Februar 2021

Datentreuhänder: Potenziale, Erwartungen, Umsetzung

Workshop der AG Datentreuhänderschaft des RfII am 25. September 2020

Zusammenfassender Workshop-Bericht

In einer Stellungnahme DATENTREUHANDSTELLEN GESTALTEN – ZU ERFAHRUNGEN DER WISSENSCHAFT hat der Rat für Informationsinfrastrukturen (RfII) im April 2020 auf den aktuellen Diskurs um den Aufbau von Datentreuhändern reagiert. Der RfII interpretiert Datentreuhandstellen als Infrastrukturen neuen Typs. Ausgehend von Erfahrungen mit Konzepten des Datenteilens in der Wissenschaft werden in der Stellungnahme einige damit verbundene Potenziale, aber auch Diskussionsbedürfnisse herausgearbeitet. Diese betreffen unter anderem Anforderungen an die Wahrnehmung der Treuhänderschaft, den Aufgabenumfang sowie eine geeignete Qualitätssicherung.

Die Arbeitsgruppe Datentreuhänderschaft des RfII, die sich seit einem Jahr intensiv mit dem Thema beschäftigt, hat hieran anschließend einen Workshop ausgerichtet, mit dem Ziel, einen sektorenübergreifenden Austausch zu initiieren. Der Workshop wurde am 25. September 2020 als Videokonferenz abgehalten. Unter dem Titel „Datentreuhänder: Potenziale, Erwartungen, Umsetzung“ diskutierten 15 eingeladene Sachverständige mit RfII-Mitgliedern über Herausforderungen und Chancen, die mit dem Aufbau von Datentreuhändern verbunden sein können.

Dabei sollten auch sektorspezifische Herausforderungen des Datenteilens, insbesondere in Bezug auf Mobilitäts-, Medizin- und Unternehmensdaten in den Blick genommen werden, um sich aus unterschiedlichen Sichtweisen über den Bedarf an Datentreuhandlösungen und mögliche Ansätze einer Institutionalisierung auszutauschen.

In ihrer Einführung verwies **Marit Hansen**, Landesbeauftragte für Datenschutz Schleswig-Holstein und Leiterin der Arbeitsgruppe Datentreuhänderschaft, auf den dynamischen Diskurs rund um das Thema Datentreuhänder und den thematischen Fokus des Workshops, der inhaltlich in drei Sessions gegliedert war: Diskutiert wurde über Aufgaben eines Treuhänders, Zugangsmodelle und Fragen der Qualitätssicherung.

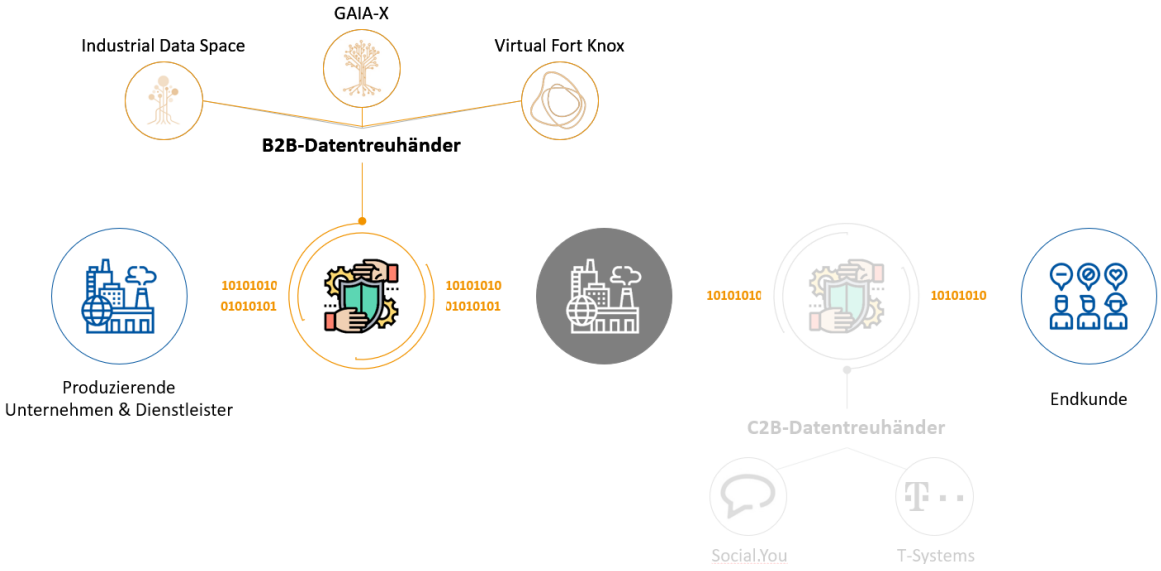
Moderiert wurden die Sessions von den AG-Mitgliedern **Marit Hansen**, **Petra Gehring** (TU Darmstadt und Vorsitzende des RfII) und **Dietrich Nelle** (BMBF). Zur besseren Illustration der Workshop-Diskussion wird in diesem Bericht auf einzelne vortragsunterstützende Folien von Teilnehmerinnen und Teilnehmern zurückgegriffen.

