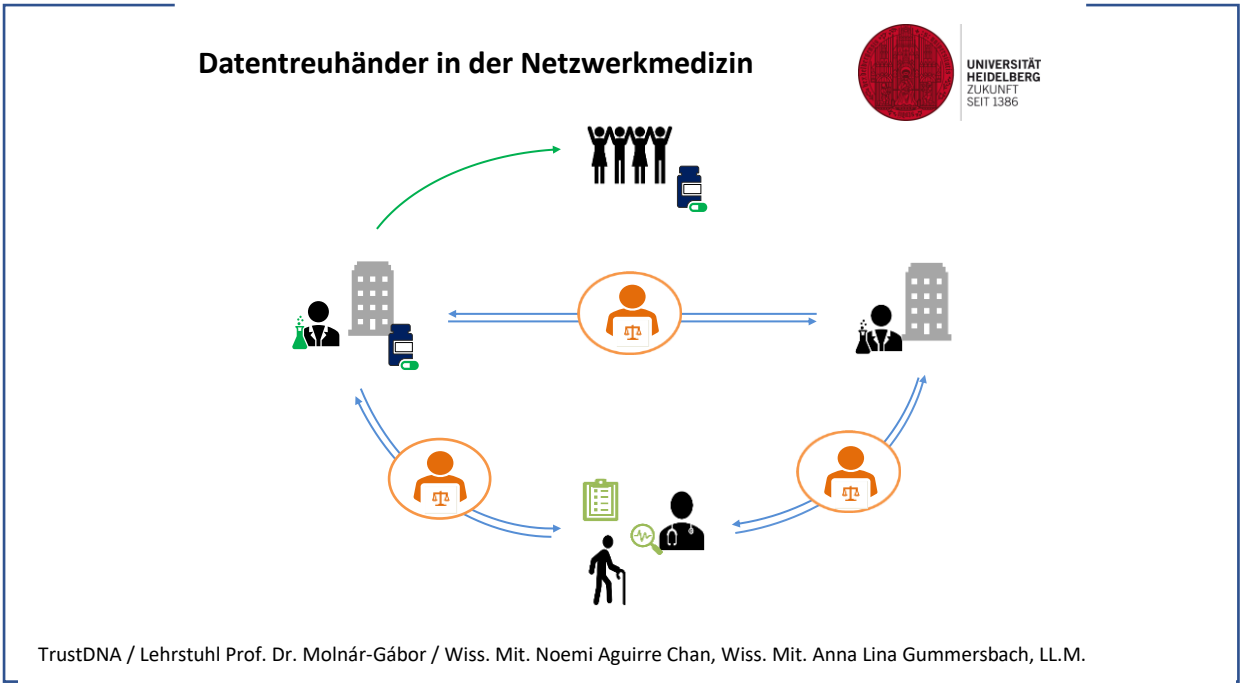

Abbildung 2: Datentreuhänder in der Netzwerkmedizin (eigene Darstellung von Noemi Aguirre Chan und Anna Lina Gummersbach)

IV. Rechtsvergleich mit dem Vereinigten Königreich

Die rechtsvergleichende Analyse anhand konkreter Beispiele für eine erfolgreiche Datentreuhandinitiative aus dem Vereinigten Königreich (*UK Biobank* und *Genomics England*), wurde mit Unterstützung einer der Honorarkräfte abgeschlossen.

Folgende zentrale Erkenntnisse konnten im Berichtzeitraum gewonnen werden. Die durch den Rechtsvergleich gewonnen Erkenntnisse fanden Berücksichtigung in der Bearbeitung von AP2, AP3 und AP5.

1. Datentreuhandmodelle im Vereinigten Königreich

Es wurde der Frage nachgegangen, wie Datentreuhandmodelle im Vereinigten Königreich auftreten und dabei rechtlich umgesetzt werden, um daraus möglicherweise Parallelen und Unterschiede für die angestrebte deutsche bzw. europäische rechtliche Etablierung von Datentreuhandmodellen zu gewinnen.

a) Zum Begriff des „data trust“

Wir haben untersucht wie Datentreuhänder nach angloamerikanischem Recht behandelt werden, um hieraus rechtsvergleichend Erkenntnisse für eine zu priorisierende Rechtsform eines Datentreuhänders zu gewinnen. Hierbei haben wir herausgefunden, dass die rechtliche

[5] ISv Art. 2 Nr. 8 DGA. Die EHDS-VO beschränkt „Gesundheitsdateninhaber“ (Art. 2 Abs. 2 lit. t i EHDS-VO) bezüglich der Verarbeitung von personenbezogenen Daten auf (gemeinsam) Verantwortliche. Dies könnte den Eindruck erwecken, dass Dateninhaber im Gesundheitsbereich immer verantwortlich sein müssen, was aber nicht unbedingt der Fall sein muss.
[6] ISv Art. 2 Nr. 9 DGA.

Behandlung von Datentreuhändern im angloamerikanischen Rechtsraum nicht abschließend geklärt ist, Datentreuhandmodelle befinden sich auch hier noch in der Phase von Pilotprojekten.

Rechtlich werden Datentreuhandmodelle mehrheitlich als sogenannter *„data trust“* eingeordnet. Dabei ist der angloamerikanische Begriff „trust“ nicht identisch mit dem deutschen Begriff der „Treuhand“. Die „Treuhand“ umschreibt ein übergeordnetes Konzept der Verwaltung von Vermögensgütern und kann verschiedene rechtliche Ausgestaltungen annehmen. Der angloamerikanische „trust“ ist hingegen ein feststehender Rechtsbegriff, der die Rechten und Pflichten zwischen drei Akteuren („settlor“, „trustee“ und „beneficiary“) festlegt. Der Begriff „data trust“ impliziert im englischen Rechtssprachraum, dass ein Datentreuhänder im Rechtssinne dem „trust law“ bzw. „equity law“ unterworfen ist, was bislang weder in der Praxis umgesetzt wird bzw. dessen Umsetzung erhebliche Schwierigkeiten entgegenstehen (dazu sogleich). Einzig die sog. „*Data Trusts Initiative*“[7] will sich im Rahmen von Pilotprojekten der Entwicklung von „data trusts“ im Rechtssinne widmen, die treuhänderische Verantwortung haben, Betroffenenrechte entsprechend der für den „trust“ festgelegten Bestrebungen auszuüben.[8]

Im Nachgang hierzu wären „Datentreuhänder“ nach deutschem Begriffsverständnis vielmehr vergleichbar mit einem weiten Begriffsverständnis von „data trusts“ als „data fiduciary“ oder als „data institutions“, also jene Unternehmen, Stiftungen oder Behörden bzw. Universitäten, denen Daten für Zwecke des Gemeinwohls anvertraut wurden, was im Vereinigten Königreich in der Praxis vorzufinden ist (dazu unter e) „Non-trust law“ Modelle).

b) Bedenken bezüglich „data trust“ als „trust“ im Rechtssinne

Es konnte herausgearbeitet werden, dass die rechtliche Konstruktion eines „data trust“ im Rechtssinne erheblichen Bedenken ausgesetzt und damit im Vereinigten Königreich nicht vielversprechend ist. Ein „trust“ im Rechtssinne erfordert eine Aufteilung von Rechts- und Billigkeitstitel am Eigentum („legal and equitable title to property“), wobei der „trustee“ den „legal title“ hält, aber gegenüber dem „beneficiary“, der den „equitable title“ hält, eine treuhänderische Verpflichtung hat zu seinen Gunsten mit dem Eigentum umzugehen.

Dafür wurde untersucht, ob personenbezogene Daten oder entsprechende Betroffenenrechte Eigentum („property“) darstellen können und ob die für einen „trust“ im Rechtssinne benötigte Aufteilung in Rechts- und Billigkeitstitel und Übertragung des Rechtstitels auf den „trustee“ in diesem Kontext überhaupt möglich wäre.

Dass Daten selbst nicht „property“ sein können, wurde gerichtlich bereits in einem Präzedenzfall angenommen (Oxford v Moss [1978] 68 Cr App 183). Präzedenzfälle zu der Frage, ob die Betroffenenstellung oder einzelne Betroffenenrechte übertragbar sind, fehlen. Es gibt vereinzelte Gerichtsentscheidungen, in denen insbesondere vertragliche Rechte als nichtkörperliche Gegenstände als „property“ angesehen werden, jedoch sind jene Entscheidungen wohl nicht verallgemeinerungsfähig, sondern bilden die Ausnahme. Es erscheint daher wenig vielversprechend, die Betroffenenstellung oder einzelne Betroffenenrechte als auf einen „trustee“ übertragbar im Sinne des „property“ anzusehen.

---

[7] *Delacroix* und *Lawrence* haben seit ihrem maßgebenden Aufsatz in 2019 (*Delacroix/Lawrence* (2019) ‘Bottom-up data Trusts: disturbing the ‘one size fits all’ approach to data governance’ International Data Privacy Law, 9(4), 236–252) ihre Arbeit an der Entwicklung von „data trusts“ in der *Data Trusts Initiative* fortgesetzt; weitere Informationen auf der Website der *Data Trusts Initiative*, abrufbar unter https://datatrusts.uk/ (16.06.2025).

[8] Zum Verständnis von “Data Trusts” siehe entsprechende Erläuterungen in *Delacroix/Lawrence/Montgomery*, (2020) ‘Selecting a data sharing structure: a value-based choice’, abrufbar unter https://datatrusts.uk/2020/03/27/selecting-digital-structures (16.06.2025).

In der englischsprachigen Literatur wird darüber hinaus vereinzelt diskutiert, ob man statt auf das Konzept „property“ nicht auf ein davon zu unterscheidendes Konzept „ownership“ zurückgreifen könnte. Problematisch dabei ist jedoch, dass „ownership“ in der Regel im Zusammenhang mit „property“ verstanden wird. Das Konzept ein Objekt, das nicht „property“ ist zu „ownen“ ist relativ neu.[9]

Um Parallelen und Unterschiede um die Frage der Übertragbarkeit von personenbezogenen Daten bzw. damit verbundenen Rechtspositionen herauszufinden, wurde eine Untersuchung zum Begriffsverständnis von Eigentum, Inhaberschaft und Dateninhaberschaft aus deutscher Perspektive angestrengt.

Insgesamt wurde die rechtliche Konstruktion eines Datentreuhänders als „data trust“ im Rechtssinne seitens unserer Honorarkraft als nicht vielversprechend angesehen.

c) Zu den „fiduciary duties“ einer „data institution“ bzw. eines „data fiduciary“

Eine weitere Fokussierung auf die rechtliche Konstruktion eines „data trust“ wurde aus oben genannten Gründen als nicht vielversprechend angesehen. Ansatzpunkte für einen Rechtsvergleich könnten aber aus den sog. „fiduciary duties“ folgen.

Die Besonderheit des „trust“ liegt in der verschärften Haftung des sogenannten „(data) trustee/ fiduciary/ stewards“ bei Verletzung der *„fiduciary duties“*. Die „fiduciary duties“ umfassen die Pflicht in bestem Interesse des Treugebers zu handeln, Interessenskonflikte zu vermeiden und ein Verbot sich selbst am Treugut zu bereichern. Der Umfang dieser „fiduciary duties“ sowie die Folgen der Verletzung ist aber stark einzelfallabhängig.

Eine Untersuchung der Arbeiten von Balkin[10] ergab, dass „fiduciary duties“ im Zusammenhang mit Daten durch Gerichte einer Partei immer dann auferlegt werden können, wenn die andere Partei sich in einer Position befindet, welche sich durch Vulnerabilität und durch Abhängigkeit aufgrund einer Informationsasymmetrie auszeichnet. *Dobkin* schlägt aufbauend darauf eine Liste spezifischer Pflichten im Kontext von „information fiduciaries“ vor. Demzufolge können „information fiduciaries“ das ihnen entgegengebrachte Vertrauen insbesondere durch vier Handlungsweisen missbrauchen:

1. indem sie die anvertrauten Daten zum Manipulieren nutzen
2. indem sie die anvertrauten Daten zur Diskriminierung benutzen
3. indem sie die anvertrauten Daten ohne Einwilligung mit Dritten teilen
4. indem sie ihre eigenen Privacy Policies verletzen.[11]

Diese Liste ist jedoch eher auf „Tech Giganten“ wie Google oder Facebook angelegt. Insofern ist nach weiteren, spezifischeren „fiduciary duties“ im Zusammenhang mit Gesundheitsdaten zu suchen. Rechtsprechung im Vereinigten Königreich zu spezifischen “fiduciary duties” für Datentreuhänder gibt es bisher nicht.

---

[9] Zu „property“ als einem „set of rules“, das “ownership” regelt *Worthington*, Legal notions of ‘property’ and ‘ownership’ in: Data ownership, rights and controls: Reaching a common understanding, Discussions at a British Academy, Royal Society and techUK seminar on 3 October 2018, S. 13, abrufbar unter https://royalsociety.org/-/media/policy/projects/data-governance/data-ownership-rights-and-controls-October-2018.pdf (16.06.2025).

[10] *Balkin* (2016) ‘Information Fiduciaries and the First Amendment’ UC Davis Law Review, 49(4), 1183-1234.

[11] *Dobkin* (2018) ‘Information Fiduciaries in Practice: Data Privacy and User Expectations’ Berkeley Technology Law Journal, 33(1), 1, 7.

Vor dem Hintergrund des Verständnisses von „fiduciary duties“ als Pflicht in bestem Interesse des Treugebers zu handeln, Interessenskonflikte zu vermeiden und ein Verbot sich selbst am Treugut zu bereichern hat *ein Rechtsvergleich mit Deutschland hat ergeben, dass den „fiduciary duties“ äquivalente Pflichten bereits jedem Vertrag inhärent sind*. Äquivalente Pflichten sind entweder vertraglich geregelt oder aber im Rahmen der Treue- und Rücksichtnahmepflichten gemäß § 241 Abs. 2 BGB mit entsprechendem Haftungsrisiko gemäß § 280 Abs. 1 BGB zu beachten. Eine unterschiedliche rechtliche Behandlung zwischen dem Bruch „normaler Vertragspflichten“ und dem Bruch funktionsäquivalenter „fiduciary duties“ konnte nicht festgestellt werden.

d) Zur Frage der Übertragbarkeit der Betroffenenstellung bzw. von Betroffenenrechten unter der DSGVO („to alienate“ bzw. „to mandate“)

Die Betroffenenrechte nach Art. 12 ff. DSGVO sind de lege lata nicht übertragbar im Sinne von „alienable“, das heißt sie können nicht auf einen Dritten (z.B. einen „trustee“) in der Weise übertragen bzw. abgetreten werden, dass der ursprüngliche Inhaber dabei sein Recht aufgibt, sie selbst auszuüben. Die Übertragbarkeit der Betroffenenstellung selbst auf den Datentreuhänder wurde als nicht möglich festgestellt. Darüber hinaus wird diskutiert, ob die Betroffenenrechte nach Art. 12 ff. DSGVO „mandatable“ sind.

Bei der Frage, ob Betroffenenrechte nach Art. 12 ff. DSGVO übertragbar im Sinne von „mandatable“ sind, plädieren *Delacroix und Lawrence*[12] dafür, dass dies (erst) de lege ferenda möglich wäre, indem der nationale Gesetzgeber diese Rechte als „mandatable“ kennzeichnet. Diese Möglichkeit ergebe sich aus dem Rechtsgedanken des Art. 80 DSGVO, welcher Rechte aus Art. 77 bis 79 DSGVO für „mandatable“ erklärt. Nach Einschätzung unserer Honorarkraft wäre das Eingreifen des nationalen Gesetzgebers jedoch in mehrerlei Hinsicht fraglich. So ist hierzu im Vereinigten Königreich kein politischer Wille erkennbar, es ist bislang nicht einschätzbar inwieweit ein solches Vorgehen europarechtskonform wäre und auch wie eine solche Gesetzgebung aussehen würde. Es verbleiben ferner Zweifel, ob ein solches „mandate“ die Art von Titelübertragung darstellen könnte, die normalerweise für einen „trust“ im Rechtssinne benötigt wird. Schwierig zu sagen ist auch, in welcher Position eine betroffene Person wäre, die nur den Billigkeitstitel („equitable title“) ihrer Betroffenenrechte halten würde oder ob dies überhaupt möglich wäre. Wie gesagt, sind die Betroffenenrechte de lege lata nicht „alienable“.

