Mai 2022

Datentreuhandmodelle: Qualitätsanforderungen – Ermöglichungsbedingungen – Haftungsfragen

Fachgespräch der AG Datentreuhänderschaft am 3. März 2022 (Online-Veranstaltung)

Zusammenfassender Bericht

Der Diskurs rund um den Aufbau und die Gestaltung von Datentreuhändern ist durch Offenheit und Heterogenität hinsichtlich der diskutierten Ansätze geprägt. Die mit dem Konzept der Datentreuhänderschaft verbundenen Potenziale sollen weiterhin, wie unter anderem der Koalitionsvertrag der Ampelkoalition vorsieht, erschlossen und geprüft werden.[1] Gleichzeitig werden seitens der EU vor allem durch den Data Governance Act (DGA) und den angestrebten Data Act rechtliche Rahmenbedingungen geschaffen, die auf Entstehungsmöglichkeiten von Datentreuhändern einwirken. Zudem schreiten die Vorbereitungen im Aufbau der sektorenspezifischen European Data Spaces weiter voran. Fraglich ist, inwieweit hieraus eine Dynamik erwachsen kann, die dazu beiträgt, dass sich Datentreuhänder etablieren und auch genutzt werden. Zur Ausgestaltung und Umsetzung von Datentreuhandstrukturen in Deutschland bestehen Umsetzungsvorschläge beispielsweise für den Anwendungsbereich Gesundheits- und Mobilitätsdaten. Dabei wird deutlich, dass erhebliche Rechtsunsicherheiten bestehen und die Zielvorstellungen weiterhin zu diskutieren sind.[2]

Die AG Datentreuhänderschaft des RfII sieht vor diesem Hintergrund drei wesentliche Aspekte als entscheidend an, um nachhaltig Infrastrukturen zur Verbesserung des sektorenübergreifenden Datenteilens zu schaffen: Welche Qualitätskriterien sind an Datentreuhänder als auch an die bereitgestellten Daten zu stellen? Welche Ermöglichungsfaktoren sind entscheidend, damit Datentreuhandstrukturen überhaupt aufgebaut und auch genutzt werden? Sind Versicherungslösungen geeignet, um im Kontext der Datentreuhänderschaft entstehende Risiken auszugleichen, das Vertrauen in diese Infrastrukturen zu stärken und damit deren Entstehung zu befördern?

Hierzu hat der RfII am 3. März 2022 in einem zweiten Fachgespräch seiner Arbeitsgruppe „Datentreuhänderschaft“ mit ausgewählten Sachverständigen vertieft diskutiert. Marit Hansen und Petra Gehring führten gemeinsam in die Veranstaltung ein und legten die Sichtweise des RfII dar, der mit diesem Themenfeld einen über die Wissenschaft hinausgehenden, erweiterten Blick eingenommen hat. Einleitend wurde auf das Begriffsverständnis des RfII hingewiesen,

[1] Koalitionsvertrag 2021 – 2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), BÜNDNIS 90 / DIE GRÜNEN und den Freien Demokraten (FDP), S. 17.
[2] Louisa Specht-Riemenschneider/Wolfgang Kerber (2022): Designing Data Trustees – A Purpose-Based Approach.

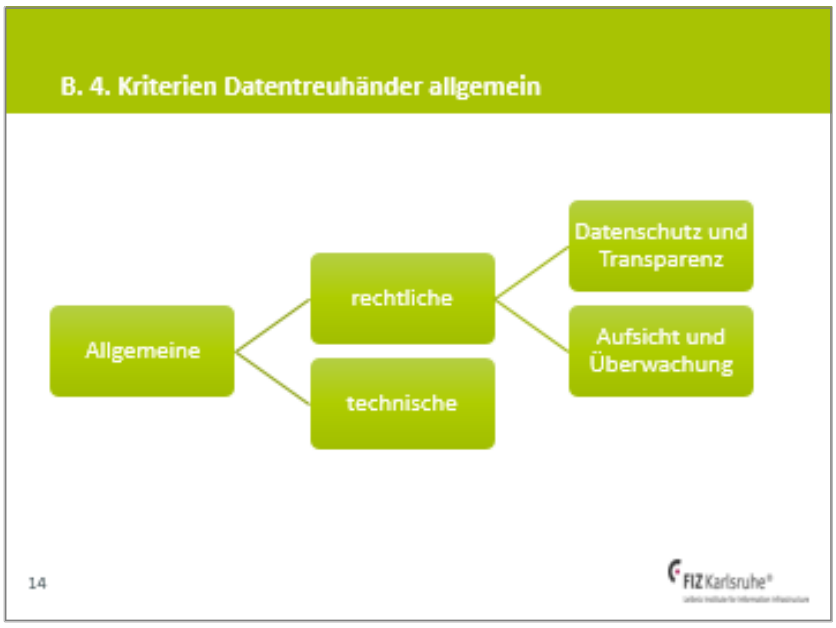
demzufolge Datentreuhänder als neutrale Stellen verstanden werden, die Interessen von Datengebern und Datennutzern in einen Ausgleich bringen und durch die Etablierung von Schnittstellen sektorenübergreifendes Datenteilen erleichtern können.

Die drei folgenden Sessions zu Qualitätskriterien, Ermöglichungsfaktoren und Versicherungslösungen wurden von der RfII-Vorsitzenden Petra Gehring, der Leiterin der AG Datentreuhänderschaft Marit Hansen sowie dem RfII-Mitglied Dietrich Nelle moderiert.