SESSION I - AUFGABEN EINES TREUHÄNDERS

Die erste Session drehte sich um Modelle von Datentreuhänderschaft und die Bedarfe, die sektorspezifisch durch neu geschaffene Datentreuhänder gedeckt werden könnten. Über alle Sektoren hinweg wurde deutlich, dass weitere Anstrengungen in den Aufbau eines Vertrauensprozesses notwendig sind, um das Datenteilen zwischen Datenerzeugern und -nutzern zu erhöhen. Datentreuhänder könnten, sofern sie gewisse Merkmale erfüllen, hierfür einen Beitrag leisten.

Dies beschrieb **Robert Schmitt**, RWTH Aachen, in seinem Vortrag „Datentreuhänder in der Produktion“ mit Blick auf mittelständische Unternehmen, die – wie er darlegte – die bei ihnen erzeugten Daten als Grundlage ihrer Wettbewerbsfähigkeit interpretieren. Insofern seien bei kleinen und mittleren Unternehmen (KMU) Sorgen über Datenschutz und den möglichen Kontrollverlust über die eigenen Daten verbreitet. Gleichzeitig erkenne man aber die Notwendigkeit des Datenaustauschs in den Wertschöpfungsketten, in die die Unternehmen im Zuge der Güterproduktion eingebunden sind.

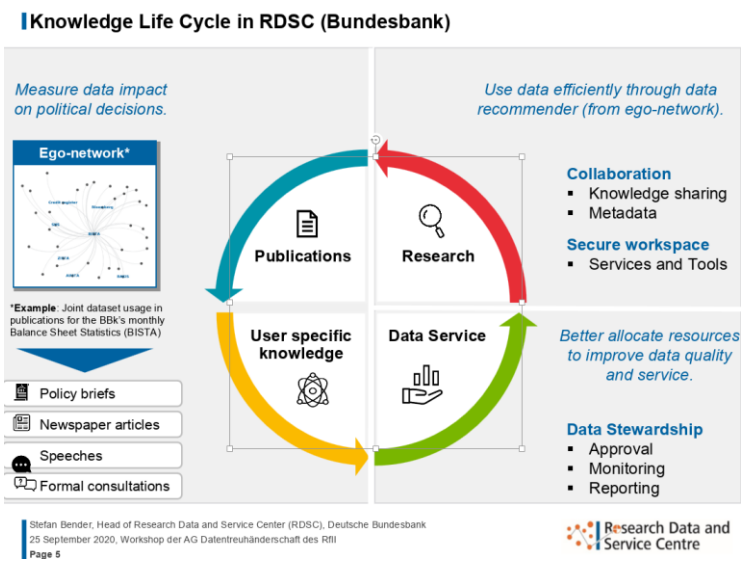
Eine Unterscheidung zwischen C2B- und B2B-Datentreuhändern erscheint sinnvoll



Schmitt plädierte für eine Unterscheidung zwischen Business-to-Business (B2B-) und Customer-to-Business (C2B)-Datentreuhändern. Im B2B-Bereich könnten Datentreuhänder zu einer Erhöhung der Wertschöpfung beitragen. Bislang habe nur ein äußerst geringer Anteil der KMU ihre Wertschöpfungsketten digital vernetzt, hierdurch könnten aber neue Formen der Kollaboration entstehen. Als zentrale Merkmale, die mit Blick auf den Aufbau von Datentreuhändern zu berücksichtigen seien, nannte er unter anderem die Frage der Governance, der Dezentralität, des Datenschutzes und der Skalierbarkeit.