Auch die Idee, dass der Datentreuhänder im Endeffekt in großem Stil Betroffenenrechte ausüben könnte, begegnete rechtlichen Bedenken insoweit, als bislang rechtsunsicher ist, inwieweit ein solches Verständnis dem Verständnis des Bundesverfassungsgerichts vom Recht auf informationelle Selbstbestimmung entgegenstünde.

e) „Non-trust law” Modelle

Als Datentreuhändermodelle, die nicht als „*Data trust*“ im „*trust law“* Sinne zu verstehen sind, wurden *UK Biobank (Ltd.)*, *Genomics England (Ltd.)*, *SAIL Databank* und *NHS Digital* untersucht.

UK Biobank ist eine groß angelegte biomedizinische Datenbank und Forschungsressource mit genetischen Daten, Gesundheitsdaten und Lifestyle-Daten von 500.000 Teilnehmern aus dem Vereinigten Königreich, die einen globalen Datenzugang für gesundheitsbezogene Forschung im öffentlichen Interesse ermöglicht.[13] Die Datenbank ist sowohl ein Unternehmen als auch

[12] *Delacroix/Lawrence* (2019) ‘Bottom-up data Trusts: disturbing the ‘one size fits all’ approach to data governance’ International Data Privacy Law, 9(4), 236–252.
[13] *UK Biobank*, Background, abrufbar unter https://www.ukbiobank.ac.uk/learn-more-about-uk-biobank/about-us (16.06.2025).

eine eingetragene Stiftung, öffentlich finanziert und der Vorstand besteht vor allem aus Vertretern aus dem Bereich der öffentlichen Hochschulen und dem Forschungssektor.

Ein ähnliches Set-up findet man in der Infrastruktur hinter dem öffentlichen Dienst für genomische Medizin: *Genomics England.* Es wurde zur Umsetzung des *100.000 Genome Project* von der Regierung des Vereinigten Königreiches etabliert.[14] Das Projekt ist zwar abgeschlossen, von der dabei aufgebauten *National Genomic Research Library* (NGRL) profitieren Forscher weltweit aber bis heute. *Genomics England* ist ein Unternehmen, das vollständig im Eigentum des Gesundheitsministeriums steht und von diesem finanziert wird. Wie bei *UK Biobank* besteht sein Vorstand überwiegend aus hochrangigen Wissenschaftlern.

Auf diese beiden Datentreuhandmodelle wird sich die weitere rechtsvergleichende Untersuchung konzentrieren.

NHS Digital ist der Arbeitstitel des gesetzlich vorgeschriebenen Informationszentrums für das Gesundheits- und Sozialwesen („Health and Social Information Care Centre"). *NHS Digital* setzt die Erhebung und Weiterleitung von Gesundheitsdaten in England von seinem Vorgänger „care.data" fort. Neben Freigaben an gewinnorientierte Einrichtungen und die Hochschulforschung, erfolgen die meisten Datenfreigaben an andere NHS Organisationen oder lokale Behörden basierend auf dem *Health and Social Care Act 2012* bei der Freigabe anonymer Daten für Zwecke der Gesundheits- oder Sozialfürsorge oder zur Förderung der Gesundheit, im Falle einer Freigabe der Nutzung von personenbezogenen Gesundheitsdaten ohne Einwilligung basierend auf dem *NHS Act 2006* zu medizinischen Zwecken inklusive medizinischer Forschung. *NHS Digital's* Datenerhebung basiert auf einem Opt-out System.

SAIL Databank ist getrennt vom NHS, nutzt ihn aber als „*Trusted Third Party*", das heißt eine sichere Organisation, die vertrauliche, personenbezogene Informationen innerhalb des NHS für Verknüpfungszwecke verarbeitet. Bei *SAIL Databank* handelt es sich um eine umfangreiche Bevölkerungsdatenbank in Wales. Sie hat u.a. ein „Consumer Panel", das sie zu Datenschutzfragen in datenintensiver Forschung aus der Perspektive von Dienstnutzern und Pflegern berät. Forscher werden ermutigt sich mit dem Panel zu treffen und ihre Anträge mit ihm zu diskutieren und beraten zu werden. Dieser „Tandem-Ansatz" steht im Gegensatz zu der Top-down Entwicklung von *NHS Digital*. Ferner bezieht *SAIL Databank* im Gegensatz zu *NHS Digital* Forscher und Methodiker, die verstehen wie Daten für die Forschung genutzt werden, mit ein.

2. Forschungsfrage und Methodik für den Rechtsvergleich

Aufbauend auf dieser grundlegenden Untersuchung zu Datentreuhändern („data institutions") im Vereinigten Königreich, ermittelten wir die folgende konkrete Forschungsfrage für den Rechtsvergleich anhand von *UK Biobank* und *Genomics England*:

> *Was ist das Datenschutz-Design dieser Datentreuhänder/"data institutions" im Vereinigten Königreich, wie ermöglichen sie Patient:innenbeteiligung und inwieweit würde sich ihr Design Übertragen in Deutschland in die neuen europäischen Strukturen des DGA und der EHDS-VO eingliedern?*

Das Datenschutz-Design spezifizierten wir mit einem Fokus auf die *Rechtsgrundlagen*, *Rollen unter der DSGVO* und *geeigneten technischen und organisatorischen Maßnahmen*, sowie welche Funktionen und Aufgaben/Pflichten die Datentreuhänder haben und ob sie ein

[14] *Genomics England*, Origins, abrufbar unter https://www.genomicsengland.co.uk/about-us/origins (16.05.2025).

Datenschutzsiegel, Zertifikat oder Verhaltensregeln nutzen. Im Rahmen der Analyse des Datenschutz-Designs sollten die einzelnen Verarbeitungsvorgänge (z.B. Datenerhebung, Speicherung, Löschung, Transfer, etc.), wenn möglich und sinnvoll, getrennt betrachtet werden.

Mit der Unterstützung unserer Honorarkraft wurde das Datenschutz-Design von *UK Biobank* und *Genomics England* mit genanntem Fokus im Berichtzeitraum untersucht.

Zur Beantwortung der Frage welche Aussichten das Datenschutz-Design von *Genomics England* und *UK Biobank* übertragen in Deutschland hätte unter die Strukturen des DGA und der EHDS-VO eingegliedert zu werden, sollen einzelne Elemente ihres datenschutzrechtlichen Designs, namentlich ihre Funktion, die Patienteneinbindung, die Nutzung einer sicheren Verarbeitungsumgebung sowie ihre internationale Öffnung genauer betrachtet werden. Diese Elemente versprechen mit Blick auf Kernvorgaben des DGA und der EHDS-VO zu Datentreuhändern als Ausgangspunkt des Vergleichs am vielversprechendsten.

3. Aussichten zur Eingliederung des Datenschutz-Designs in europäische Strukturen

Um zu beantworten, welche Aussichten das Datenschutz-Design von *Genomics England* und *UK Biobank* übertragen in Deutschland hätte unter die Strukturen des DGA und der EHDS-VO eingegliedert zu werden, sollen ihre Funktion, die Patienteneinbindung, die Nutzung einer sicheren Verarbeitungsumgebung sowie ihre internationale Öffnung im Folgenden mit Blick auf entsprechende Vorgaben aus DGA und EHDS-VO sowie dem deutschen Gesundheitsdatennutzungsgesetz (GDNG)[15] untersucht werden.

Der DGA sieht sog. *Anbieter von Datenvermittlungsdiensten* (Art. 10 ff. DGA) und *anerkannte datenaltruistische Organisationen* (Art. 16 ff. DGA), die EHDS-VO sog. *Zugangsstellen für Gesundheitsdaten* (Art. 55 EHDS-VO) für die Sekundärnutzung[16] von Gesundheitsdaten vor, die als Datentreuhänder in Betracht kommen. Die gesetzlichen Vorgaben zu diesen speziellen Formen von Datentreuhändern sollen nachfolgend als Vergleichsmaßstab dienen.

Um das deutsche Gesundheitswesen auf die Anbindung an den EHDS vorzubereiten, wurden erste Schritte mit dem Gesundheitsdatennutzungsgesetz (GDNG) unternommen.[17] Gemäß § 3 Abs. 1 GDNG wird eine sog. *zentrale Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten* beim Bundesinstitut für Arzneimittel und Medizinprodukte eingerichtet.[18] Für ihre Weiterentwicklung ist vorgesehen, dass sie die sich aus der EHDS-VO ergebenden Aufgaben wahrnimmt.[19] Auch diese Stelle kommt als Datentreuhänder in Betracht, weshalb die Vorgaben des GDNG in die folgende Untersuchung ergänzend mit einbezogen werden.

a) Funktion

Die folgende Darstellung der Funktion soll einen ersten Eindruck zu den genannten Akteuren vermitteln.

---

[15] Gesundheitsdatennutzungsgesetz vom 22. März 2024 (BGBl. 2024 I Nr. 102).
[16] Art. 2 Abs. 2 lit. e i.V.m. Art. 53 EHDS-VO.
[17] GDNG-Kabinettentwurf, BT-Drs. 20/9046, S. 2.
[18] Hintergrund dafür ist folgender: „Das Bundesinstitut für Arzneimittel und Medizinprodukte hat hier bereits vorbereitende Arbeiten durch den Aufbau des Forschungsdatenzentrums Gesundheit und die Gemeinsame Aktion für den europäischen Gesundheitsdatenraum, genannt TEHDAS (Towards the European Health Data Space, https://tehdas.eu/) geleistet. Das Bundesinstitut für Arzneimittel und Medizinprodukte vertritt zudem die deutsche Perspektive im Pilotprojekt EHDS2 zur Erprobung grenzüberschreitender Zugänge zu Sekundärzwecken (https://www.ehds2pilot.eu/) und bekommt ab 2023 EU-Mittel zum Aufbau nationaler Zugangsstellen für Gesundheitsdaten.“ GDNG-Kabinettentwurf, BT-Drs. 20/9046, S. 50.
[19] Ibid.

Anbieter von Datenvermittlungsdiensten werden definiert gemäß Art. 2 Nr. 11 DGA als Anbieter von „Dienst[en], mit [denen] (…) durch technische, rechtliche oder sonstige Mittel Geschäftsbeziehungen zwischen einer unbestimmten Anzahl von betroffenen Personen oder Dateninhabern[20] einerseits und Datennutzern[21] andererseits hergestellt werden sollen, um die gemeinsame Datennutzung[22], auch für die Zwecke der Ausübung der Rechte betroffener Personen in Bezug auf personenbezogene Daten, zu ermöglichen“ unter Ausschluss bestimmter in Art. 2 Nr. 11 Buchst. a bis d DGA genannter Dienste. Hervorzuheben ist ihre Funktion Geschäftsbeziehungen von betroffenen Personen bzw. Dateninhabern mit Datennutzern für die gemeinsame Datennutzung herzustellen.[23] Aus datenschutzrechtlicher Sicht relevant ist die Ermöglichung der Ausübung von Betroffenenrechten nach DSGVO.

Anerkannte datenaltruistische Organisationen[24] sollen Ziele von allgemeinem Interesse fördern (vgl. Art 2 Nr. 16, Art. 18 lit. a und b, Art. 19 Abs. 4 lit. h DGA). Zu diesen Zielen gehören gemäß Erwgr. 45 S. 2 f. DGA unter anderem die Gesundheitsversorgung und die Unterstützung der wissenschaftlichen Forschung.

Zugangsstellen für Gesundheitsdaten sollen „den Zugang zu elektronischen Gesundheitsdaten in den Mitgliedstaaten unterstützen“ und tragen so „wesentlich zur Förderung der Sekundärnutzung gesundheitsbezogener Daten“ bei (Erwgr. 64 S. 1 EHDS-VO). Außerdem sollen sie einen Beitrag zur einheitlichen Anwendung der EHDS-VO in der gesamten Union leisten (Art. 55 Abs. 1 UAbs. 2 S. 1, Erwgr. 65 S. 1 EHDS-VO). Damit nehmen sie eine zentrale Rolle zur Gewährleistung der Sekundärnutzung im EHDS wahr.

Die *zentrale Datenzugangs- und Koordinierungsstelle* soll laut dem GDNG-Kabinettentwurf zentraler Ansprechpartner für Datennutzende sein.[25] Sie unterstützt und berät gem. § 3 Abs. 2 S. 1 GDNG Datennutzende beim Zugang zu Gesundheitsdaten. Dabei übernimmt sie „die Funktion eines Mittlers zwischen Antragstellenden und datenhaltenden beziehungsweise datenmittelnden Stellen“.[26] Darüber hinaus ist sie auch für die Genehmigung der Verknüpfung und Verarbeitung von pseudonymisierten Daten des FDZ Gesundheit nach § 303d SGB V mit pseudonymisierten Daten der klinischen Krebsregister der Länder nach § 65c SGB V für Forschungsvorhaben auf Antrag und der Festlegung der sicheren Verarbeitungsumgebung in der die Daten den Antragstellenden verfügbar gemacht werden zuständig. Neben der Mittler- und Entscheidungsfunktion hat die Datenzugangs- und Koordinierungsstelle, wie ihr Name schon vermuten lässt, auch eine Koordinierungsfunktion. Dies wird mit Blick auf ihre koordinierenden Aufgaben, etwa im Rahmen der Datenverknüpfung, deutlich.[27]

Genomics England und *UK Biobank* ermöglichen Datenzugang für die Forschung und tragen zur Verbesserung der Gesundheitsversorgung bei. Damit fördern sie Ziele von allgemeinem Interesse. Unsere Honorarkraft gelangte zu der Einschätzung, dass *UK Biobank* und *Genomics England* beide ein Vorbild für datenaltruistische Organisationen sein könnten, weswegen sich die nachfolgende Untersuchung auf die Vorgaben des DGA zu diesen Organisationen beschränkt.

b) Patienteneinbindung

[20] Art. 2 Nr. 8 DGA.
[21] Art. 2 Nr. 9 DGA.
[22] Art. 2 Nr. 10 DGA.
[23] HK-DGA/Specht-Riemenschneider Art. 2 Rn. 66.
[24] Datenaltruismus wird in Art. 2 Nr. 16 DGA definiert.
[25] GDNG-Kabinettentwurf, BT-Drs. 20/9046, S. 50.
[26] GDNG-Kabinettentwurf, BT-Drs. 20/9046, S. 51.
[27] Im GDNG-Kabinettentwurf heißt es sie „übernimmt koordinierende Aufgaben bei Anträgen auf Datenverknüpfung und Datennachnutzung“, BT-Drs. 20/9046, S. 3.

In unserem Vorhaben sollen Prozesse aufgestellt werden, um Patient:innen aktiv in das Forschungsdatenmanagement einzubinden. Dementsprechend wurden die gesetzlichen Vorgaben sowie vergleichend Prozesse der ausgewählten Akteure im Vereinigten Königreich zur Patienteneinbindung untersucht.

Datenaltruismus nach DGA ist allein auf Basis einer freiwilligen Einwilligung betroffener Personen vorgesehen, Art. 2 Nr. 16 DGA. Anerkannte datenaltruistische Organisationen müssen gemäß Art. 21 Abs. 3 DGA Werkzeuge zur Einholung und zum einfachen Widerruf der Einwilligung bereitstellen.