SESSION I – QUALITÄTSKRITERIEN

Die erste Session, moderiert von **Petra Gehring**, griff den Aspekt der Qualitätskriterien auf, die an Datentreuhänder als auch an die bereitgestellten Daten selbst angelegt werden sollten.

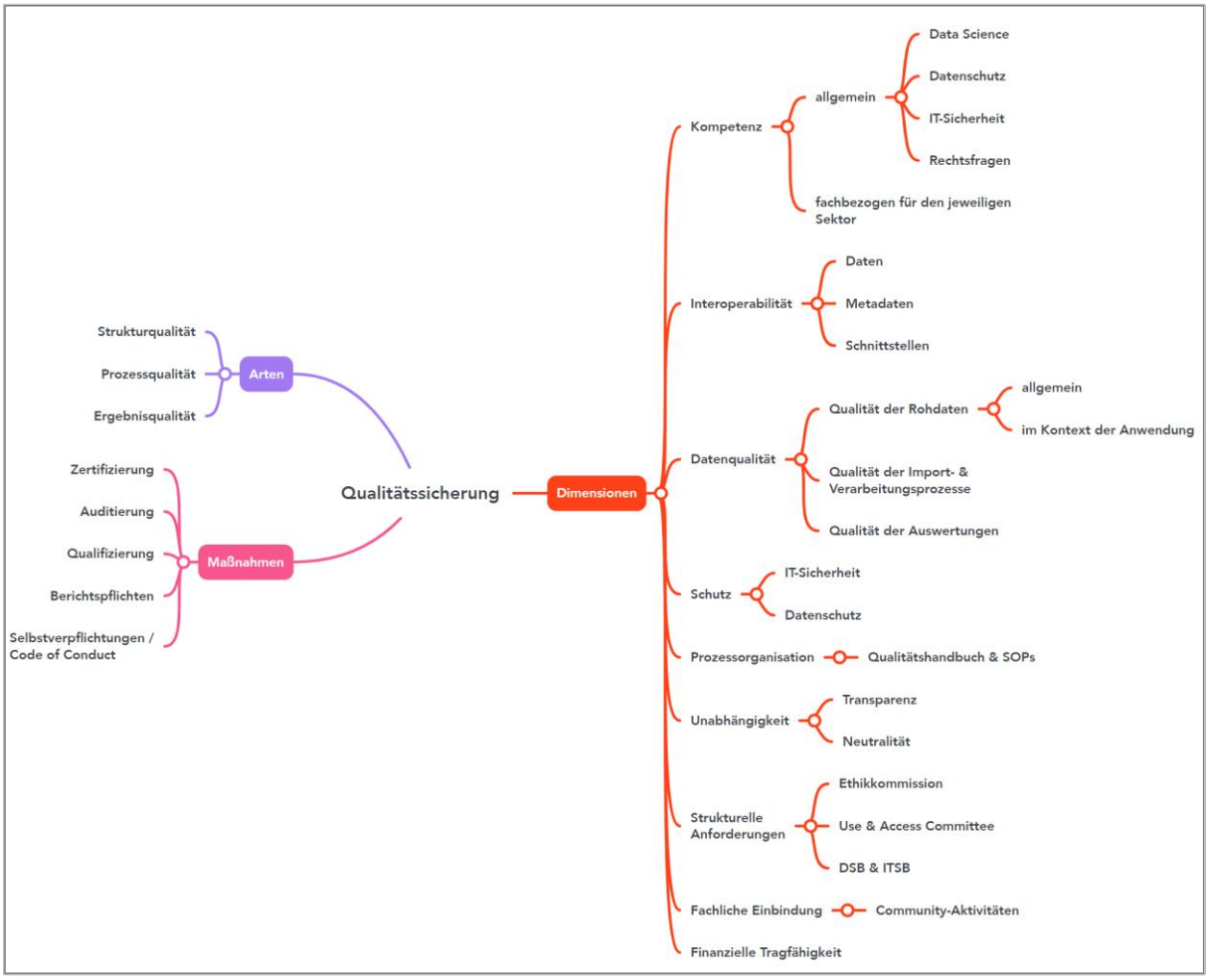
Eingangs problematisierte **Franziska Boehm**, FIZ Karlsruhe/ KIT Karlsruhe, dass Qualitätskriterien in den EU-Rechtsetzungsvorhaben (v.a. in Bezug auf den Data Governance Act) sehr allgemein gefasst sind. Sie sprach die Gefahr an, dass Rechtsfragen auf die spätere Rechtsprechung verlagert werden. Dagegen brauche es umfassende Anstrengungen im Bereich der Qualitätssicherung. Dabei bestehe zwischen der Qualität des Datentreuhänders und der Daten auch eine Wechselwirkung. Qualitätskriterien in Bezug auf die Daten sollten über die FAIR-Kriterien hinausgehen und seien weiter auszudifferenzieren. So legte sie dar, dass Nachnutzungsmöglichkeiten technisch als auch rechtlich festgehalten werden sollten. Metadaten könnten Angaben über die Verarbeitungsmöglichkeiten und Verantwortlichkeiten sowie über die rechtliche Nachnutzung enthalten. Für Letzteres sei ein eigenes maschinenlesbares Vokabular notwendig. Für jeden Datensatz müsse ausführlich geprüft werden, welche Rechte und Interessen betroffen und welche technischen Anforderungen (z.B. BSI-Standards[3]) zu berücksichtigen seien.



[3] Bei den BSI-Standards handelt es sich um Empfehlungen und Maßnahmen zu Aspekten der Informationssicherheit, die das Bundesamt für Sicherheit in der Informationstechnik formuliert bzw. definiert hat; https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html (zuletzt abgerufen am 13.05.2022).