Dass es keine einfache Aufgabe darstellt, detaillierte Daten beispielsweise zu beziehungsweise aus Banken und Unternehmen für die nicht-kommerzielle Forschung zur Verfügung zu stellen, machte **Stefan Bender**, Forschungsdaten- und Servicezentrum der Deutschen Bundesbank, deutlich. Er gab einen Einblick in die Arbeit des Forschungsdatenzentrums der Bundesbank, das

vom Rat für Sozial- und Wirtschaftsdaten (RatSWD) akkreditiert ist und Daten für nicht-kommerzielle Forschungszwecke bereitstellt. Das Forschungsdatenzentrum biete weitgehend Originaldaten in sehr granularer Art an, die zum Teil sehr detaillierte Informationen zu Banken und Unternehmen beinhalten und demnach nicht offen zugänglich sein können. Das FDZ sei Teil des „Knowledge Life Cycle“ in der Bundesbank. Wichtig sei, dass die Daten für die externen Anspruchsgruppen die FAIR-Prinzipien erfüllen, also findbar, zugänglich, interoperabel und nachnutzbar sind. Mit Blick auf die Herausforderungen einer Datentreuhandstelle unterschied Bender drei Dimensionen, die zu berücksichtigen sind: Wissen (u.a. im Bereich Data Science, Programmierung, Anonymisierung), Rahmenbedingungen mit Blick auf den Datenzugang und Vertrauen (mit Blick auf die Datenerzeuger und Datennachfrager).

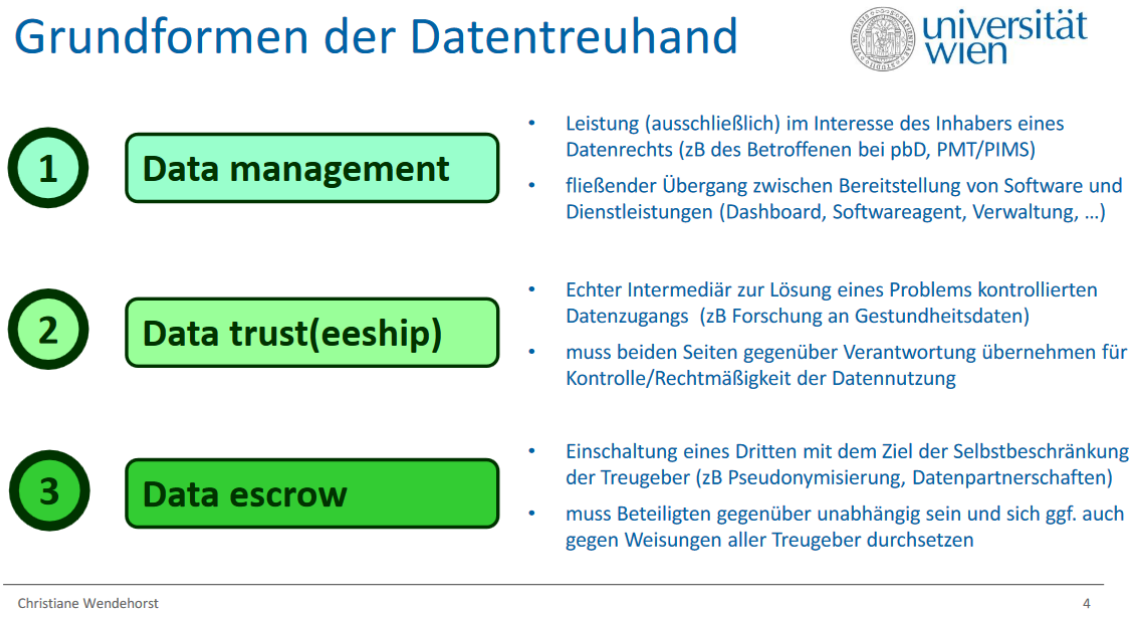


Ähnlich wie Robert Schmitt ging Thomas Zurek, SAP, auf allgemeine Schwierigkeiten für Unternehmen ein, Daten herauszugeben. Dies betreffe beispielsweise Daten, die offenbaren, welche Geschäftsprozesse im Unternehmen ablaufen. Datensicherheit müsse hinsichtlich des Zugangs zu Daten, aber auch des Zugangs zu Metadaten hergestellt werden. Als weitere entscheidende Kriterien nannte er Compliance mit Rahmenvorgaben, Angaben zur Datenprovenienz und Datenschutz. Neben den zu berücksichtigenden legalen Anforderungen müsste aus seiner Sicht auch transparent sein, wer zu welchem Zeitpunkt welche Daten eingesehen habe. Dies sollte im Falle der Bereitstellung von Daten durch einen Datentreuhänder nachvollziehbar sein.