Die EHDS-VO sieht demgegenüber grundsätzlich einen Opt-out statt einem Opt-in Ansatz vor und etabliert in Art. 71 Abs. 1 EHDS-VO das Recht natürlicher Personen zum Widerspruch (Opt-out) gegen die Verarbeitung ihrer personenbezogenen Gesundheitsdaten für die Sekundärnutzung. Die Mitgliedstaaten sind dazu verpflichtet, einen leicht verständlichen und barrierefreien Mechanismus zum Widerspruch einzurichten (Abs. 2). Gemäß Art. 58 Abs. 3 S. 3 EHDS-VO haben natürliche Personen zudem ein Recht auf Nichtwissen bezogen auf wesentliche Befunde, über die eine Zugangsstelle von einem Gesundheitsdatennutzer informiert wird.

Vorbereitend umgesetzt wurde das Widerspruchsrecht im Zuge der Einführung des GDNG im geänderten § 363 GDNG, der die Widerspruchsmöglichkeit (Opt-out) gegen die Übermittlung von Daten aus der elektronischen Patientenakte an das FDZ Gesundheit für die Verarbeitung zu Forschungszwecken vorsieht (§ 363 Abs. 1, 2 und 5 SGB V). Über die Benutzeroberfläche eines geeigneten Endgeräts bzw. gegenüber der Ombudsstelle (§ 342a SGB V) können Versicherte ihren Widerspruch erklären (§ 363 Abs. 5 S. 2 SGB V). Ferner ist der Widerspruch gesetzlich im Rahmen des neuen § 25b SGB V gegen die Datenverarbeitung zur Durchführung einer datengestützten Auswertung durch die Kranken- und Pflegekassen zum Gesundheitsschutz eines Versicherten und zu spezifischen aufgelisteten Zwecken, wie der Erkennung seltener Krankheiten (§ 25b Abs. 1 Nr. 1 SGB V), vorgesehen.

Relevant für die Patienteneinbindung ist auch, dass Vertreter der Patientenorganisationen am Arbeitskreis zur Gesundheitsdatennutzung beteiligt sind, der beratend an der Evaluation, Weiterentwicklung und Ausgestaltung der Aufgabenwahrnehmung der Datenzugangs- und Koordinierungsstelle mitwirkt (§ 3 Abs. 4 GDNG), auch wenn Patienten hier nicht direkt sondern vielmehr mittelbar durch Vertretung ihre Interessen geltend machen können.

Die Untersuchung unserer Honorarkraft zur Patienteneinbindung von *Genomics England* hat ergeben, dass eine Einwilligung von Teilnehmenden eingeholt wird, um ihre Daten in der *National Genomic Reserach Library* (NGRL) zu speichern.[28] Sie haben die Möglichkeit ihre Einwilligung über ein online Portal[29] ganz oder teilweise zu widerrufen. Darin können sie auch ihre Proben verfolgen. Für Teilnehmende des *100.000 Genome Project* gibt es einen „*Check My Choices*“ Bereich, in dem sie einsehen können, ob sie eingewilligt haben über zusätzliche Befunde informiert zu werden und können ihre diesbezügliche Wahl ändern, wenn sie dies wünschen. Dies könnte Übertragen auf Datentreuhänder in Deutschland dem in der EHDS-VO vorgesehen Recht auf Nichtwissen in Art. 58 Abs. 3 S. 3 EHDS-VO zugute kommen. Mitgliedstaatliche Regelung die zu einem anbweichenden Umgang mit genomischen Daten führen könnten, müssen beachtet werden. Außerdem hat *Genomics England* einen Teilnehmerausschuss („*Participant Panel*“), der ihren Vorstand („*Board*“) berät und auch in anderen Gremien involviert ist, um Teilnehmende, Patienten und ihre Familien auf allen

[28] Genomics England, Taking Part, abrufbar unter https://www.genomicsengland.co.uk/patients-participants/taking-part (16.06.2025).
[29] https://jiraservicedesk.extge.co.uk/plugins/servlet/desk/category/participantpage (16.06.2025).

Ebenen zu vertreten.[30] Wie erläutert, wurde die mittelbare Einbindung von Patienten durch Vertreter in bestimmten Gremien auch vom GDNG aufgegriffen (vgl. § 3 Abs. 4 GDNG).

UK Biobank hat auch ein Gremium, um Interessen der Teilnehmenden einzubringen, die „*Participant Advisory Group*".[31] Sie berät *UK Biobank* zu Themen wie etwa der Kommunikation mit und Informierung von Teilnehmenden sowie zur Sammlung von Gesundheitsdaten von Teilnehmenden und wie sie Forschern zur Verfügung gestellt werden. Ferner hat *UK Biobank* auch ein online Portal für Teilnehmende, indem sie ihre Kontaktdaten aktualisieren und Fragebögen zu ihrer Gesundheit ausfüllen können.[32] Allerdings ist es nicht möglich über das Portal ihre Einwilligung zur Teilnahme am *UK Biobank* Forschungsprojekt zu Widerrufen.[33] Außerdem verfolgt *UK Biobank* im Unterschied zu *Genomics England* den Ansatz, dass sie grundsätzlich Teilnehmenden kein Feedback zu ihrer Gesundheit geben, wozu alle Teilnehmenden zustimmen müssen, um teilnehmen zu können.[34] Dies hat praktische, aber auch ethische Gründe.[35]

c) Sichere Verarbeitungsumgebung

Aufgrund der Relevanz von sicheren Verarbeitungsumgebungen für die Sekundärnutzung von Gesundheitsdaten im Unionsrecht und der Tatsache, dass Vorgaben dazu auf europäischer und nationaler Ebene im Detail noch nicht abschließend geregelt sind, soll im Folgenden ein näherer Blick auf die Umsetzung von Verarbeitungsumgebungen durch *UK Biobank* und *Genomics England* geworfen werden.

Der Gesundheitsdatenzugang für die Sekundärnutzung soll im europäischen Gesundheitsdatenraum durch die nationalen Zugangsstellen nur über eine sichere Verarbeitungsumgebung gewährt werden, die organisatorischen und technischen Maßnahmen, sowie Interoperabilitäts- und Sicherheitsanforderungen unterliegt (Art. 73 Abs. 1 S. 1 EHDS-VO). Die von der sicheren Verarbeitungsumgebung zu erfüllenden Sicherheitsmaßnahmen werden in Art. 73 Abs. 1 S. 2 EHDS-VO in einer nicht abschließenden Liste näher bestimmt. Dazu zählt etwa die Minimierung des Risikos unbefugten Kopierens, Änderns, Lesens oder Entfernens von in der sicheren Verarbeitungsumgebung gehosteten Gesundheitsdaten „durch dem Stand der Technik entsprechende technische und organisatorische Maßnahmen" (lit. b). Ferner müssen die Zugangsstellen sicherstellen, dass Gesundheitsdatennutzer aus der sicheren Verarbeitungsumgebung nur nicht personenbezogene Gesundheitsdaten (inklusive solchen in einem anonymisierten statistischen Format) herunterladen können (Abs. 2 UAbs. 2). Ferner sollen sie dafür Sorge tragen, dass regelmäßig Audits, auch durch Dritte, durchgeführt werden und sollen im Fall von festgestellten Risiken, Mängeln oder Schwachstellen Abhilfemaßnahmen ergreifen (Abs. 3).

---

[30] Genomics England, The Participant Panel, abrufbar unter https://www.genomicsengland.co.uk/patients-participants/participant-panel (16.06.2025); siehe auch die Terms of Reference, abrufbar auf der genannten Seite.
[31] UK Biobank, UK Biobank Participant Advisory Group, abrufbar unter https://www.ukbiobank.ac.uk/explore-your-participation/contribute-further/uk-biobank-participant-advisory-group (16.06.2025).
[32] UK Biobank, Explore your participation, abrufbar unter https://www.ukbiobank.ac.uk/explore-your-participation (16.06.2025).
[33] Zur Ausübung und weiteren Informationen zum Widerruf bei UK Biobank siehe die Privacy Notice, abrufbar unter https://www.ukbiobank.ac.uk/explore-your-participation/basis-of-your-participation (16.06.2025).
[34] UK Biobank, Following your health, abrufbar unter https://www.ukbiobank.ac.uk/explore-your-participation/following-your-health (16.06.2025).
[35] Ibid; Siehe dazu auch UK Biobank, Participant Information Sheet, S. 5, abrufbar unter https://www.ukbiobank.ac.uk/media/3utoizlp/imaging-information-sheet-v17-1-28-06-2024.pdf (16.06.2025); UK Biobank Ethics and Governance Framework, Version 3.0, Oktober 2007, S. 6 ff. abrufbar unter https://www.ukbiobank.ac.uk/media/0xsbmfmw/egf.pdf (16.06.2025).

Darüber hinaus wird die Kommission unter anderem ermächtigt, die technischen und organisatorischen Anforderungen und die Datenschutzanforderungen der sicheren Verarbeitungsumgebung mittels Durchführungsrechtsakten festzulegen (Abs. 5). Aufgrund des eher vage gehaltenen Normtextes, liegt es somit in der Hand der Kommission datenschutzrechtlich relevante Standardisierungen für den Gesundheitsdatenzugang durch die sichere Verarbeitungsumgebung vorzunehmen und die Tätigkeit von Zugangsstellen als Datentreuhänder rechtssicherer zu gestalten.

Dies hat auch Auswirkungen auf anerkannte datenaltruistische Organisationen, die personenbezogene Gesundheitsdaten „unter Verwendung einer sicheren Verarbeitungsumgebung" verarbeiten (Abs. 4). Hierbei soll die genutzte sichere Verarbeitungsumgebung auch die in Art. 73 Abs. 1 S. 2 lit. a bis f EHDS-VO festgelegten Sicherheitsmaßnahmen erfüllen. Erwgr. 78 S. 2 führt aus, dass mit Blick auf die Sensibilität von Daten im Gesundheitswesen das Regelwerk zum Datenaltruismus nach DGA zusätzliche Kriterien festlegen sollte. Sofern diese Vorschriften im Regelwerk die Nutzung einer sicheren Verarbeitungsumgebung im Gesundheitsbereich vorsehen, sollte die Verarbeitungsumgebung den in der EHDS-VO festgelegten Kriterien entsprechen (S. 3).

Das Verfügbarmachen von Daten in einer sicheren Verarbeitungsumgebung ist auch im GDNG vorgesehen. Die Datenzugangs- und Koordinierungsstelle soll diese für den jeweiligen Antrag auf Verknüpfung und Verarbeitung von spezifischen pseudonymisierten Daten für Forschungsvorhaben festlegen (§ 4 Abs. 5 S. 1 GDNG) und darüber hinaus Konzepte „zur Nutzung von sicheren Verarbeitungsumgebungen als Maßnahme zur Verbesserung des Datenschutzes und der Datensicherheit im Rahmen der Weiterverarbeitung von Gesundheitsdaten zu Forschungszwecken und weiteren im Gemeinwohl liegenden Zwecken" erstellen (§ 3 Abs. 2 Nr. 9 lit. a GDNG). Gesetzlich festgelegt ist, dass „[i]n einer sicheren Verarbeitungsumgebung (…) durch geeignete technische und organisatorische Maßnahmen sichergestellt sein [muss], dass die Verarbeitung durch die Antragstellenden auf das für den jeweiligen Nutzungszweck erforderliche Maß beschränkt ist und insbesondere ein Kopieren der Daten verhindert werden kann" (§ 4 Abs. 5 S. 2 GDNG). Ferner muss es sich um die sichere Verarbeitungsumgebung einer öffentlich-rechtlichen Stelle handeln (§ 4 Abs. 5 S. 1 GDNG). Das Bundesministerium für Gesundheit wird gemäß Abs. 9 S. 1 Nr. 2 ermächtigt Näheres zu den Anforderungen an sichere Verarbeitungsumgebungen und den Auswahlkriterien der sicheren Verarbeitungsumgebung durch die Datenzugangs- und Koordinierungsstelle durch Rechtsverordnung zu regeln. Dabei handelt sie im Benehmen mit dem oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie mit dem Bundesamt für Sicherheit in der Informationstechnik (Abs. 9 S. 2).[36]

Genomics England ermöglicht zugelassenen Forschern über eine sichere, cloud-basierte Forschungsumgebung („*Research Environment*") Zugang zu und Analyse von pseudonymisierten („*de-identified*") Daten in der NGRL entsprechend ihrem genehmigtem Forschungsprojekt.[37] Bevor Zugang gewährt wird, müssen die Forscher jedoch ein „*information governance training*" durchlaufen. Forschern stehen in der Forschungsumgebung nur bestimmte Tools zu Verfügung und sie können die Daten nicht aus der sicheren Forschungsumgebung entfernen, ein „*copy and paste*" der Informationen aus der Forschungsumgebung heraus ist nicht möglich. Es besteht nur die Möglichkeit

[36] Im Verfahren der Datenbereitstellung von Daten der elektronischen Patientenakte zu Forschungszwecken durch das Forschungsdatenzentrum (FDZ) (im Rahmen des Datentransparenzverfahrens nach §§ 303a ff. SGB V sowie § 363 SGB V) soll ebenfalls eine sichere Verarbeitungsumgebung im Sinne einer gesicherten virtuellen Umgebung unter der Kontrolle des FDZ genutzt werden (§ 20 Abs. 1 S. 2 Nr. 2, Abs. 4 Forschungsdatenzentrum Gesundheit-Verordnung).
[37] Genomics England, The Research Environment, abrufbar unter https://www.genomicsengland.co.uk/research (16.06.2025).

Zusammenfassungen ihrer Datenanalyse auf Antrag über ein „Airlock“ System zu exportieren. Die entsprechende Zusammenfassung wird jedoch vorher überprüft, um Re-identifizierung von Teilnehmenden zu verhindern. Außerdem ist der Internetzugang innerhalb der Forschungsumgebung auf bestimmte Seiten beschränkt („*whitelisted sites*“). Ein unabhängiges „*Access Review Committee*“ bestimmt die Bedingungen für den Zugang und die Datennutzung in der Forschungsumgebung. Mit Blick auf die Vorgaben der EHDS-VO und des GDNG könnte die Forschungsumgebung von *Genomics England* als Praxisbeispiel Vorbildcharakter haben.

UK Biobank sieht ebenfalls eine cloud-basierte Forschungsanalyse Plattform („*Research Analysis Platform*“) für die Analyse von pseudonymisierte („*de-identified*“) Daten durch zugelassene Forscher vor.[38] Dazu müssen Forscher ein sog. „*Material Transfer Agreement*“ unterzeichnen, einen Standard, der die Nutzung von Daten regelt. Aktivitäten auf der Plattform unterliegen einer Audit-Protokollierung und die Plattform selbst wird regelmäßigen Cyber-Security und Schwachstellentests unterzogen. Auch hier finden sich mithin Parallelen zu den erläuterten gesetzlichen Vorgaben auf europäischer Ebene wieder.

d) Internationale Öffnung

Gemäß Art. 87 Abs. 1 S. 1 EHDS-VO werden personenbezogene elektronische Gesundheitsdaten von Zugangsstellen bei der Anonymisierung, Pseudonymisierung und anderen Verarbeitungsvorgänge im Rahmen der Art. 67 bis 72 EHDS-VO über sichere Verarbeitungsumgebungen (Art. 73 und 75 Abs. 9 EHDS-VO) oder über HealthData@EU grundsätzlich in der Union gespeichert und verarbeitet. Abweichend davon dürfen sie ausnahmsweise in einem Drittland gespeichert und verarbeitet werden, sofern ein Angemessenheitsbeschluss gemäß Art. 45 DSGVO für das Drittland gilt (Abs. 2).