In Bezug auf den Datentreuhänder führte sie ausführlich rechtliche als auch technische Qualitätsaspekte aus. Es sei zu gewährleisten, dass ein Treuhänder Datenschutz- wie Transparenzanforderungen (u.a. Protokollierungspflichten) erfülle. Auf die Erarbeitung und Einhaltung von Standards müsse hingewirkt werden z.B. bei der Datensicherheit, den Verantwortlichkeiten bzw. der Haftung oder den Zugangsrechten. Boehm führte aus, dass die Qualitätsanforderungen am besten sektorspezifisch zu entwickeln seien. Hierbei sei auf Mindeststandards zu achten, die in Bezug auf das jeweilige Datentreuhändermodell einheitlich sein sollten. Europaweit einheitliche Standards und eine Art Labeling seien schließlich eine Voraussetzung dafür, dass sich Qualitätseigenschaften auch kommunizieren lassen.

Thomas Ganslandt, Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF), zeigte die verschiedenen Dimensionen des Qualitätsbegriffs im Kontext der Datentreuhänderschaft auf (siehe Folie unten). Dies umfasse unter anderem die finanzielle Tragfähigkeit und die fachliche Einbindung des Datentreuhänders, aber auch strukturelle Anforderungen. Beispielhaft nannte er die Bildung eines Ethikgremiums und Use & Access Committees sowie den Austausch mit der Fachcommunity, wodurch auch die Interessen der Datengeber berücksichtigt würden.



Einen Schwerpunkt legte er auf die Herausforderungen im Bereich Interoperabilität und Datenqualität, welche er am Beispiel der Medizininformatikinitiative (MII) aufzeigte. So seien zunächst Datenstrukturen und Schnittstellen abgestimmt worden. Dabei hätten die vier Konsortien der MII individuelle technische Umsetzungen entwickelt. Mit Blick auf den modularen Kerndatensatz habe man es mit ähnlichen Daten, aber unterschiedlichen Semantiken zu tun. In einem offenen Prozess, auch unter Einbindung der Community, seien Formate festgelegt worden, die auch international anschlussfähig sind. Er wies zudem auf kostenlose Standards für Gesundheitsdaten wie HL7 FHIR hin. Letzterer sei in der Forschung einsetzbar, international anschlussfähig und erleichtere den Datenaustausch. Im Hinblick auf den Aspekt Datenqualität führte er aus, dass in der Medizininformatikinitiative die Daten aus verschiedenen Quellsystemen stammten, sodass es zu Verzerrungen in den Daten kommen kann. Daher brauche es Extraktions- und Transformationsschritte in den Kerndatensatzformaten. Bislang werde dies innerhalb der Konsortien individuell gelöst, teilweise unter Anwendung von Community-Tools. Hinsichtlich der Durchführung von Audits zum Zwecke der Qualitätsprüfung von Datentreuhandstrukturen sei, wie er abschließend darlegte, ein Bezug zur Fachlichkeit und Kompetenzen im Bereich der Data Science sinnvoll.

Diskussion

In der folgenden Diskussion wurde die Grundsatzfrage aufgeworfen, welches Konstrukt an Datentreuhändern mit welchen Folgewirkungen geschaffen werden sollte – vor allem angesichts der Risiken, die aus Zugriffsmöglichkeiten auf große Datenbestände resultieren können. Dies ist mit der Frage verbunden, wie unerwünschten Machtkonzentrationen bereits durch die Gestaltung der Governance-Strukturen entgegengewirkt werden kann. Hinsichtlich der Gefahr des Machtmissbrauchs betonte Ganslandt, „dass wir in der Medizininformatikinitiative das Problem dadurch lösen, dass wir keine zentrale Datensammlung anlegen, sondern dezentrale Datenhaltungen auf der Ebene der Universitätskliniken nutzen. Datenauswertungen werden dann nach entsprechenden Freigaben der Standorte föderiert durchgeführt."