Die EHDS-VO sieht auch eine grenzüberschreitende Infrastruktur für die Sekundärnutzung von elektronischen Gesundheitsdaten vor, genannt *HealthData@EU* (Art. 75 EHDS-VO). Hierzu haben nicht nur eigens dafür benannte nationale Kontaktstellen, ein Zugangsdienst der Union (Kontaktstelle der Einrichtungen, Organe und sonstige Stellen der Union) sowie gesundheitsbezogene Forschungsinfrastrukturen oder ähnliche Infrastrukturen (unter bestimmten Voraussetzungen) Zugang (Art. 75 Abs. 1, 2 und 4 EHDS-VO). Ebenso können Drittländer oder internationale Organisationen befugte Teilnehmer werden, sofern gewisse Voraussetzungen erfüllt sind (Art. 75 Abs. 5 EHDS-VO).[39] Dabei ist unter anderem Kapitel V der DSGVO einzuhalten.[40] Darüber hinaus können Mitgliedstaaten im Einklang mit Art. 9 Abs. 4 DSGVO weitere Bedingungen für die Übermittlung von und den internationalen Zugang zu personenbezogenen Gesundheitsdaten (inklusive Beschränkungen) beibehalten oder einführen (Art. 90 S. 2 EHDS-VO). Ferner regelt die EHDS-VO die Zulässigkeit von Anträgen auf Gesundheitsdatenzugang und Gesundheitsdatenanfragen aus Drittländern (Art. 91 EHDS-VO).

Genomics England und *UK Biobank* ermöglichen Datenzugang global für zugelassene Forscher unter bestimmten Bedingungen. *Genomics England* erlaubt Zugang zu ihrer sicheren Forschungsumgebung für Forscher außerhalb des Vereinigten Königreichs nur unter drei alternativen Bedingungen: sofern das Land aus dem sie stammen entweder die Angemessenheitskriterien entsprechend den neuesten UK GDPR[41] Vorgaben erfüllt, die

[38] UK Biobank, UK Biobank Research Analysis Platform, abrufbar unter https://www.ukbiobank.ac.uk/enable-your-research/research-analysis-platform (16.06.2025).
[39] Dazu auch Erwgr. 81 EHDS-VO.
[40] Siehe auch Art. 90 S. 1 EHDS-VO.
[41] Siehe dazu Information Commissioner’s Office, The UK GDPR, abrufbar unter https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/ (16.06.2025): „The GDPR is retained in domestic law as the UK GDPR, but the UK has the

Risikobewertung von *Genomics England* betreffend der Datensicherheit erfüllt oder hinsichtlich des Zugangs zu Daten, die an *Genomics England* durch *NHS England* bereitgestellt werden, als geeignet von *NHS England* („from time to time“) genehmigt wird.[42]

UK Biobank übermittelt personenbezogene Daten an zugelassene Forscher außerhalb des Vereinigten Königreiches nur in zwei Fällen: entweder ist das entsprechende Land von einer „*adequacy regulation*“ abgedeckt oder die Übermittlung entspricht dem „*UK Addendum to the European Commission's Standard Contractual Clauses issued by the UK Information Commissioner under s.119A(1) of the Data Protection Act 2018*“.[43]

Im Vergleich zu den Vorgaben der EHDS-VO ist eine Parallele mit Blick auf die Berufung auf einen etwaigen Angemessenheitsbeschluss hervorzuheben. Hinsichtlich der Möglichkeit als gesundheitsbezogene Forschungsinfrastrukturen befugte Teilnehmer in HealthData@EU zu werden müssen die oben erläuterten Vorgaben beachtet werden, was bei einer Übertragung der Infrastruktur von *Genomics England* und *UK Biobank* in Deutschland zu berücksichtigen wäre.

e) Zwischenergebnis

Die Untersuchung der Aussichten des Datenschutz-Designs von *Genomics England* und *UK Biobank* übertragen in Deutschland unter die Strukturen des DGA und der EHDS-VO eingegliedert zu werden, hat mit Blick auf ihre Funktion, die Patienteneinbindung, die Nutzung einer sicheren Verarbeitungsumgebung sowie ihre internationale Öffnung aufgezeigt, dass Parallelen erkennbar sind und sie als Praxisbeispiele Vorbildcharakter für Datentreuhandinitiativen, insbesondere hinsichtlich der Umsetzung einer sicheren Verarbeitungsumgebung, haben könnten.

5. Ergebnis

Durch den Rechtsvergleich anhand von *UK Biobank* und *Genomics England* konnten hilfreiche Anhaltspunkt für die praktische Umsetzung von Datentreuhandinitiativen an der Schnittstelle zwischen Versorgung und Forschung erlangt werden.

V. Datentreuhänder und Gesundheitsdateninfrastrukturen

Im Berichtzeitraum entstand ferner ein Beitrag zum Rechtshandbuch „*Datentreuhand und Recht*“ (hrsg. von Johannes Buchheim, Florian Möslein und Sebastian Omlor) zum Thema „*Dateninfrastrukturen für die Forschung mit Gesundheitsdaten*“, der die Bedeutung und den Einsatz von Datentreuhändern im Zusammenhang mit Dateninfrastrukturen mit Blick auf datenschutzrechtliche Fragestellungen unter Berücksichtigung legislativer Entwicklungen behandelt. Das Handbuch mit unserem Beitrag wird 2025 beim Verlag C.H.Beck veröffentlicht.

independence to keep the framework under review. (…) The key principles, rights and obligations remain the same. However, there are implications for the rules on transfers of personal data between the UK and the EEA.“

[42] Genomics England, Genomics England privacy notice, abrufbar unter https://www.genomicsengland.co.uk/privacy-policy (16.06.2025).

[43] UK Biobank, Privacy Notice, abrufbar unter https://www.ukbiobank.ac.uk/explore-your-participation/basis-of-your-participation (16.06.2025).

C. Entwicklung eines dynamischen Einwilligungskonzeptes (M2.a)

Unter Berücksichtigung relevanter, aktueller gesetzlichen Entwicklungen auf europäischer und nationaler Ebene wurde ein dynamisches Einwilligungskonzept im TrustDNA Vorhaben entwickelt. Dabei wurden wir von einer unserer Honorarkräfte unterstützt.

I. Rechtlicher Hintergrund zur dynamischen Einwilligung

Um personenbezogene (pseudonymisierte) Patientendaten im Anwendungsbereich der DSGVO verarbeiten zu können muss die Verarbeitung auf einer Rechtsgrundlage gem. Art. 6 Abs. 1 UAbs. 1 DSGVO beruhen. Für eine Verarbeitung von genetischen Daten und Gesundheitsdaten ist zusätzlich Art. 9 Abs. 2 DSGVO zu berücksichtigen, der eine abschließende Liste von Ausnahmetatbeständen zu dem grundsätzlichen Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten (Absatz 1) enthält. Zu diesen Ausnahmetatbeständen zählt nach Art. 9 Abs. 2 lit. a DSGVO die ausdrückliche Einwilligung der betroffenen Person für einen oder mehrere festgelegte Zwecke.

Sollen Patientendaten zu Forschungszwecken verarbeitet werden ist bei einer Einwilligung als Rechtsgrundlage jedoch regelmäßig problematisch, dass zum Zeitpunkt der Datenerhebung der Zweck der Verarbeitung nicht vollständig angegeben werden kann (so Erwgr. 33 S. 1 DSGVO), was dazu führen kann, dass den Anforderungen an die Zweckbestimmung nicht genügt wird. Dies betrifft insbesondere Langzeitstudien.[44] In der Praxis haben sich deshalb verschiedene Einwilligungsmodelle etabliert, um dieser Herausforderung datenschutzkonform zu begegnen.

Das Modell der dynamischen Einwilligung ermöglicht es Betroffenen eine eingangs allgemein formulierte Einwilligung mit Fortschreiten des Forschungsprojektes kleinteiliger, abgestuft weiterzuführen.[45] Durch die Nutzung eines digitalen Tools können sie ihre Einwilligungsentscheidungen jederzeit einsehen und anpassen und es erlaubt Forschern gleichzeitig den betroffenen Personen Informationen zu den Forschungsvorhaben bereitzustellen und zu überblicken, welche Einwilligungen für die von ihnen verwendeten Daten vorliegen.[46]

Im Unterschied zu einer breiten Einwilligung als alleiniger rechtlicher Basis, die nicht weiter ausdifferenziert bzw. konkretisiert wird, ist der phasenorientierte Ansatz der dynamischen Einwilligung besser vereinbar mit den verschärften Einwilligungsbedingungen des Art. 9 Abs. 2 lit. a DSGVO.[47] Außerdem kommt der Ansatz dem in der DSGVO verankerten Prinzip der Transparenz zugute.[48] Positive Resonanz erfährt das Modell des „dynamic consent“ auch von Patient:innenseite, wie die Ergebnisse einer qualitativen Studie aus dem Vereinigten Königreich von 2016 zeigen.[49] Hervorzuheben ist hier die aktive Einbindung der Patient:innen im Forschungsprozess durch Kommunikationskanäle,[50] was in unserem Projekt ebenfalls angedacht ist. Kritisiert wird, dass ein zu kleinteiliger und kontinuierlicher Informations- und

[44] Ehmann/Selmayr/Raum DS-GVO Art. 89 Rn. 37.
[45] Vgl. nur Kaye et al., European Journal of Human Genetics 23 (2015), 141-146; vgl. auch EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1) 4. Mai 2020, Rn. 158.
[46] Teare/Prictor/Kaye, European Journal of Human Genetics 29 (2021), 649, 650, 653.
[47] Vgl. Spitz/Cornelius MedR 2022, 191, 194 f.; Molnár-Gábor DuD 2021, 799, 803.
[48] Zu weiteren Argumenten, die für den Ansatz der dynamischen Einwilligung sprechen, Molnár-Gábor DuD 2021, 799, 803.
[49] Spencer et al., Journal of Medical Internet Research 18 (2016)e66, 1 ff.
[50] Ibid.

Einwilligungsprozess zu einem „information overload“[51] und „consent fatigue“[52] bei den betroffenen Personen führen könnte, was bei der Umsetzung eines dynamischen Einwilligungsmodells berücksichtigt werden sollte. Hilfreich könnte hier etwa sein, dass betroffene Personen mithilfe des digitalen Tools ihre Einwilligungs- und Informationspräferenzen selbst festlegen können.[53] Zudem sollte beachtet werden, dass eine ausreichende Informationsgrundlage im Vorfeld einer Einwilligungserteilung, sowohl vor der eingangs allgemein formulierten weiten als auch vor den später erforderlichen kleinteiligeren abgestuften Einwilligungen, notwendigerweise geschaffen werden muss, damit betroffene Patienten überhaupt informiert einwilligen können.[54] Informationsmechanismen sollten eine Komplexitätsreduktion vorsehen und gleichzeitig die Informiertheit des Einwilligenden erreichen.[55]

II. Ziel des Einwilligungskonzepts im TrustDNA Vorhaben

Die Entwicklung eines dynamischen Einwilligungskonzepts im TrustDNA Vorhaben ist darauf ausgelegt ein digital unterstütztes Einwilligungsformat zu entwickeln, dass den datenschutzrechtlichen Vorgaben des Art. 4 Nr. 11, Art. 6 Abs. 1 UAbs. 1 lit. a, Art. 7, Art. 9 Abs. 2 lit. a und den Erwägungsgründen der DSGVO entspricht. Durch die dynamischen Einwilligungsmöglichkeiten sollen Daten für die medizinische Forschung in der Netzwerkmedizin besser zugänglich sein, wo bisher Rechtsunsicherheit bezüglich der Einwilligung als Rechtsgrundlage für die Nutzung von personenbezogenen Daten für die medizinische Forschung in kooperativen Formen der Datenverarbeitung herrschte. In der Umsetzung soll das Konzept sinnvoll in Prozesse der vorgesehenen Treuhandstelle eingebunden werden sowie das Einwilligungsmanagement ergänzen und erleichtern. Ferner sind als weiche Faktoren die anwenderfreundliche Handhabung von Formularen bzw. des Tools zur Erteilung bzw. dynamischen Anpassung der Einwilligung, die Verständlichkeit des Einwilligungsformats sowie eine lückenlose Erreichbarkeit aus Betroffenenperspektive zu berücksichtigen. Die folgenden Erläuterungen des Einwilligungskonzeptes konzentrieren sich auf datenschutzrechtliche Erwägungen.

III. Use-Case: DNA-Med

Als Anwendungsbeispiel der Netzwerkmedizin dient das *Deutsche Netzwerk für angewandte Präzisionsmedizin* (DNA-Med entstand aus der Initiative „Hauptstadt Urologie“ an der Charité - Universitätsmedizin Berlin.[56] Organisiert als gemeinnützige GmbH bietet DNA-Med ein Netzwerk für Prostatakrebspatienten, in dem Patienten und ihre behandelnden Ärzte mit Expert:innen für uru-onkologische Krebstherapie und Präzisionsmedizin vernetzt werden.) Hier wird explizit auf den Bericht des Projektpartners an der Charité verwiesen.

---

[51] Hinweis auf diese Kritik in Molnár-Gábor DuD 2021, 799, 803 mit Verweis auf Sheehan et al., Public Health Ethics 12 (2019), 225, 228.
[52] Hinweis auf diese Kritik in Kaye et al., European Journal of Human Genetics 23 (2015), 141, 143 mit Verweis auf Steinsbeckk/Myskja/Solberg European Journal of Human Genetics 21 (2013) 897, 898 f.; Sheehan et al., Public Health Ethics 12 (2019), 225, 228.
[53] Zum Beispiel wie häufig und über welches Medium sie informiert werden möchten, dazu Kaye et al., European Journal of Human Genetics 23 (2015) 141, 143.
[54] Dazu Spitz/Cornelius MedR 2022, 191, 193 f.
[55] Kühling ZfDR 2021, 1, 9.
[56] Dazu und weitere Informationen zu DNA-Med in BMBF – Nationale Dekade gegen Krebs, DNA-Med, abrufbar unter https://www.dekade-gegen-krebs.de/de/wir-ueber-uns/die-unterstuetzer/_documents/dna-med.html (13.06.2025).

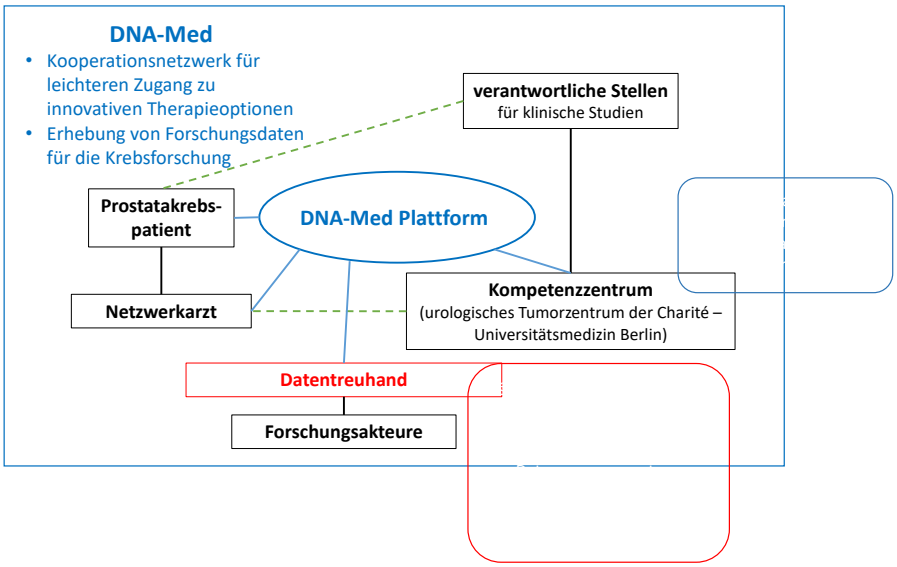

Abbildung 3: Einbindung einer Datentreuhand in das DNA-Med Netzwerk (eigene Darstellung von Anna Lina Gummersbach)

IV. Einbindung eines dynamischen Einwilligungsmodells in DNA-Med

Im Rahmen der Registrierung auf der DNA-Med Plattform wird der Patient über die Datenverarbeitungen im Zusammenhang mit der Nutzung der DNA-Med Plattform informiert und die erforderlichen datenschutzrechtlichen Einwilligungen werden eingeholt, bevor er seine persönlichen Profil-Daten eingibt. Für die Einwilligung in die Verarbeitung der pseudonymisierten Patientendaten zu Forschungszwecken kommt die Anwendung des dynamischen Einwilligungsmodells in Betracht.

Nach einer eingangs erteilten, allgemein gefassten Einwilligung, könnten Patienten über ein online Tool („*dynamic consent interface*“) im Laufe der Forschungsvorhaben kleinteiligere Einwilligungen bzw. Anpassungen oder Ergänzungen ihrer Einwilligung vornehmen oder sie teilweise oder ganz Widerrufen. Die Plattform des DNA-Med Netzwerks könnte dafür als sicherer Kommunikationskanal verwendet werden und entsprechende digitale Tools zur Verfügung stellen. Außerdem hätten Patienten über das *interface* die Möglichkeit ihre getroffenen Einwilligungsentscheidungen jederzeit zu überprüfen und nachträglich anzupassen, insbesondere wenn sich ihre Lebensumstände ändern oder neue Informationen zu Forschungsvorhaben mit ihren Daten vorliegen, die ihnen über die Plattform mitgeteilt werden. Gleichzeitig könnten die zuständigen Stellen in Forschungsvorhaben automatisiert über die Anpassungen informiert werden und die Datenverarbeitung entsprechend beschränken oder erweitern. So könnte ein dynamisches Einwilligungsmodell im DNA-Med Netzwerk etabliert werden, das durch die DNA-Med Plattform infrastrukturell umgesetzt würde.

V. Phasen der dynamischen Einwilligung

Über das „*dynamic consent interface*“ auf der Plattform des DNA-Med Netzwerks könnten Patienten ihre getroffenen Einwilligungen einsehen und von sich aus anpassen oder (teilweise) widerrufen, zum Beispiel, wenn sich ihr Gesundheitszustand ändert. Im Folgenden sollen die Phasen der dynamischen Einwilligung und insbesondere Situationen behandelt werden, in denen die eingangs erteilte, breite Einwilligung durch abgestufte Einwilligungen ergänzt werden müsste.

Im Folgenden sollen näher betrachtet werden, wann die eingangs erteilte Einwilligung durch abgestufte Einwilligungen ergänzt werden könnte.

In Betracht kommt zunächst, entsprechend dem genannten Hinweis, dass sobald die beteiligten Forschungsakteure und Forschungsvorhaben, etwa Forschungsfrage und -methode, sich konkretisieren die Patienten darüber informiert und eine konkrete Einwilligung dazu eingeholt werden sollte. Der EDSA spricht ferner davon, dass mit Fortschreiten der Forschung „Einwilligungen in die nachfolgenden Schritte des Projektes eingeholt werden [können], bevor die nächste Phase beginnt“ unter der Bedingung, dass eine solche Einwilligung „nach wie vor den anzuwendenden ethischen Standards der wissenschaftlichen Forschung entsprechen“ sollte.[57]

Es stellt sich insbesondere die Frage, wann von einer relevanten Änderung des Forschungsvorhabens auszugehen ist, die eine erneute Einwilligung notwendig macht. Entscheidend dafür ist, ob eine Zweckänderung vorliegt.[58] Voraussetzung dafür ist eine wesentliche inhaltliche Änderung der Datennutzung in der Forschung, wie zum Beispiel ein neues Forschungsprojekt, eine organisatorische oder institutionelle Änderung oder wesentlich abweichende Forschungsfrage.[59]

VI. Umsetzung des Einwilligungskonzeptes durch einen Datentreuhänder

Ein Datentreuhänder könnte zur Bereitstellung und Verwaltung des „*dynamic consent interface*“ im Zusammenhang mit dem Einwilligungsmanagement eingesetzt werden. In Ausübung dieser Aufgabe wäre er als Auftragsverarbeiter der DNA-Med gGmbH tätig, die als Verantwortlicher im Sinne der DSGVO für die Erfassung und Verwendung personenbezogener Patientendaten betreffend die Nutzung der DNA-Med Plattform auftritt. Im Rahmen der Weisungen durch die DNA-Med gGmbH könnte der Datentreuhänder dabei seiner Funktion entsprechend die datenschutzkonforme Teilung personenbezogener Daten zwischen betroffener Person und Datennutzer in der Forschung fördern. Diese Option wurden in enger Kooperation mit dem Teilprojekt an der Charité untersucht.

VII. Anknüpfung an europäische Initiativen

Ferner wurde die Relevanz der Einwilligung als Rechtsgrundlage unter dem Europäischen Gesundheitsdatenraum (European Health Data Space, EHDS) untersucht.

Ausweislich Erwgr. 51 S. 4 EHDS-VO bildet die Verordnung selbst „eine Rechtsgrundlage für die Sekundärnutzung personenbezogener elektronischer Gesundheitsdaten, einschließlich der Schutzmaßnahmen, die die Verarbeitung besonderer Datenkategorien nach Artikel 9 Absatz 2 Buchstaben g bis j der Verordnung (EU) 2016/679 um die Verarbeitung besonderer Datenkategorien in Bezug auf rechtmäßige Zwecke, vertrauenswürdige Governance für die Gewährung des Zugangs zu Gesundheitsdaten durch die Einbeziehung von Zugangsstellen für Gesundheitsdaten und die Verarbeitung in einer sicheren Umgebung sowie die in der Datengenehmigung festgelegten Modalitäten für die Datenverarbeitung zu ermöglichen“. In Erwgr. 52 S. 8 f. EHDS-VO werden als Rechtsgrundlagen ferner ausdrücklich Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO im Einklang mit Art. 9 Abs. 2 lit. i und j (für Gesundheitsdateninhaber) und Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO in Verbindung mit (soweit zutreffend) Art. 9 Abs. 2 lit. g bis j DSGVO (für Zugangsstellen) festgehalten.

Die EHDS-VO sieht grundsätzlich ein Opt-Out Verfahren (mit Widerspruchsmöglichkeit nach Art. 71 EHDS-VO) anstelle eines Opt-In Verfahrens (mit Einwilligung) vor, um gewisse Kategorien elektronischer Gesundheitsdaten für die Sekundärnutzung zur Verfügung zu

[57] EDSA, Leitlinien 05/2020, Rn. 158.
[58] Spitz/Cornelius MedR 2022, 191, 195.
[59] Ibid.

stellen, was auch genetische Daten betrifft (Art. 51 Abs. 1 lit. f EHDS-VO).[60] Der noch im Entwurf zur EHDS-VO (EHDS-VO-E[61]) enthaltene Art. 33 Abs. 5 EHDS-VO-E wies darauf hin, dass sich die nationalen Zugangsstellen bei der Gewährung des Gesundheitsdatenzugangs auf die in Kapitel IV festgelegten Pflichten berufen sollten, sofern nach nationalem Recht die Einwilligung der betroffenen natürlichen Person erforderlich ist. Dieser Absatz ist im in Kraft getretenen Verordnungstext nicht mehr enthalten. Allerdings findet man im Art. 51 Abs. 4 EHDS-VO die Möglichkeit für Mitgliedstaaten „strengere Maßnahmen und zusätzliche Schutzmaßnahmen" einzuführen, um den Wert und die Sensibilität von bestimmten Datenkategorien, wie genetischen Daten, zu schützen. Vor diesem Hintergrund könnte man überlegen, ob der Normtext so ausgelegt werden kann, dass er die Einwilligung als eine „strengere Maßnahme oder Schutzmaßnahme" erfasst. Ist dies nicht der Fall, müsste man davon ausgehen, dass durch die Einführung der Opt-Out Regelung eine Einwilligung, also Opt-In, um genetische Daten für die Sekundärnutzung im Rahmen des EHDS zur Verfügung zu stellen, ausgeschlossen wäre.

Relevant ist die Fragestellung vor dem Hintergrund, dass es im deutschen Recht eine Regelung zur Einwilligung für die Datenverarbeitung im Rahmen des *Modellvorhabens zur umfassenden Diagnostik und Therapiefindung mittels Genomsequenzierung bei seltenen und bei onkologischen Erkrankungen* (im Folgenden *Modellvorhaben Genomsequenzierung*) gibt. Hier ist eine vorherige schriftliche oder elektronische Einwilligung der Versicherten für die Nutzung ihrer personenbezogenen Daten zu wissenschaftlichen Forschungszwecken (§ 64e Abs. 6 S. 2, Abs. 11 S. 3 Nr. 4 SGB V) bzw. zur Fallidentifizierung durch einen ersuchenden Leistungserbringer (§ 64e Abs. 6 S. 2, Abs. 9c S. 7 Nr. 1 SGB V) notwendig. Durch die Vorgaben des § 64e SGB V zur vorherigen Einwilligung hat der nationale Gesetzgeber von seiner Möglichkeit nach Art. 9 Abs. 4 DSGVO Gebrauch gemacht.[62]

Für die Auslegung des Art. 51 Abs. 4 EHDS-VO kann Erwgr. 52 EHDS-VO herangezogen werden, dessen Satz 5 besagt, dass „die Mitgliedstaaten keine weiteren Bedingungen gemäß Artikel 9 Absatz 4 der Verordnung (EU) 2016/679 für die Verarbeitung personenbezogener elektronischer Gesundheitsdaten für die Sekundärnutzung im Rahmen der vorliegenden Verordnung beibehalten oder einführen [sollten], einschließlich Beschränkungen und spezifischer Bestimmungen, die die Einwilligung natürlicher Personen erfordern, mit Ausnahme der Einführung strengerer Maßnahmen und zusätzlicher Schutzmaßnahmen auf nationaler Ebene, die darauf abzielen, die Sensibilität und den Wert bestimmter Daten zu schützen, wie in der vorliegenden Verordnung festgelegt". Mit Blick auf Erwgr. 11 S. 1 EHDS-VO wird deutlich, dass die EHDS-VO die Einwilligung als Schutzmaßnahme versteht. Legt man nun Art. 51 Abs. 4 EHDS-VO im Lichte der genannten Erwägungsgründe aus kann die Einwilligung als zusätzliche Schutzmaßnahe ausnahmsweise zum Schutz der Sensibilität und dem Wert von genetischen Daten in mitgliedstaatlichem Recht als zusätzliche Bedingung iSd Art. 9 Abs. 4 DSGVO eingeführt oder beibehalten werden. Somit kann auch die Regelung des § 64e SGB V zur Einwilligung unter dem EHDS bestehen bleiben.

D. Handreichungen und SOPs (M2.b)

Handreichungen zum Ausgleich unspezifischer Angaben in Alteinwilligungen durch Rechtemanagement sowie SOPs für das Rechtemanagement bei Neueinwilligungen wurden im Berichtzeitraum fertiggestellt. Auch für diesen Meilenstein war die aktuelle gesetzliche

[60] Ein Opt-Out Verfahren ist auch mit Einführung des GDNG in Vorbereitung auf die Anbindung an den EHDS in Deutschland eingeführt worden, vgl. § 363 Abs. 1 SGB V.
[61] COM(2022) 197 final.
[62] Vgl. BeckOGK/Roters SGB V § 64e Rn. 28.

Entwicklung auf europäischer und nationaler Ebene im Bereich der Bereitstellung von Gesundheitsdaten für Forschungszwecke relevant.

I. Handreichungen

Um Daten in der Netzwerkmedizin der Forschung auf Grundlage einer sog. Alteinwilligung[63] zur Verfügung zu stellen, sollen die nachfolgenden Handreichungen berücksichtigt werden. Diese bieten einen Maßstab, um festzustellen, ob die jeweilige Alteinwilligung als Rechtsgrundlage angewendet werden kann und bieten Leitlinien zum Umgang mit und Ausgleich von unspezifischen Angaben in Alteinwilligungen. Rechtlicher Ausgangspunkt ist Erwgr. 171 S. 3 DSGVO.[64] Geprüft werden muss zum einen, ob die Alteinwilligung mit den datenschutzrechtlichen Vorgaben der DSGVO vereinbar und zum anderen ob die Art der primären[65] Verarbeitung mit der sekundären[66] vergleichbar ist.[67]

1. Vereinbarkeit der Alteinwilligung mit DSGVO-Vorgaben

Für die Prüfung der Vereinbarkeit mit DSGVO-Vorgaben sind unter anderem die Grundsätze aus Art. 5 Abs. 1 DSGVO heranzuziehen.[68] Daran ist der gesamte Verarbeitungskontext der Alteinwilligung, etwa der Zweck der Verarbeitung, der/die Verarbeiter, Eigenschaften der Daten, Art der Verarbeitung (auch Maßnahmen zur Datensicherheit) und das Datenschutzniveau sowie Empfänger, zu messen.[69] Sind die Angaben der Alteinwilligung derart unspezifisch, dass sie den Grundsätzen der DSGVO nicht genügen, stellt die Alteinwilligung keine taugliche Rechtsgrundlage dar. In diesem Fall ist eine neue Einwilligung einzuholen, die hinreichend spezifische Angaben zum Ausgleich der unspezifischen Angaben der Alteinwilligung enthält. Sind die Angaben noch hinreichend spezifisch, um die Vorgaben zu erfüllen, muss der nächste Schritt der Prüfung vorgenommen werden.

2. Vergleichbarkeit der primären mit der sekundären Verarbeitung

Zur Prüfung der Vergleichbarkeit von primärer und sekundärer Vereinbarkeit ist auf das Risiko[70] der Verarbeitung abzustellen.[71] Maßstab ist dabei, ob das Risiko und die Tragweite der Weiterverarbeitung für die betroffene Person „zum Zeitpunkt der Einwilligung überschaubar war und in welchem Umfang eine Weiterverarbeitung erfolgt".[72] Dazu sind die Art der Daten, der Zweck der Verarbeitung, Art und Weise der Verarbeitung und der Verantwortliche Verarbeiter genauer zu untersuchen.[73] Auch hier ist zu bedenken, ob die Angaben der Alteinwilligung hinreichend spezifisch für eine Vergleichbarkeit sind.

Für die Vergleichbarkeit der Daten kommt es mit Blick auf Art. 4 Nr. 1 DSGVO darauf an, welches Risiko mit ihnen einhergeht, wie sensitiv sie sind und auf die Informationen, die sie enthalten.[74] Dabei muss zunächst geklärt werden, ob sich die Dateninformationen geändert haben.[75] Wenn dies der Fall ist, müssen die neuen Informationen sowie die damit

[63] Alteinwilligungen meint Einwilligungen, deren Erteilung vor der Geltung der DSGVO lag.
[64] Molnár-Gábor/Kaldowski/Schenk ZD 2022, 376.
[65] Gemeint ist die Verarbeitung, die die Alteinwilligung ursprünglich betraf.
[66] Gemeint ist die Verarbeitung im Rahmen der Zurverfügungstellung der Daten für die Forschung.
[67] Molnár-Gábor/Kaldowski/Schenk ZD 2022, 376.
[68] Molnár-Gábor/Kaldowski/Schenk ZD 2022, 376, 378.
[69] Ibid.
[70] Siehe dazu unter E. Technische und organisatorische Maßnahmen (TOMs) (M3).
[71] Roßnagel ZD 2019, 157, 162.
[72] Molnár-Gábor/Kaldowski/Schenk ZD 2022, 376, 376, 379.
[73] Ibid.
[74] Ibid.
[75] Siehe Abbildung 2 in ibid.

einhergehenden Risiken für die Betroffenen vorhersehbar sein.[76] Das ist wiederum gegeben, wenn das Risiko noch immer gleich bzw. vergleichbar ist oder die Erhebung neuer Informationen in der Einwilligung genannt wurde.[77]

Für die Vergleichbarkeit der Verarbeitungszwecke kommt es insbesondere auf die Bestimmtheit der Einwilligung und ob eine Privilegierung der Forschung nach Art. 5 Abs. 1 lit. b DSGVO angenommen werden kann an.[78]

Für die Vergleichbarkeit der verantwortlichen Verarbeiter ist entscheidend, ob in der Alteinwilligung mehrere oder ein konkreter Verarbeiter als gem. Art. 24 DSGVO Verantwortlicher vorgesehen sind.[79] Außerdem ist maßgeblich, inwieweit der Kreis der Verarbeiter ausgelegen bzw. erweitert werden kann.[80] Unspezifische Angaben müssen mithin entsprechend ausgelegt werden. Eine Vergleichbarkeit kann etwa durch organisatorische Anpassungsmaßnahmen erreicht werden, die eine Zugangsbeschränkung, z.B. durch Rechtemanagement, beinhalten.[81] So kann das dem Verarbeiter anhaftende Risiko reduziert und auf ein Maß gebracht werden, das mit der primären Verarbeitung vergleichbar ist.[82] An der Vergleichbarkeit wird es jedoch in der Regel fehlen, wenn nur ein spezifischer und kein weiterer Verarbeiter in der ursprünglichen Alteinwilligung vorgesehen ist.[83] Die Prüfung muss aber stets im Einzelfall erfolgen.