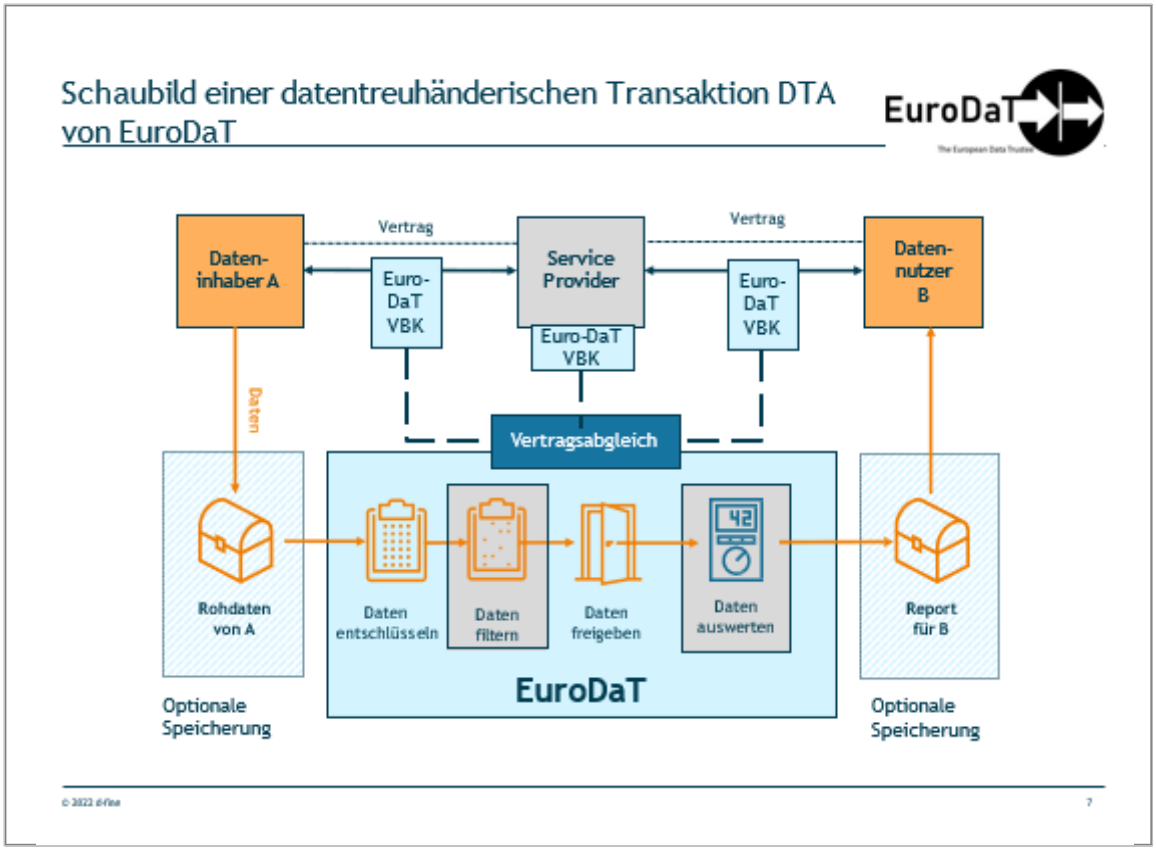
In Bezug auf die rechtlichen Rahmenbedingungen schätzten die Diskutantinnen und Diskutanten die derzeitige Rechtsgrundlage als nicht ausreichend ein. Der Data Governance Act der EU (DGA) wirke bislang eher einschränkend als anreizbildend. Ob durch den DGA Anreize für Datenintermediäre außerhalb des Rahmens staatlicher Förderung gegeben würden sei fraglich. Auch zeige sich, dass innerhalb der Datenwirtschaft Unsicherheiten bestehen, welche Folgen sich in der Praxis aus den Rechtsakten der Europäischen Union ergeben werden und welche Initiativen beziehungsweise welche bereits bestehenden Strukturen des Datenteilens sich auf rechtlich abgesichertem Boden befinden. Dies beträfe insbesondere den Datenschutz und die Nachnutzung von Daten. Rechtsunsicherheiten setzten sich in Unsicherheiten bei technischen Standards fort. Aufgegriffen wurde zudem der Bedarf, für Daten und Datensätze Metadaten zu rechtlichen Möglichkeiten und Restriktionen ihrer Nutzung, Verwertung und Vermarktung zu erstellen. Dabei argumentierte Boehm, dass es eine Art Creative Commons-Lösung für die Datennutzung brauche, auf deren Grundlage Klarheit über die jeweiligen Nachnutzungsrechte geschaffen werden kann.

Deutlich wurden auch die Potenziale, Tools für die Datenauswertung oder auch Governance-Prozesse der Medizininformatikinitiative in anderen wissenschaftlichen Fachbereichen zu nutzen. Am Ende der ersten Session wurde der Bedarf artikuliert, angesichts der sich stellenden Rechts- und Umsetzungsfragen zu einem sektorenübergreifenden Austausch zusammenzukommen. Dies betreffe einerseits die offene Frage, was rechtlich geregelt werden solle und was nicht. Langwierige Aushandlungsprozesse würden oft von der technischen Entwicklung und der Marktdynamik überholt. Auch erschien es sinnvoll, sich sektorenübergreifend über generische Aspekte von Datentreuhänderschaft zu verständigen, wie zum Beispiel ob eine Zertifizierung erfolgen soll, wer entsprechende Kriterien erarbeitet und wer darauf aufbauend eine solche Zertifizierung durchführt.

Session II – Ermöglichungsfaktoren

Die zweite Session, die von Marit Hansen moderiert wurde, beleuchtete den Aspekt, welche Faktoren den Aufbau und die Nutzung von Datentreuhändern ermöglichen können.

Egbert Schark von d-fine verdeutlichte, wie aktuell bestehende Gestaltungsspielräume im Bereich des Datenteilens durch pragmatische Herangehensweisen genutzt werden können. Es sei wichtig, „Experimentierräume zu schaffen und zu lernen, was funktioniert und wo die Herausforderungen liegen." Er präsentierte das Modell eines transaktionsbasierten Datentreuhänders, der dem Schutzbedarf der Daten und damit auch der Datengebenden gerecht werde. Essentiell wichtig sei es, den notwendigen Vertrauensaufbau von Datengebern und Datennutzern in die Treuhand zu befördern. Gleichzeitig könne man der Gefahr von Machtkonzentrationen vorbeugen, die durch das Poolen von Daten an einer Stelle entstehen kann. Der wirtschaftliche Wert von Einzeldaten sei häufig gering. In der Regel entstehe ein quantifizierbarer Wert von Daten erst durch deren Zusammenführung in großer Menge. Dieser Wert lasse sich im Vorhinein – also vor Zusammenführung und Analyse – nicht hinreichend definieren, da die Wertschöpfung in genau diesem Prozess läge. Damit ließe sich auch die Schutzbedürftigkeit der Daten vorab nicht genau festlegen. Da sich Datentreuhänder durch die Ansammlung von immer mehr Daten zu mächtigen Infrastrukturen herausbilden können, sollte es keinen unmittelbaren Transfer und keine nicht widerrufbare Freigabe von Daten geben. Vor diesem Hintergrund führe ein Datentreuhänder im transaktionsbasierten Ansatz einzelne Transaktionen durch, in denen jeweils die Datenfreigabe (auch auf Grundlage eines Vertragsabgleichs) geprüft werde. Dies veranschaulichte Schark am Beispiel des Projekts EuroDaT, eines geplanten Datentreuhänders für Finanzdaten.