Für die Vergleichbarkeit der Art und Weise der Verarbeitung ist das zugesicherte Datenschutzniveau sowie das damit einhergehende Risiko für die Rechte der Betroffenen entscheidend.[84] Im Einzelfall kann die Vergleichbarkeit unter Umständen durch eine Anpassung der TOMs erzielt werden.[85] Auch hier könnte ein Rechtemanagement eingebunden werden, das zum Ausgleich unspezifischer Angaben in Alteinwilligungen beiträgt. Dies wurde während der Projektarbeit zusammen mit den Verbundpartnern an der Charité eruiert.

[76] Ibid.
[77] Ibid.
[78] Beachte hierzu weitere Erläuterungen und Abbildung 3 in Molnár-Gábor/Kaldowski/Schenk ZD 2022, 376, 380.
[79] Molnár-Gábor/Kaldowski/Schenk ZD 2022, 376, 381, siehe auch Abbildung 4 in dies. 380.
[80] Ibid.
[81] Ibid.
[82] Ibid.
[83] Molnár-Gábor/Kaldowski/Schenk ZD 2022, 376, 383.
[84] Ibid.
[85] Beachte dazu die Ausführungen unter E. Technische und organisatorische Maßnahmen (TOMs) (M3).

II. SOPs

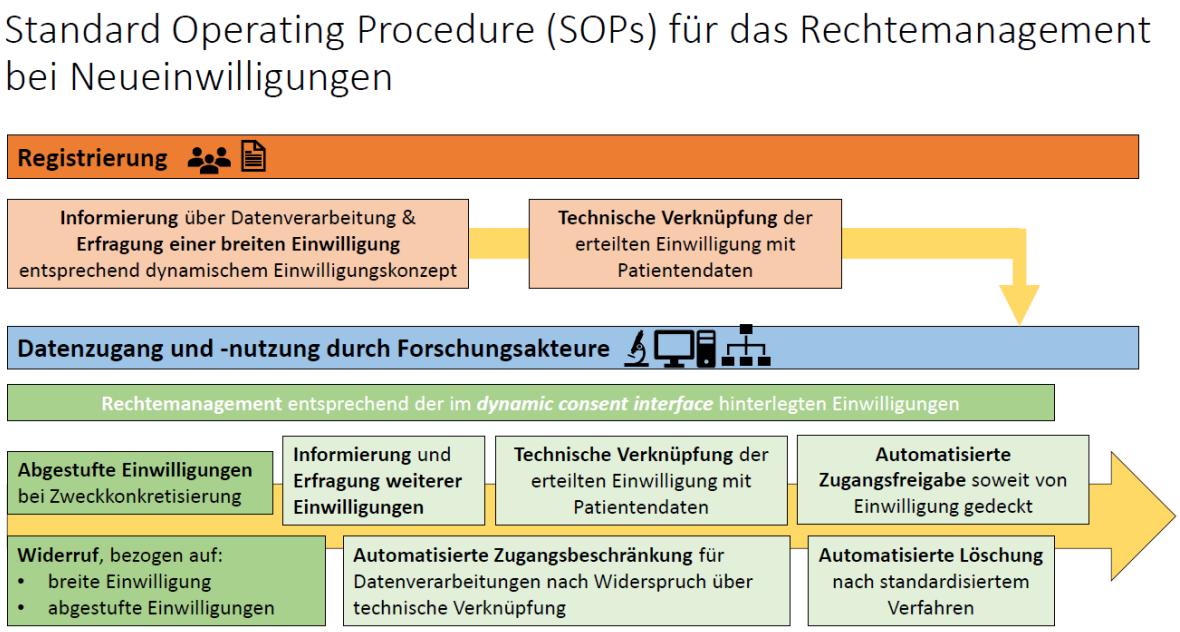

Abbildung 4: Standard Operating Procedure(SOPs) (eigene Darstellung von Marc Nestor und Anna Lina Gummersbach)

E. Technische und organisatorische Maßnahmen (TOMs) (M3)

Im Berichtzeitraum wurden die Untersuchungen zu TOMs des Datenzugangs und der Nutzung im rechtswissenschaftlichen Teilprojekt abgeschlossen. Hierbei wurde auf die Expertise einer Honorarkraft zurückgegriffen und ein fruchtbarer Austausch mit den Projektpartnern hat stattgefunden.

I. Einleitung

Technische und organisatorische Maßnahmen (TOMs) müssen gem. Art. 24 Abs. 1 S. 1 DSGVO getroffen werden, um eine datenschutzgemäße Verarbeitung gemäß der DSGVO sicherzustellen. Dies beinhaltet gemäß Art. 32 Abs. 1 DSGVO ein dem Risiko für die Freiheiten und Rechte von natürlichen Personen angemessenes Schutzniveau zu gewährleisten. Der Risikobegriff wird von der DSGVO nicht konkret bestimmt. In einer Zusammenschau von Erwgr. 75 und 94 S. 2 DSGVO lässt er sich laut Datenschutzkonferenz (DSK) wie folgt herleiten: „Ein Risiko im Sinne der DS-GVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann“; „[e]s hat zwei Dimensionen: Erstens die Schwere des Schadens und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten“.[86] Die Eintrittswahrscheinlichkeit und Schwere des Risikos bzw. des Schadens müssen bei der Festlegung von TOMs berücksichtigt werden (Art. 24 Abs. 1 S. 1, 25 Abs. 1, 32 Abs. 1 1. Hs. DSGVO). Das Risiko ist objektiv zu beurteilen (Erwgr. 76 S. 2 DSGVO). Der Schaden kann physischer, materieller oder immaterieller Natur sein (Erwgr. 75 DSGVO). Als mögliche Schäden nennt Erwgr. 75 und 85 S. 1 DSGVO beispielhaft etwa die Diskriminierung, die Rufschädigung, den Identitätsbetrug oder -diebstahl oder den Verlust der Vertraulichkeit von personenbezogenen Daten, die dem Berufsgeheimnis unterliegen. Hinsichtlich der Sicherheit der Verarbeitung benennt Art. 32 Abs. 2 DSGVO mit der

[86] DSK, Kurzpapier Nr. 18, Stand: 26.04.2018, S. 1.

Verarbeitung verbundene Risiken insbesondere durch den Verlust, die Veränderung, die Vernichtung oder den unbefugten Zugang zu beziehungsweise die unbefugte Offenlegung von personenbezogenen Daten.

Im Rahmen der Vorgaben zu Datenschutz durch Technikgestaltung („*data protection by design*“) und durch datenschutzfreundliche Voreinstellung („*data protection by default*“) verlangt Art. 25 DSGVO vom Verantwortlichen eine frühzeitige Befassung mit datenschutzrechtlichen Vorgaben und einer entsprechend frühzeitigen Festlegung geeigneter TOMs, die die Datenschutzgrundsätze, wie die Datenminimierung (siehe dazu Abs. 2) wirksam umsetzen und notwendige Garantien in die Verarbeitung integrieren, um den Anforderungen der DSGVO zu genügen und die Betroffenenrechte zu schützen.[87]

Neben den genannten Faktoren der Eintrittswahrscheinlichkeit und Schwere müssen bei der Festlegung von geeigneten TOMs gem. Art. 25 Abs. 1 und Art. 32 Abs. 1 1. Hs. DSGVO auch der Stand der Technik und die Implementierungskosten sowie Umstände, Umfang, Art und Zwecke der Verarbeitung berücksichtigt werden.

Die Festlegung von geeigneten TOMs gehört zu den zentralen Pflichten von (gemeinsam) Verantwortlichen und Auftragsverarbeitern und ist damit ein zentraler Bestandteil der datenschutzkonformen Verarbeitung personenbezogener Daten. Die DSGVO sieht zudem die regelmäßige Bewertung, Überprüfung und Evaluierung der Wirksamkeit der TOMs vor (vgl. Art. 24 Abs. 1 S. 2, Art. 32 Abs. 1 S. 1 2. Hs. lit. d DSGVO).[88] Eine Herausforderung stellt jedoch die regelmäßig mit Rechtsunsicherheit behaftete Entscheidung über geeignete TOMs im Einzelfall dar. Zwar zählt die DSGVO in Art. 32 Abs. 1 2. Hs. lit. a bis d DSGVO beispielhaft TOMs wie zum Beispiel die Pseudonymisierung (lit. a) auf, die auch von Art. 25 Abs. 1 DSGVO erfasst wird.[89] Die gelisteten Maßnahmen sind aber sehr generell gehalten,[90] sodass die Prüfung der „Geeignetheit“ der Maßnahmen dem Rechtsanwender im Einzelfall überlassen bleibt. Weder der Normtext mit Blick auf die Erwägungsgründe noch Leitlinien des Europäischen Datenschutzausschusses (EDSA) waren bislang in der Lage die mit der Auslegung der weit gefassten Vorgaben verbundenen Rechtsunsicherheit auf Verarbeiterseite zu beseitigen. Orientierung für Verantwortliche und (soweit anwendbar) Auftragsverarbeiter in Deutschland bieten die Vorgaben der Datenschutzkonferenz (DSK) in ihrem Kurzpapier Nr. 5 (zur „Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO“)[91] und Nr. 18 (zum „Risiko für die Rechte und Freiheiten natürlicher Personen“)[92], sowie das von ihnen empfohlene Standard-Datenschutzmodell (SDM)[93], das als ein Werkzeug zu verstehen ist, „mit dem die risikoadäquate Auswahl und rechtliche Bewertung der von der DS-GVO geforderten technischen und organisatorischen Maßnahmen“ sowie die Erfüllung der datenschutzrechtlichen Rechenschafts- und Nachweispflichten durch Verantwortliche unterstützt wird.[94]

---

[87] DSK, Das Standard-Datenschutzmodell, Version 3.1a, S. 5 abrufbar unter: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode-V31a.pdf (11.06.2025); siehe auch Erwgr. 78 DSGVO.
[88] Ibid.
[89] Erwgr. 78 S. 3 DSGVO äußert sich beispielhaft zu Maßnahmen, die den Grundsätzen des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen genügen.
[90] Außerdem gibt es etwa im technischen Bereich mehrerer Pseudonymisierungsverfahren, dazu Kühling/Buchner/Jandt DS-GVO Art. 32 Rn. 18.
[91] DSK, Kurzpapier Nr. 5, Stand: 17.12.2018.
[92] DSK, Kurzpapier Nr. 18, Stand: 26.04.2018.
[93] DSK, Das Standard-Datenschutzmodell, Version 3.1a, abrufbar unter https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode-V31a.pdf (11.06.2025); kritisch zum Standard-Datenschutzmodell in der Version 3.0 Hansen-Oest DSB 2023, 318.
[94] LfDI MV, Standard-Datenschutzmodell, abrufbar unter https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ (11.06.2025).

Im Folgenden soll zunächst auf mögliche Lösungsansätze im Umgang mit der beschriebenen Rechtsunsicherheit im Kontext der Verarbeitung von Gesundheitsdaten vor dem Hintergrund aktueller legislativer Vorgaben auf europäischer Ebene und in Deutschland eingegangen werden (II.). Sodann wird auf die Untersuchung hingewiesen, geeignete TOMs unter Einbindung eines Datentreuhänders im *Deutschen Netzwerk für angewandte Präzisionsmedizin* (DNA-Med)[95] zu definieren (III.).

II. TOMs im Gesundheitskontext, insb. Sekundärnutzung

Die DSGVO sieht selbst gemäß Art. 24 Abs. 3 DSGVO zwei Mittel zur Erhöhung der Rechtssicherheit vor: genehmigte Verhaltensregeln nach Art. 40 DSGVO und Zertifizierungen nach Art. 42 DSGVO, deren bisherige Umsetzung in der Praxis nachfolgend näher erörtert wird (1.). Ferner wird die Pseudonymisierung als kontextuelle Anonymisierung evaluiert (2.). Darüber hinaus könnten die Vorgaben des DGA sowie bereichsspezifische Vorgaben der EHDS-Verordnung und des GDNG als Konkretisierung datenschutzrechtlicher Vorgaben zu einer höheren Rechtssicherheit für die Rechtsanwender beitragen (3.). Schließlich könnte die Rechtsunsicherheit minimiert werden, indem sich der Rechtsanwender bei der Auslegung der weit gefassten Anforderungen an TOMs dem Grundsatz der Verhältnismäßigkeit bzw. der Risikominimierung im Einzelfall verschreibt (4.). Gerade im letzteren Fall können Datentreuhänder eine wichtige Rolle einnehmen.

1. Genehmigte Verhaltensregeln und Zertifizierungen

Als Gesichtspunkt, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen sieht die DSGVO in Art. 24 Abs. 3 die Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DSGVO oder eines genehmigten Zertifizierungsverfahrens gem. Art. 42 DSGVO vor.[96] Ein genehmigtes Zertifizierungsverfahren kann explizit auch als Faktor zum Nachweis zur Erfüllung der Anforderungen aus Art. 25 Abs. 1 und 2 und Art. 32 Abs. 1 DSGVO herangezogen werden (Art. 25 Abs. 3 und Art. 32 Abs. 3 DSGVO).

Trotz erster Umsetzungen stecken Zertifizierungen nach der DSGVO immer noch in den Kinderschuhen. Ferner droht gerade die Tätigkeit des Datentreuhänders in der Netzwerkmedizin an der Schnittstelle zwischen Versorgung und Forschung aufgrund seines besonderen und komplexen Verarbeitungskontextes, insbesondere im Zusammenhang mit genetischen und biomedizinischen Daten, von der Anwendbarkeit einzelner Zertifizierungsprogramme ausgeschlossen zu sein. So sollen beispielsweise die durch den EDSA genehmigten Europrivacy-Zertifizierungskriterien im Bereich „E-Health“ Anwendung finden, während Verarbeitungsvorgänge im Zusammenhang mit „biomedizinischen Daten“ und die Datenverarbeitung von genetischen Daten aus dem Anwendungsbereich der Europrivacy-Kriterien ausgenommen sind.[97] Insofern ist nach weiteren Mitteln zur Konkretisierung der Anforderungen an TOMs zu suchen.

Genehmigte Verhaltensregeln gemäß Art. 40 DSGVO könnten die zu ergreifenden TOMs für eine Branche oder Berufsgruppe mitbestimmen. Allerdings ist in der Europäischen Union davon nur in geringem Maße Gebrauch gemacht worden und es kommen für Datentreuhänder in der Netzwerkmedizin in Deutschland auch nur drei genehmigte Verhaltensregeln in

---

[95] Dazu BMBF – Nationale Dekade gegen Krebs, DNA-Med, abrufbar unter https://www.dekade-gegen-krebs.de/de/wir-ueber-uns/die-unterstuetzer/_documents/dna-med.html (11.06.2025).
[96] Ferner wird die Einhaltung von genehmigten Verhaltensregeln und Zertifizierungen gem. Art. 83 Abs. 2 S. 2 lit. j DSGVO bei der Verhängung und der Höhe einer Geldbuße berücksichtigt.
[97] EDSA, Stellungnahme 28/2022, Rn. 12; Europrivacy, Europrivacy Overview, https://www.europrivacy.com/en/ep/overview (11.06.2025): *„Thanks to its hybrid model, Europrivacy is applicable to almost all data processing activities, including to innovative technologies such as artificial intelligence, blockchain, e-health, and Internet of things. There is a number of specific exclusions, such as biomedical data”.*

Betracht. Diese sind die nationale „Trusted Data Processor“-Verhaltensregel[98], der „EU Cloud Code of Conduct“[99] sowie der „CISPE – Code of Conduct for Cloud Infrastructure Service Providers in Europe”[100]. Ihr Anwendungsbereich beschränkt sich jedoch in persönlicher Hinsicht auf Auftragsverarbeiter beziehungsweise auf Auftragsverarbeiter als Cloud-Anbieter und ihr sachlicher Anwendungsbereich ist im Einzelfall sorgfältig zu prüfen. Die Anwendbarkeit der „Trusted Data Processor“-Verhaltensregel zum Beispiel, die „ausschließlich allgemein und generell geltende Mindestanforderungen im Verhältnis zwischen Auftraggeber und Auftragsverarbeiter“ enthält, „ohne gesonderte eventuell besonders bestehende Schutzbedarfe abzudecken“ erscheint in der Netzwerkmedizin, in der eine Vielzahl der verarbeiteten Daten potentiell als besonders sensibel nach Art. 9 DSGVO einzustufen sind, äußerst fraglich.[101]

Somit verbleibt Rechtsunsicherheit für Datentreuhänder in der Netzwerkmedizin als Verantwortliche bzw. Auftragsverarbeiter bezüglich der Wahl geeigneter technischer und organisatorischer Maßnahmen. Es ist abzuwarten, ob zukünftig durch genehmigte Verhaltensregeln und Zertifizierungsmöglichkeiten hier Abhilfe geschaffen werden kann.

2. Pseudonymisierung

Die Pseudonymisierung wird von Art. 25 Abs. 1 und Art. 32 Abs. 1 2. Hs. lit. a DSGVO explizit als mögliche TOM genannt. Eine Legaldefinition findet man in Art. 4 Nr. 5 DSGVO. Erwgr. 26 S. 2 DSGVO macht deutlich, dass es sich dabei um personenbezogene Daten handelt, im Unterschied zu anonymisierten (vormals personenbezogenen) Daten, deren Verarbeitung, etwa zu Forschungszwecken, nicht im Anwendungsbereich der DSGVO liegt (Erwgr. 26 S. 5 f. DSGVO). Die Frage, ob es sich bei einer Pseudonymisierung um eine kontextuelle Anonymisierung handelt, hat mithin weitreichende Folgen, da die Anwendbarkeit der DSGVO auf Datenverarbeitungsvorgänge vom Vorliegen personenbezogener Daten abhängig ist (vgl. Art. 2 Abs. 1 i.V.m. Art. 4 Nr. 1 DSGVO). Gemäß Art. 4 Nr. 1 1. Hs. DSGVO handelt es sich dabei um solche Informationen, „die sich auf eine identifizierte oder identifizierbare Person (…) beziehen“. Berücksichtigt werden sollten in der Frage der Identifizierbarkeit einer natürlichen Person laut Erwgr. 26 S. 3 DSGVO alle Mittel, „(…) die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren (…)“. Dafür sollten „alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind“ (Erwgr. 26 S. 4 DSGVO). Der EuGH präzisiert diesen Beurteilungsmaßstab insofern, als dass für die Beurteilung der Identifizierbarkeit solche Mittel nicht Berücksichtigung finden sollten, die einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würden, da das Risiko einer Identifizierung hier „de facto vernachlässigbar“ ist.[102] Die im April 2023 vom EuG

---

[98] VFV, Verhaltensregel „Anforderungen an Auftragsverarbeiter nach Art. 28 DS-GVO“ Version 1.0, 09.06.2022, abrufbar unter https://www.verhaltensregel.eu/wp-content/uploads/2022/11/Verhaltensregel_Trusted_Data_Processor_V1.pdf (11.06.2025); LfDI BW, Verhaltensregeln für Auftragsverarbeiter, abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/verhaltensregeln-fuer-auftragsverarbeiter/ (11.06.2025).

[99] CISPE Data Protection Code of Conduct for Cloud Infrastructure Service Providers, 9.2.2021, abrufbar unter https://www.codeofconduct.cloud/the-code/ (11.06.2025).

[100] EU Cloud Code of Conduct, What is the EU Cloud Code of Conduct? abrufbar unter https://eucoc.cloud/en/about/about-eu-cloud-coc (11.06.2025).

[101] VFV, Verhaltensregel „Anforderungen an die Auftragsverarbeiter nach Artikel 28 DS-GVO“ Version 1.0, 09.06.2022, S. 2, abrufbar unter https://www.verhaltensregel.eu/wp-content/uploads/2022/11/Verhaltensregel_Trusted_Data_Processor_V1.pdf (11.06.2025).

[102] EuGH 19.10.2016 – C-582/14, ECLI:EU:C:2016:779 = NJW 2016, 3579 Rn. 45 f. – Breyer.

getroffene Entscheidung[103] bestätigt den risikobasierten Ansatz des EuGH.[104] Ferner kommt es laut EuG für die Annahme des Personenbezugs auf die Möglichkeit jeder datenverarbeitenden Stelle einzeln an, betroffene Personen zu identifizieren.[105] Interessant ist diese Position vor allem mit Blick auf die Situation der Weitergabe von pseudonymisierten Daten an Dritte. Hat der Empfänger keine Möglichkeit die pseudonymisierten Daten zu re-identifizieren, sind sie dem EuG folgend für ihn ohne Personenbezug und die von ihm durchgeführte Datenverarbeitung unterfällt nicht dem Anwendungsbereich der DSGVO.[106] Für Datentreuhänder an der Schnittstelle zwischen Versorgung und Forschung hat die Frage nach dem Verständnis des Personenbezugs Relevanz, wenn sie etwa personenbezogene Daten pseudonymisieren, bevor sie der Forschung bereitgestellt werden sollen, oder Pseudonymisierungstools als Produkt anbieten.

Die Abgrenzung zwischen nicht personenbezogenen (anonymisierten) und personenbezogen (pseudonymisierten) Daten ist unter der EHDS-VO sehr relevant. Die EHDS-VO verweist für die Begriffsbestimmung von „personenbezogenen Daten“ und „Gesundheitsdaten“ sowie „genetischen Daten“ auf die DSGVO, Art. 2 Abs. 1 lit. a EHDS-VO. Für die Zwecke der Verordnung bestimmt die EHDS-VO zusätzlich, dass „personenbezogene elektronische Gesundheitsdaten“ genetische Daten sowie Gesundheitsdaten bezeichnet, die in elektronischer Form verarbeitet werden (Abs. 2 lit. a). Gemäß Art. 2 Abs. 2 lit. b EHDS-VO sind „nicht personenbezogene elektronische Gesundheitsdaten“ wie folgt definiert: „elektronische Gesundheitsdaten, die keine personenbezogenen elektronischen Gesundheitsdaten sind und zu denen sowohl Daten zählen, die anonymisiert wurden, sodass sie sich nicht mehr auf eine bestimmte oder bestimmbare natürliche Person (im Folgenden „betroffene Person“) beziehen, als auch Daten, die sich nie auf eine betroffene Person bezogen haben“. Den Datennutzer trifft beim Antrag auf Zugang zu Gesundheitsdaten zur Sekundärnutzung eine Begründungs- und Rechenschaftspflicht gem. Art. 67 Abs. 2 lit. e, Abs. 4 EHDS-VO, wenn er Zugang zu personenbezogenen Gesundheitsdaten in pseudonymisierter Form statt Gesundheitsdaten in anonymisierter Form beantragt. Außerdem ist eine Abgrenzung auch essentiell, wenn es um die Frage geht, ob Gesundheitsdatennutzer elektronische Gesundheitsdaten aus der sicheren Verarbeitungsumgebung herunterladen dürfen, vgl. Art. 73 Abs. 2 UAbs. 2 EHDS-VO.

Denkbar ist, dass sich die Kommission zum Anonymitätsbegriff im Sinne des EHDS-VO im Wege von Durchführungsrechtakten im Zusammenhang mit den Anforderungen an eine sichere Verarbeitungsumgebung äußert (siehe Art. 73 Abs. 5 EHDS-VO). Auf Ebene der Anwendung könnten schriftliche Beiträge des EHDS-Ausschusses in Bezug auf die Sekundärnutzung zur „Durchführung der Vorschriften für den Zugang zu elektronischen Gesundheitsdaten“ gem. Art. 94 Abs. 2 lit. b i) EHDS-VO für mehr Rechtssicherheit sorgen. Eine klare und einheitliche Auslegung wird in der Praxis dringend erforderlich sein, da ansonsten regelmäßig die Zugänglichkeit zu elektronischen Gesundheitsdaten übermäßig beschränkt würde. Hierzu sei nochmals auf die eingeschränkte Downloadmöglichkeit von elektronischen Gesundheitsdaten des Art. 73 Abs. 2 UAbs. 2 EHDS-VO hingewiesen. Schließlich könnte sich auch die Rechtsprechung des EuG[107] zum relativen Personenbezug (siehe oben) auf die Abgrenzung im Rahmen der Anwendung der EHDS-VO auswirken.

3. Konkretisierungen von TOMs durch DGA, EHDS-VO und GDNG

[103] EuG 26.4.2023 - T-557/20, ECLI:EU:T:2023:219 = ZD 2023, 399 mAnm Baumgartner.
[104] EuG 26.4.2023 - T-557/20, ECLI:EU:T:2023:219 = ZD 2023, 399, 404.
[105] EuG 26.4.2023 - T-557/20, ECLI:EU:T:2023:219 = ZD 2023, 399, 402 Rn. 97 und 403.
[106] EuG 26.4.2023 - T-557/20, ECLI:EU:T:2023:219 = ZD 2023, 399, 403 f.
[107] EuG 26.4.2023 - T-557/20, ECLI:EU:T:2023:219 = ZD 2023, 399.

Der DGA sieht im Bereich des Datenaltruismus ein von der Europäischen Kommission zu erlassendes Regelwerk in Art. 22 DGA vor, das entscheidend zur Konkretisierung von geeigneten TOMs beitragen und für mehr Rechtssicherheit bei Datentreuhändern in Form von datenaltruistischen Organisationen sorgen könnte. Dieses betrifft Fragen der technischen IT-Sicherheit sowie der bereitzustellenden Werkzeuge für die Einwilligung und den Widerruf sowie der zu erbringenden Informationsanforderungen. Durch die Ausarbeitung von geeigneten technischen Anforderungen und angemessenen Informationsanforderungen könnte die Kommission einen entscheidenden Beitrag zur Erhöhung der Rechtssicherheit bezüglich TOMs für die Tätigkeit anerkannter datenaltruistischer Organisationen leisten, sofern sie dem Regelwerk Bedeutung für die Erfüllung datenschutzrechtlicher Vorgaben zumisst. Bisher hat die Kommission jedoch noch kein Regelwerk erlassen. Als weitere Schutzvorkehrung sieht Erwgr. 46 S. 6 DGA die Möglichkeit vor, dass anerkannte datenaltruistische Organisationen eine sichere Verarbeitungsumgebung[108] für die Verarbeitung von einschlägigen Daten bereitstellen, was im Regelwerk Berücksichtigung finden könnte.

Datenschutz-relevante Anhaltspunkte zur Konkretisierung von TOMs könnte auch die EHDS-VO beitragen. In Betracht kommen hier insbesondere die Vorgaben zur sicheren Verarbeitungsumgebung. Der Gesundheitsdatenzugang für die Sekundärnutzung soll im europäischen Gesundheitsdatenraum durch die nationalen Zugangsstellen, die als Datentreuhänder agieren könnten, über eine sichere Verarbeitungsumgebung gewährt werden, die organisatorischen und technischen Maßnahmen, sowie Interoperabilitäts- und Sicherheitsanforderungen unterliegt (Art. 73 Abs. 1 S. 1 EHDS-VO). Die von der sicheren Verarbeitungsumgebung zu erfüllenden Sicherheitsmaßnahmen werden in Art. 73 Abs. 1 S. 2 EHDS-VO in einer nicht abschließenden Liste näher bestimmt. Dazu zählt etwa die Minimierung des Risikos unbefugten Kopierens, Änderns, Lesens oder Entfernens von in der sicheren Verarbeitungsumgebung gehosteten Gesundheitsdaten „durch dem Stand der Technik entsprechende technische und organisatorische Maßnahmen“ (lit. b). Gesundheitsdatennutzer dürfen ferner nur „mittels einer persönlichen und eindeutigen Nutzerkennung und vertraulicher Zugriffsverfahren (…) ausschließlich auf die von ihrer Datengenehmigung erfassten Daten zugreifen“ (lit. d). Ferner sollen Gesundheitsdatennutzer nicht in der Lage sein, personenbezogene Gesundheitsdaten aus der sicheren Verarbeitungsumgebung herunterzuladen (Abs. 2 UAbs. 2). Die Durchführung regelmäßiger Audits der sicheren Verarbeitungsumgebung und das Ergreifen von Abhilfemaßnahmen bei festgestellten Risiken, Mängeln oder Schwachstellen ist ebenfalls vorgesehen (Abs. 3). Darüber hinaus wird die Kommission unter anderem ermächtigt, die technischen und organisatorischen Anforderungen und die Datenschutzanforderungen der sicheren Verarbeitungsumgebung mittels Durchführungsrechtsakten festzulegen (Abs. 5). Aufgrund des eher vage gehaltenen Normtextes, liegt es somit in der Hand der Kommission datenschutzrechtlich relevante Standardisierungen für den Gesundheitsdatenzugang durch die sichere Verarbeitungsumgebung vorzunehmen und die Tätigkeit von Zugangsstellen als Datentreuhänder rechtssicherer zu gestalten. Dies hat auch Auswirkungen auf anerkannte datenaltruistische Organisationen, die personenbezogene Gesundheitsdaten „unter Verwendung einer sicheren Verarbeitungsumgebung verarbeiten“ (Abs. 4). Hierbei soll die genutzte sichere Verarbeitungsumgebung auch die in Art. 73 Abs. 1 S. 2 lit. a bis f EHDS-VO festgelegten Sicherheitsmaßnahmen erfüllen.[109] Dies gilt gemäß Erwgr. 78 S. 2 f. EHDS-VO

[108] Definiert in Art. 2 Nr. 20 DGA.

[109] Beachte auch Erwgr. 78 S. 4 und Art. 57 Abs. 2 lit. c EHDS-VO, hierin werden die in der Datenstrategie der EU angelegten Bestrebungen deutlich, die digitale Zukunft Europas möglichst einheitlich und interoperable zu regulieren (COM(2020) 66 final, S. 14 ff., 20).

auch für die gegebenenfalls im Regelwerk nach Art. 22 DGA vorgesehenen Nutzung einer sicheren Verarbeitungsumgebung im Gesundheitswesen.

Das GDNG soll das deutsche Gesundheitswesen in ersten Schritten auf die Anbindung an den EHDS vorbereiten.[110] Zur Konkretisierung von TOMs sind hier insbesondere die Vorgaben zur Verknüpfung von pseudonymisierten Daten des FDZ Gesundheit und der klinischen Krebsregister der Länder nach § 4 GDNG interessant. Vorgesehen ist gemäß § 4 Abs. 5 S. 1 GDNG, dass nach Erteilung der Genehmigung zur Verknüpfung und Verarbeitung dieser Daten für Forschungsvorhaben durch die Datenzugangs- und Koordinierungsstelle, die als Datentreuhänder in Betracht kommt, die Daten „mit einer von der Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten für den jeweiligen Antrag festzulegenden sicheren Verarbeitungsumgebung einer öffentlich-rechtlichen Stelle verknüpft und den Antragstellenden als pseudonymisierte Einzeldatensätze, ohne Sichtbarmachung von Pseudonymen, verfügbar gemacht“ werden. In dieser sicheren Verarbeitungsumgebung muss gemäß Satz 2 „durch geeignete technische und organisatorische Maßnahmen sichergestellt sein, dass die Verarbeitung durch die Antragstellenden auf das für den jeweiligen Nutzungszweck erforderliche Maß beschränkt ist und insbesondere ein Kopieren der Daten verhindert werden kann“. Näheres zu den Anforderungen an die sichere Verarbeitungsumgebungen sowie den Kriterien für die Auswahl dieser durch die Datenzugangs- und Koordinierungsstelle obliegt gem. § 4 Abs. 9 S. 1 Nr. 2 dem BMG durch Rechtsverordnung mit Zustimmung des Bundesrates und im Benehmen mit der BfDI und dem BSI (§ 4 Abs. 9 S. 2 GDNG).