Der Datennutzer erhalte ausschließlich die Datenauswertung, nicht aber die Daten selbst. Ebenso habe der Datentreuhänder keinen direkten bzw. exklusiven Zugriff auf die Daten, die beim Datengeber verbleiben oder auf die Datenanalyseergebnisse, die an den beauftragenden Datennutzer gehen. Somit seien Datengeber, Datennutzer und Datendienstleister voneinander entkoppelt.

Matthias Spielkamp, AlgorithmWatch, machte die zivilgesellschaftliche Perspektive auf den Datentreuhänder-Diskurs deutlich und gab einen Überblick über die von AlgorithmWatch durchgeführten Datenspendeprojekte. Diese zielten darauf, Funktionsweisen algorithmischer Systeme zu untersuchen. Spielkamp zeigte auf, dass diese Projekte vor allem über Browser Plug-Ins umgesetzt und Datenspender über Mainstreammedien angeworben werden. Es stellten sich Fragen der Nachnutzung und des Konzeptmanagements. So müssten Anreize geschaffen werden, damit die Datenspender in ihrer Spende auch einen Nutzen erkennen können – wobei dieser Nutzen nicht zwingend in einer monetären Kompensation bestehen müsse. Auch transparente Informationen über die Verwendung der Spende könnten die Funktion eines sinnstiftenden Anreizes für Datenaltruismus haben. Ausführlicher beleuchtete er das vom BMBF geförderte DataSkop-Projekt. Hier erhielten Datenspender Informationen dazu, was mit ihren Daten erforscht werden soll. Spielkamp betonte die rechtlichen Herausforderungen im Kontext der Datentreuhänderschaft. Regulierungsversuche wie z.B. der europäische Data Governance Act schafften bislang mehr bürokratische Hürden, als sie Anreize zur Datenspende eröffneten. Zugleich sei die Rechtsunsicherheit beim Aufbau von Datentreuhandstrukturen sehr hoch. Hierzu verwies er auf das Gutachten von Michael Funke zur „Vereinbarkeit von Data Trusts mit

der Datenschutzgrundverordnung“. Er plädierte dafür, im laufenden Diskurs über die Schaffung von Datentreuhändern darüber nachzudenken, „wie eine solche Datenweiternutzung auch für die Zivilgesellschaft funktionieren kann. So ist mitzudenken, dass es noch einen anderen Akteur gibt, der nicht staatlich, privat oder kommerziell unterwegs ist.“

Diskussion

Der Fokus der Diskussion lag zunächst auf der Frage, inwieweit ein pragmatischer Ansatz hinsichtlich des Aufbaus von Datentreuhandstrukturen angesichts des hohen Kontrollaufwands umgesetzt werden kann. Egbert Schark wies darauf hin, dass auch hier diskutiert werden müsse, ob ein Datentreuhänder anzustreben sei, der alles selbt prüfe. Denkbar sei gegebenenfalls, dass beispielsweise die Prüfung der Analysealgorithmen durch Dritte erfolge. So könne ein Ökosystem geschaffen werden, in dem keine prinzipiellen Zusagen getroffen werden, dass der Datentreuhänder diese Aufgaben alleine übernehmen müsse. Dieser würde aber absichern, dass der Algorithmus gekapselt von den Daten laufe. Daraufhin wurde hinterfragt, inwieweit die gemeinsamen Verantwortlichkeiten – mitunter in Verträgen – festgelegt werden können. Anknüpfend an die Diskussion aus der ersten Session zur Übertragbarkeit/ Adaptionsfähigkeit von Best Practice-Beispielen unter anderem aus der Medizininformatikinitiative wurde die Frage nach Musterlösungen diskutiert. Beispielsweise könnten Ansätze und Erfahrungen aus dem Feld der Medizininformatikinitiative hinsichtlich des Umgangs mit personenbezogenen Daten in anderen Anwendungsfeldern fruchtbar sein. Eine Gelingensbedingung hinsichtlich des Aufbaus von Datentreuhändern stellten in jedem Falle Prozesse des wechselseitigen Lernens dar – gerade auch im Verhältnis der Rechtsgestaltung zum Aufbau tragfähiger Geschäftsmodelle (s.u.).

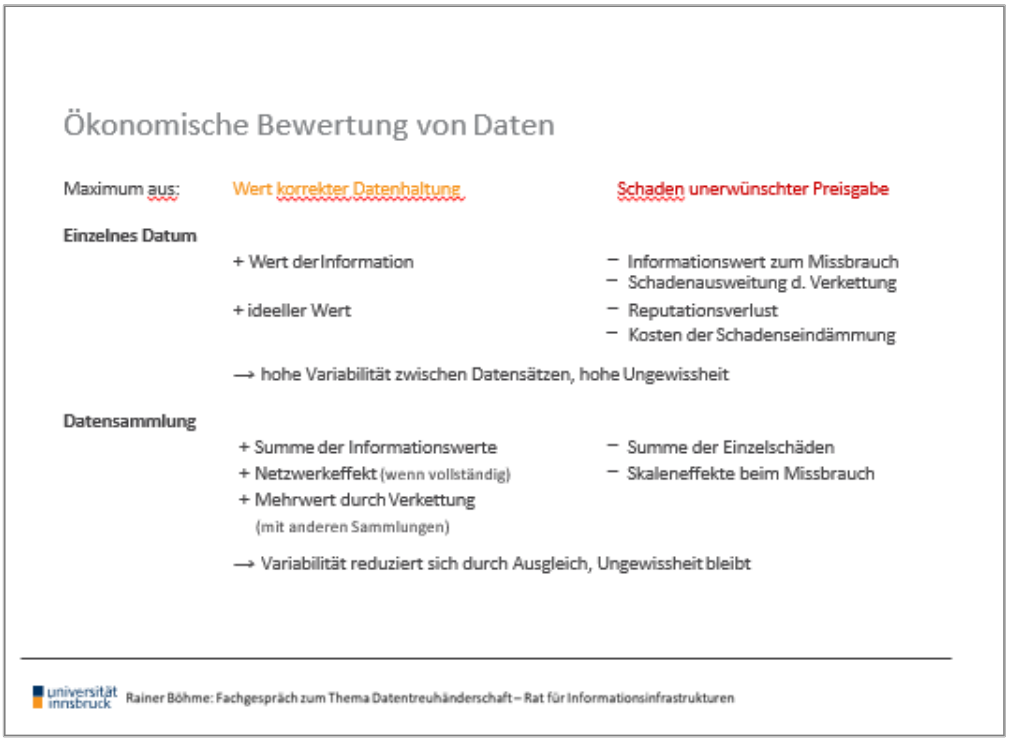
Ausgelotet wurden auch Ermöglichungsfaktoren im Zusammenhang mit Datenspenden und Einwilligungsverfahren. So wurde für eine breitere Anwendung des sogenannten *broad* oder *dynamic consent* plädiert, welcher in Deutschland noch kaum genutzt werde. Ein weiterer zentraler Aspekt der Diskussion lag auf dem Bedarf an Experimentierfeldern. Hier wurde die Rolle von Forschungsprojekten unterstrichen, um Datentreuhandstrukturen weiter zu erproben. Zum Abschluss wurde aufgeführt, dass Unsicherheiten bei den rechtlichen Rahmenbedingungen gerade auf Seiten kleinerer und mittlerer Initiativen und Unternehmen Herausforderungen hinsichtlich ungeklärter Risiken für potenzielle Geschäftsmodelle mit sich brächten. Allerdings könne mit dem Aufbau auch nicht erst gewartet werden, bis alle Rechtsfragen abschließend geklärt seien. So unterstrich Franziska Boehm, dass angesichts der Dynamik der digitalen Transformation „wir nicht erst den rechtlichen Rahmen schaffen können und dann erst mit den Daten arbeiten und Innovationen anstoßen. Deswegen sind Forschungsprojekte, insbesondere auch zu den rechtlichen Rahmenbedingungen so wichtig.“ Lineare Modelle funktionierten in einer digitalen Welt nicht mehr. Vielmehr komme dem Recht heute eine Ermöglichungsfunktion zu: man könne nicht erst abwarten, bis alles durchreguliert sei und dann erst Geschäftsmodelle darauf aufbauen. Auch stelle es eine Herausforderung dar, die verschiedenen Rechtsbereiche in digitalen Innovationsprozessen zusammenzuführen. Grundsätzlich sollte das Recht mit Blick auf die Etablierung von Datentreuhandstrukturen Offenheit im Sinne von

Spielraum für weitere technische Anschlussmöglichkeiten und wirtschaftliche Dynamiken erzeugen. Schark und Spielkamp betonten allerdings auch eindringlich, dass der Aufbau tragfähiger Geschäftsmodelle im Datentreuhandbereich auf verlässliche rechtliche Ausgangsgrundlagen nicht gänzlich verzichten könne. Das unternehmerische Risiko auch und gerade im Haftungsbereich sei ansonsten insbesondere für kleinere Start-ups so groß, dass ein diversifizierter Markt sich gar nicht erst entwickeln könne.

SESSION III – VERSICHERUNGSLÖSUNGEN

Die dritte Session, moderiert von **Dietrich Nelle**, legte den Schwerpunkt auf die Frage nach dem Potenzial von Versicherungslösungen hinsichtlich der Ermöglichung von Datentreuhändern.

Rainer Böhme, Universität Innsbruck, legte dar, wie sich Cyber-Versicherungen als neues Versicherungsprodukt seit den 1980er Jahren entwickelten und zog vor diesem Hintergrund Schlussfolgerungen für den Datentreuhänder-Kontext. Der Markt sei – und zwar entgegen früherer Prognosen – weiterhin klein. Es gebe im Bereich der Cyber-Versicherungen bis heute keine signifikante Prämiendifferenzierung. Dies führe dazu, dass es für Versicherte keine Anreize gebe, in präventive Sicherheitsmaßnahmen zu investieren.