Die Relevanz der Nutzung von sicheren Verarbeitungsumgebungen bei der Datenbereitstellung wird anhand der genannten Europäischen und deutschen Vorgaben zu Akteuren, die als Datentreuhänder agieren könnten, deutlich und sollte beim Einsatz von Datentreuhändern in der Netzwerkmedizin berücksichtigt werden.

4. Grundsatz der Verhältnismäßigkeit

Die Anforderungen an Rechtsanwender im Bereich der Bestimmung von TOMs sind weit gefasst und können bei der Auslegung in der Praxis zu Rechtsunsicherheit führen. Hinzukommt, dass Konkretisierungsmöglichkeiten in Form von Zertifizierungen und Verhaltensregeln, die durch den europäischen Gesetzgeber in der DSGVO selbst vorgesehen sind, bislang nur unzureichend genutzt werden. Eine möglicherweise datenschutz-relevante, kontextbezogene Konkretisierung im Bereich der Sekundärnutzung von Gesundheitsdaten durch die Kommission mittels Durchführungsrechtsakte oder durch Rechtsverordnung im Sinne des GDNG auf nationaler Ebene steht noch aus. Abgesehen davon könnte die Rechtsunsicherheit zumindest insoweit minimiert werden, als dass der Rechtsanwender sich bei der Auslegung dem Grundsatz der Verhältnismäßigkeit bzw. der Risikominimierung im Einzelfall verschreibt. Bevor mit der Verarbeitung begonnen wird, muss dabei genau geprüft werden, ob alle Maßnahmen zur Eindämmung des Risikos, die dem Verantwortlichen nach dem Grundsatz der Verhältnismäßigkeit möglich sind, unternommen wurden.[111] Die Eliminierung aller Risiken ist dabei weder möglich noch zwingende Voraussetzung.[112]

Datentreuhänder in der Netzwerkmedizin müssten also im Hinblick auf die im Rahmen ihrer Tätigkeit erfolgende Verarbeitung personenbezogener Daten zur Erfüllung ihrer datenschutzrechtlichen Pflichten einen verhältnismäßigen Interessensausgleich herstellen. Dies steht im Zusammenhang mit der Rollenverteilung nach der DSGVO. Der für die Datenverarbeitung Verantwortliche, der gem. Art. 4 Nr. 7 DSGVO über die Zwecke und Mittel

[110] Vgl. GDNG-Kabinettentwurf, BT-Drs. 20/9046, S. 2.
[111] DSK, Kurzpapier Nr. 18, Stand: 26.04.2018, S. 6.
[112] Vgl. ibid.

der Verarbeitung entscheidet, hat eine umfassende Verhältnismäßigkeitsprüfung vorzunehmen, in deren Rahmen er abwägungsrelevante Grundrechte und Interessen einzubeziehen hat. Betroffene Personen haben beispielsweise ein Interesse an einer unkomplizierten und effektiven Ausübung ihrer Betroffenenrechte (erleichtert durch einen hohen Grad an Transparenz und Informiertheit). Weitere involvierte Akteure, wie zum Beispiel Datengeber oder -nutzer, haben ein Interesse daran, ihren Compliance-Aufwand und die Kosten zur Umsetzung eines datenschutzkonformen Projektes sowie ihr datenschutzrechtliches Haftungsrisiko möglichst gering zu halten. Interessen der Allgemeinheit betreffen zum Beispiel die Verbesserung der Gesundheitsversorgung und die Unterstützung der wissenschaftlichen Forschung.[113] Anhand des Ergebnisses der Verhältnismäßigkeitsprüfung im Einzelfall muss der Datentreuhänder sodann über das „Ob" und „Wie" der Datenverarbeitung entscheiden. Sind an der Datenverarbeitung neben dem Datentreuhänder weitere Akteure aus der Netzwerkmedizin beteiligt ist eine zutreffende Rollenverteilung auch für die Verhältnismäßigkeitsprüfung relevant. Ist etwa eine gemeinsame Verantwortlichkeit zu verneinen, hat der Datentreuhänder als alleiniger Verantwortlicher unabhängig von weiteren Verantwortlichen die Verhältnismäßigkeitsprüfung durchzuführen. Die konkreten legislativen Vorgaben der EHDS-VO zur datenschutzrechtlichen Verantwortlichkeit im Bereich der Sekundärnutzung (Art. 74 Abs. 1 EHDS-VO und Art. 75 Abs. 9 S. 2 und Abs. 10 EHDS-VO) dürften Orientierung für Datentreuhänder in der Netzwerkmedizin im Anwendungsbereich des EHDS bieten und so für mehr Rechtssicherheit bei der Rollenverteilung sorgen.

III. Geeignete TOMs für die Krebsforschung in DNA-Med

Vor der Bestimmung geeigneter TOMs muss zunächst der Verarbeitungszweck und eine Rechtsgrundlage gefunden werden. Dafür wurden zunächst der Verarbeitungskontext in DNA-Med, die relevanten Datenkategorien sowie Zweck und Rechtsgrundlage der Verarbeitung untersucht (1.). Die Festlegung geeigneter TOMs setzt die Bestimmung des Risikos der Verarbeitung voraus (2.). Danach wird eine Kategorisierung von TOMs anhand von Gewährleistungszielen und bezogen auf Risikoindikatoren aufgestellt, die die Wahl geeigneter TOMs erleichtern soll (3.). Außerdem ist der weitere Maßstab (4.), namentlich der Stand der Technik und Implementierungskosten, sowie die Überprüfung, Bewertung und Aktualisierung von TOMs (5.) zu beachten.

F. Projektbezogene Vorträge und Austausch

Es wurden verschiedene Vorträge zum TrustDNA Projekt gehalten, um die Sichtbarkeit des Projekts zu erhöhen und um fachintern sowie interdisziplinär von neuen Impulsen zum Thema Datentreuhand zu profitieren.

Im November 2022 nahmen wir am *Vernetzungstreffen der BMBF-Datentreuhandmodell-Projekte (Teilvorhaben „Recht")* teil und stellten im Rahmen der Vorstellung unseres Projektes erste Ergebnisse unserer Untersuchungen vor. Dies betraf zum einen die Einwilligungsthematik (Vortragstitel: „*Einwilligungsmanagement für die Verarbeitung hochsensibler Gesundheitsdaten – Datenschutzrechtliche Herausforderungen für die TrustDNA*"). Ferner wurden erste Ergebnisse unserer rechtsvergleichenden Untersuchung zum „Data Trust" im Vereinigten Königreich (Vortragstitel: „*Data trusts unter Trust und Charity Law – Kriterien für die Vertrauenswürdigkeit eines Datenintermediärs aus rechtsvergleichender Perspektive*") präsentiert. Der Vorstellung der einzelnen Projekte folgte

[113] Siehe etwa Erwgr. 45 S. 1 bis 3 DGA zu Zielen von allgemeinem Interesse.

eine anregende Austauschrunde zu diversen rechtlichen Fragestellungen, auch im Bereich des Datenschutzrechts (zum Beispiel Legitimation von Verarbeitungsschritten nach Art. 6 DSGVO unter anderem mit Blick auf die Einwilligung, insbesondere „broad consent“). Insgesamt empfanden wir die Beteiligung am Vernetzungstreffen als sehr gewinnbringend für unsere Projektarbeit. Während des Treffens wurde angeregt auch weiterhin im Austausch zu rechtlichen Fragestellungen zur Datentreuhand zu bleiben und dafür eine Mailingliste zu erstellen, was im Nachgang zum Treffen von einem Mitarbeiter des FIZ Karlsruhe umgesetzt wurde. Ferner wurde ein gemeinsames Dokument zum Austausch über relevante rechtliche Fragestellungen und zum Teilen relevanter Fachartikel oder anderer Literatur eingerichtet. Die Möglichkeit für einen projektübergreifenden Austausch begrüßen wir sehr und haben deshalb das Angebot, an der Mailingliste teilzunehmen, gerne wahrgenommen.

Im Februar 2023 wurde ein Vortrag im Rahmen des internen Forschungskolloqiums der Arbeitsgruppe von Professorin Molnár-Gábor mit dem Titel „*Vertrauenswürdigkeit von Datentreuhändern – Untersuchung von abstrakten und konkreten Kriterien von Vertrauen de lege lata und de lege ferenda*“ gehalten sowie im gleichen Monat ein Vortrag im Rahmen der interdisziplinären BioQuant Seminarreihe der Universität Heidelberg auf Englisch mit dem Vortragstitel „*Data trustees as a tool to enhance data sharing – a legal perspective*”. Im April 2023 wurden die Ergebnisse der Forschung zum „*Zusammenhang zwischen Aufgaben und Rollen einer Datentreuhand“* im Rahmen des internen Jour Fixe der Arbeitsgruppe von Professorin Molnár-Gábor präsentiert. Das TrustDNA Vorhaben wurde ferner in einem Vortrag während des internen Retreats im Juni 2023 vorgestellt wobei insbesondere auf erforschte „*Anknüpfungspunkte für einen Code of Conduct und datenschutzrechtliche Herausforderungen bei internationalen Datentransfers“* eingegangen wurde, was für die Untersuchung der datenschutzrechtlichen Grundlagen relevant war. Beim internen Jour Fixe der Arbeitsgruppe im Oktober 2023 wurde ein Vortrag „*Zur Auslegung datenschutzrechtlicher Unberührtheitsklauseln*“ gehalten, ein Thema das ebenfalls im Zusammenhang mit der Erforschung der datenschutzrechtlichen Grundlagen relevant war. Außerdem wurden die Zwischenergebnisse des Rechtsvergleichs mit dem Vereinigten Königreich während des internen Forschungskolloquiums der Arbeitsgruppe im November 2023 präsentiert (Vortragstitel: „*Eine rechtsvergleichende Perspektve zu Datentreuhändern mit UK*“). Außerdem nahmen wir am Vernetzungstreffen der geförderten BMBF-Datentreuhandmodell-Projekte im November 2022 sowie im September 2023 und 2024

Schließlich wurde im Oktober 2024 im Rahmen des internen Retreats der Arbeitsgruppe von Professorin Molnár-Gábor ein Vortrag zur „*Grenzüberschreitenden Sekundärnutzung von Gesundheitsdaten – Organisation von Internationalen Datentransfers durch die EHDS-VO*“ gehalten, das relevant für die datenschutzrechtlichen Grundlagen war.

Die Durchführung des Projektes basierte auf einem regelmäßigen Austausch aller am Projekt beteiligten Mitarbeiter:innen und aller Projektleiter:innen. Die Honorarkräfte konnten regelmäßig konsultiert und zu Projektmeetings eingeladen werden.

Im rechtswissenschaftlichen Teilprojekt gab es einen regelmäßigen Austausch zur Bearbeitung von AP2 und AP3. Sowohl die datenschutzrechtlichen Grundlagen, das Thema der dynamischen Einwilligung/Alteinwilligung/Neueinwilligung als auch technische und organisatorischen Maßnahmen beinhalteten diverse zu erforschende Aspekte der Anforderungen an zukünftige Datentreuhänder in der Netzwerkmedizin. Dementsprechend vielfältig und umfangreich waren auch die Besprechungen. Unsere Honorarkräfte waren dabei regelmäßig zu den jeweiligen Themen (Rechtsvergleich, dynamisches Einwilligungskonzept und TOMs) in den Austausch eingebunden. Weitere Besprechungen betrafen insbesondere

die Vor- und Nachbesprechung der zahlreichen Vorträge, die Beantwortung der online durchgeführten Umfragen und Bearbeitung unseres Projektframes im Miroboard der Begleitforschung sowie einer Umfrage des Fraunhofer-Instituts für Software- und Systemtechnik ISST über das Design und die technische Umsetzung von Datentreuhändern.

G. Publikationen

Gummersbach/Nestor/Molnár-Gábor, Dateninfrastrukturen für die Forschung mit Gesundheitsdaten, in: Buchheim/Möslein/Omlor (Hrsg.) Datentreuhand und Recht (2025) (im Erscheinen)

Miranda Mourby, Fruzsina Molnar-Gabor, Secondary Uses of Patients‘ Health Data in the Euorpean Health Data Space. A UK-German comparison, in: Edward Dove (ed), Confidentiality, Privacy, and Data Protection in Biomedicine, Routledge 2024.

Alexander Bernier, Fruzsina Molnár-Gábor, Bartha Maria Knoppers, The international data governance landscape, *Journal of Law and the Biosciences*, Volume 9, Issue 1, January-June 2022, lsac005, https://doi.org/10.1093/jlb/lsac005.

H. Schlussbemerkung und Ausblick

Die geleisteten Projektarbeiten waren notwendig und angemessen, um die dargelegten Ergebnisse zur Ausarbeitung eines geeigneten Datentreuhandmodells in der Netzwerkmedizin an der Schnittstelle zwischen Versorgung und Forschung zu erreichen. Die Untersuchungen der datenschutzrechtlichen Grundlagen sowie der technischen und organisatorischen Maßnahmen des Datenzugangs und der -nutzung für die datenschutzkonforme Weitergabe von Daten an verschiedene Forschungsakteure bieten Rechtssicherheit stärkende Lösungen für kooperative Formen der Gesundheitsdatenverarbeitung in der Netzwerkmedizin und tragen so zur Ermöglichung von Forschungsvorhaben bei dort, wo Rechtunsicherheit bei der Datenweitergabe in der Netzwerkmedizin bisher ein Hindernis darstellte. Dadurch wird ein Beitrag zur Verbesserung der Datenbereitstellung im medizinischen Forschungsbereich geleistet, um Daten einfacher nutzbar zu machen. Durch die Entwicklung eines dynamischen Einwilligungskonzeptes, Handreichungen und SOPs sowie der Ergebnisse unserer rechtsvergleichenden Analyse mit erfolgreichen Datentreuhandinitiativen im Vereinigten Königreich konnten Lösungen herausgearbeitet werden, um Patient:innen aktiv in das Forschungsdatenmanagement einzubinden und so ihren Einfluss zu stärken und ihre Position in der Netzwerkmedizin zu festigen. Dabei wurde insgesamt die internationale Anschlussfähigkeit unter Berücksichtigung relevanter legislativer Entwicklungen auf europäischer und nationaler Ebene einbezogen.

Die Ergebnisse des rechtswissenschaftlichen Teilvorhabens leisten einen Beitrag zur Erforschung, Konzeptionalisierung und Umsetzung von Datentreuhandmodellen, der über den Einsatz in der Netzwerkmedizin hinaus für die Entwicklung von Standards für Datentreuhänder, insbesondere zur Ermöglichung kooperativer Formen der Datenverarbeitung sensibler Daten in Forschungskontexten, Verwendung finden kann. Dazu tragen auch die Veröffentlichungen, zur Vertrauenswürdigkeit von Datentreuhändern sowie zu ihrer Bedeutung und den Einsatz von Datentreuhändern im Zusammenhang mit Dateninfrastrukturen mit Blick auf datenschutzrechtliche Fragestellungen, bei.

Konkret können etwa die untersuchten Bedingungen einer Zurverfügungstellung der Daten hinsichtlich der Rechtsgrundlagen sowie zu technischen und organisatorischen Maßnahmen für die in Zukunft vorgesehene weitere Arbeit von GHGA an sicheren

Verarbeitungsumgebungen („Trusted Research Environments“) Anknüpfungsmöglichkeiten bieten, um den Datenschutz weiter zu verbessern.