Als zweiten Aspekt bezog er sich auf die ökonomische Bewertung von Daten und Datensammlungen, die einer Schadenskalkulation zu Grunde liegen. Ein Versicherer müsse maximal den konkreten Verlust der Daten sowie den Schaden, der durch unerwünschte Preisgabe entstanden ist, abdecken. Eine monetäre Bewertung falle aber selbst hier nicht leicht und müsse durch den Versicherungsnehmer hinreichend belegt werden können. Mit Blick auf die Entstehung von

Risikotransferansätzen beziehungsweise Versicherungslösungen im Kontext der Datentreuhänderschaft sei es wahrscheinlich, dass ein Versicherer zwar die Kosten der Schadenseindämmung übernehme, damit wäre aber nur ein kleiner Teil der potenziellen Schäden abgedeckt. Direkte Schäden nachzuweisen, sei sehr aufwändig und ließe sich – wie ein entstandener Vertrauens- und Reputationsverlust – nur schwer quantifizieren. Sollten sich nur wenige Datentreuhänder am Markt etablieren, ließen sich die antizipierten Kosten für eventuelle Kumulschäden[4] nicht hinreichend streuen. Dies hätte sehr hohe Versicherungsbeiträge zur Folge, die sich auf einen raschen Marktaufbau für Treuhänder voraussichtlich prohibitiv auswirken würden. Daher äußerte sich Böhme skeptisch, ob Versicherungslösungen als ein wirksamer Ermöglichungsfaktor mit Blick auf den Aufbau von Datentreuhandstrukturen begriffen werden könnten: „Es ist schon eine Mammutaufgabe, Datentreuhänder zu etablieren; dazu noch ein passendes Risikotransfergeschäft zu etablieren, kann ich mir kaum vorstellen."

Die Sichtweise der Versicherungswirtschaft hinsichtlich des Bedarfs an Versicherungslösungen und die damit verbundenen Herausforderungen zeigte Tibor S. Pataki vom Gesamtverband der Deutschen Versicherungswirtschaft (GDV) auf. Versicherungslösungen könnten dazu beitragen, das Vertrauen in den Datentreuhänder zu stärken. Aufgrund hoher Bußgelder im Datenschutzrecht und des Kumulrisikos würden auf Datentreuhänder potenziell hohe Haftungsrisiken zukommen. Das Risiko erhöhe sich unter anderem durch zivilrechtliche Instrumente der Musterfeststellungsklage. Die Herausforderungen im Aufbau derartiger Versicherungsangebote bestünden darin, dass es sich bei Datentreuhändern voraussichtlich um ein sehr kleines Risikokollektiv handele. Neue und unbekannte Risiken erschwerten die Kalkulierbarkeit des Schadensrisikos, das die Voraussetzung für die Entwicklung eines Versicherungsprodukts darstelle. So würden auch wenig Informationen zur Schadenswahrscheinlichkeit und in Bezug auf die Höhe des erwarteten Schadens vorliegen. Hilfreich wären klare rechtliche Rahmenbedingungen bezüglich der Aufgaben des Datentreuhänders. Auch müsste festgelegt werden, wofür der Datentreuhänder hafte und in welcher Höhe. Registrierungs- und Zertifizierungsmaßnahmen sowie eine behördliche Kontrolle könnten die Kalkulierbarkeit des Risikos erleichtern. Es dränge sich natürlich die Frage auf, ob eine staatlich vorgegebene Pflichtversicherung für die Etablierung eines Datentreuhändermarktes nicht die Lösung sei. Im Gespräch bewerteten Böhme als auch Pataki eine Pflichtversicherungslösung allerdings als kontraproduktiv. Großunternehmen würden eine solche Datenversicherung im Rahmen ihres Gesamtversicherungsumfangs pauschalisieren können. Für kleinere Datentreuhänder entstünde ein Wettbewerbsnachteil, da sie um an attraktive Versicherungsbedingungen zu gelangen einen über ihren eigentlichen Bedarf hinausgehenden Versicherungsschutz erwerben müssten. Sollte eine solche Versicherung dennoch zu günstigen Konditionen angeboten werden können, würde dies bei den Datentreuhändern eventuell Anreize für ein proaktives Risikomanagement verringern. Pataki äußerte sich

[4] Kumulschäden stellen sich klassischerweise bei Naturereignissen (Feuer, Überschwemmungen, Erdbeben etc.) ein, die zahlreiche schwer kalkulierbare Folgeschäden bei einer Vielzahl von Akteuren (Versicherten) nach sich ziehen. Der Verlust einer großen Zahl sensibler, sicherheitsrelevanter oder ökonomisch wertvoller Daten bei einem Treuhänder könnte sich ähnlich auswirken – das Kumulrisiko für den Versicherer ist entsprechend hoch einzuschätzen und wirkt sich entsprechend prämiensteigernd auf die Kostenstruktur der Versicherung aus.

dennoch vorsichtig optimistisch, dass sich Versicherungslösungen gegebenenfalls als Nischenprodukt der Versicherer entwickeln könnten. So könnte seiner Meinung nach ein Lösungsansatz darin bestehen, „dass Versicherungsverträge flexibel gestaltet werden und der Versicherungsschutz in einem kontinuierlichen Prozess weiterentwickelt und ausgeweitet werde."

Diskussion

In der Diskussion wurden nochmals die mit dem Konzept der Datentreuhänderschaft verbundenen Gefahren und Risiken angesprochen, die durch mögliche Datenverluste entstehen können. Dies betreffe nicht allein Datentreuhänderansätze, die auf einer zentralen Speicherung von Daten aufbauen, sondern auch dezentral angelegte Datentreuhänder, sofern sie auf große Datenmengen zugreifen. Intensiv wurden Potenziale von Versicherungslösungen und mögliche Ausgestaltungen diskutiert. Dabei tauchte einerseits die Frage nach der Rolle des Staates als möglicher Versicherer auf, da mit Datentreuhändern auch ein öffentliches Interesse verbunden sei. Sowohl Böhme als auch Pataki hoben die hiermit verbundenen Nachteile hervor, sollten entstandene Schadenskosten auf den Steuerzahler verteilt werden. Dies würde dem Ziel entgegenlaufen, Investitionen vor allem in eine proaktive Risikominimierung vorzunehmen und schaffe zusätzliche Bürokratie. Zudem sei es wichtig, Grundsätze der Datenminimierung bzw. der dezentralen Verteilung von Datenpools von vornherein mitzubedenken.

Langfristig ließen sich voraussichtlich durchaus Versicherungsprodukte entwickeln, die auf den Anwendungsbereich von Datentreuhändern zugeschnitten sind – auch wenn die Geschichte der Cyber-Versicherungen allgemein zeige, dass diese für die Versicherer bislang ebenfalls schwierige Geschäftsmodelle sind. Denkbar sei es, für den erstattungsfähigen Schaden des Datentreuhänders selbst auf etablierte Lösungen bei anderen Versicherungstypen zurückzugreifen, wie z.B. auf die Wertdeklaration des Versicherungsnehmers in der Hausratversicherung, in der der maximale Umfang des zu kompensierenden Schadens – und damit auch die Prämienhöhe – bestimmt wird. Eine zuverlässige Abwicklung von Schäden bei Dateninhabern oder Datennutzern sei damit allerdings nicht möglich. Hierfür müssten zusätzliche Lösungen – voraussichtlich jenseits von tradierten Versicherungsmustern – gefunden werden. Skepsis äußerte sich vor allem bezüglich der Frage, inwieweit Versicherungslösungen gegenwärtig den Aufbau von Datentreuhändern befördern könnten – auch hinsichtlich des Kostenfaktors für die Versicherten. Die Herausbildung von Versicherungsangeboten mit ausgeprägten Haftungsbegrenzungen wurde als wahrscheinlich eingeschätzt, um einerseits das Kumulrisiko für die Versicherer zu begrenzen und andererseits Angebote auch für kleine Unternehmen zu ermöglichen. In Anbetracht notwendiger europäischer Lösungen wies Pataki auf die Herausforderung hin, dass es in Bezug auf Schadensersatzansprüche bislang selbst im europäischen Binnenmarkt und erst recht im internationalen Vergleich große Unterschiede gebe.

Abschließend wurde diskutiert, inwieweit der Markt für Datenunternehmer hinreichend Anreize setze, sich auf ein solches Geschäftsfeld zu begeben, zumal der Datentreuhänder keine eigenen wirtschaftlichen Vorteile aus den Daten ziehen solle. Divergierende Haltungen bestanden in der Frage, inwieweit hier gezielte staatliche Anreize gesetzt werden sollten oder die Ent-

wicklung dem Markt zu überlassen sei. Konsens bestand in der Erwartung, dass Datentreuhänder effektiv zum Aufbau eines europäischen Datenökosystems beitragen könnten. Sie könnten eine „Marktlücke“ schließen, die Big Tech-Firmen und Hyperscaler erstens zurzeit ohnehin nicht bedienen würden und zweitens im Interesse einer Vertrauensbildung in alle Richtungen auch nicht regelhaft (mit-)erfüllen sollten.

ZUSAMMENFASSUNG

Marit Hansen legte in der Zusammenfassung den Schwerpunkt auf die Grundfrage, die sich beim Thema Datentreuhänderschaft stellt: Welche Ziele sollten mit dem Aufbau derartiger Infrastrukturen verfolgt werden und inwieweit sollte die Entwicklung aktiv mitgestaltet oder der Eigendynamik des Marktes überlassen werden. Hierzu brauche es einen sektorenübergreifenden Diskurs zu den Zielvorstellungen von Datentreuhandstrukturen. Anstrengungen sollten sich darauf richten, mithilfe von Datentreuhändern der Wissenschaft und Forschung einen verbesserten Zugang zu essenziellen Datenbeständen zu eröffnen. Zudem sei bei der Konstruktion von Datentreuhändern zu diskutieren, inwieweit auch der Datenzugang für zivilgesellschaftliche Akteure verbessert werden kann. Um bestehende Probleme der Datenökonomie zu lösen und das sektorenübergreifende Datenteilen zu erleichtern, stellten Datentreuhänder allerdings nur einen Lösungsansatz unter weiteren notwendigen Maßnahmen dar. Entscheidend sei dabei, wie Datentreuhänder reguliert, Anreize für deren Aufbau gesetzt und Räume des Experimentierens ermöglicht werden.

Zum Ende der Veranstaltung skizzierte Petra Gehring vier Aspekte, die sich aus den Impulsen und der Diskussion herauskondensierten: Angesichts der Komplexität des Themas stellten sich Überlegungen rund um Datentreuhänder als ein Experimentierfeld dar. Es müssten daher erstens in zunächst öffentlich geförderten Datentreuhand-Projekten Pfadentscheidungen getroffen werden, die zugleich auch die Möglichkeit des Scheiterns beinhalten sollten. Zweitens zeigten sich Herausforderungen gerade auch auf der rechtlichen Ebene. Dabei sei es hilfreich, das Recht nicht als Bremse, sondern primär als Gestaltungsinstrument zur Ermöglichung des Datenteilens zu verstehen und einzusetzen. Die Datentreuhänderansätze seien drittens zwar heterogen, sie folgten aber der Idee des föderierten Nutzbarmachens von Daten und Datensätzen. Und viertens zeigten sich – angesichts der in Deutschland immer noch wenigen konkreten Versuche in innovativer Weise Datentreuhänder auch wirklich nachfragegerecht aufzubauen – die Potenziale des gegenseitigen Austausches und wechselseitigen Lernens, um den Diskurs um Datentreuhänder voranzubringen.

Impressum

Rat für Informationsinfrastrukturen (RfII) - Geschäftsstelle
Papendiek 16, 37073 Göttingen
Fon 0551-392 70 50
E-Mail info@rfii.de
Web www.rfii.de