Wie sich aus Sicht der Verbraucherzentralen der Diskurs um „neue Datenintermediäre“ entwickelt, veranschaulichte Lina Ehrig, Verbraucherzentrale Bundesverband. Die Debatte sei zunächst als recht diffus wahrgenommen worden, da es kein einheitliches Verständnis über die Rollen und Ziele dieser Intermediäre gebe und am Markt auch unterschiedliche Geschäftsmodelle zu erkennen seien. Intensiv habe man sich mit Modellen beschäftigt, die sich als Angebote an Verbraucherinnen und Verbraucher richten, darunter die Personal Information Management Systems (PIMS). Diese sollen das Einwilligungsmanagement für die Verwendung der persönlichen Daten von Konsumenten durch Dritte erleichtern, sie könnten aber im Einzelfall weitere Funktionen wie die Pseudonymisierung von Daten übernehmen oder Verbraucher unterstützen, ihre Auskunft- und Löschansprüche wahrzunehmen. Die Erfahrungen mit diesem Geschäftsmodell seien nach Auffassung der Verbraucherschützer durchwachsen. Eine Herausforderung sei, wie eine informierte Einwilligung nach der Datenschutzgrundverordnung (DSGVO) erzielt werden könne. Insofern habe dieses Modell

noch keine Marktdurchdringung erfahren. Für Datenintermediäre sei die Einhaltung der DSGVO nicht ausreichend geregelt, auch nicht im Zusammenspiel mit einer Datenschutz-Zertifizierung. Es bedürfe eines europäischen Rechtsrahmens, der Treuepflichten und Haftungsfragen regelt, Transparenzanforderungen formuliert und Monopole verhindert.

Inwieweit eine Unterscheidung unterschiedlicher Formen von Datentreuhändern notwendig ist, zeigte Christiane Wendehorst, Universität Wien, auf. Einleitend merkte sie an, dass die Datenethikkommission in Datenmanagement und -treuhandsystemen ein großes Potenzial gesehen habe. Nun stelle sich aber die Frage der konkreten Ausgestaltung. Wendehorst unterschied drei Grundformen der Datentreuhand und nannte die damit verbundenen spezifischen Herausforderungen.



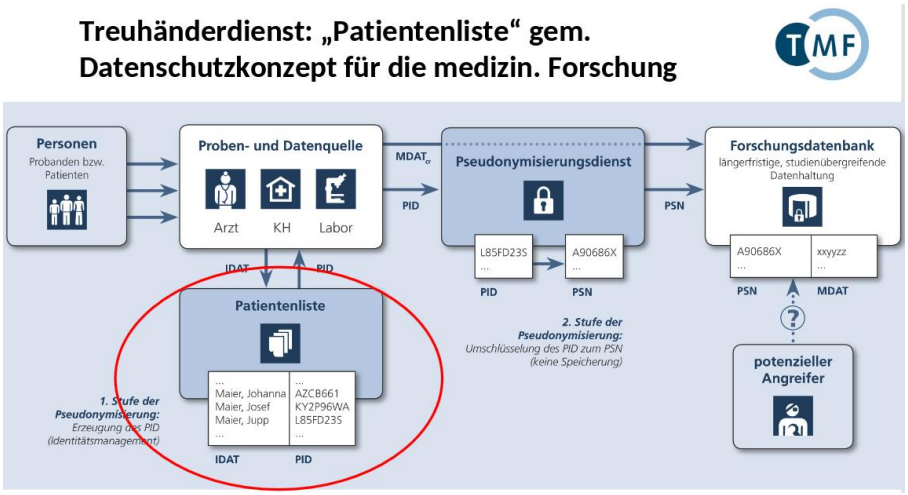
Zu nennen seien erstens Datenmanagementsysteme (zum Beispiel Privacy Management Tools/Personal Information Management Systems), deren Aufgabe es ist, einseitig die Interessen des Betroffenen wahrzunehmen. Es handele sich um eine spezielle Verwaltungsdienstleistung. Hier brauche es verschiedene Mechanismen, wie zum Beispiel Qualitätssicherung, um berechtigtes Vertrauen sicherzustellen. Zweitens sei die Datentreuhand mit einem Treuhänder als echtem Intermediär zwischen Datenerzeuger und Datennachfrager zu nennen. Sie stelle einen Lösungsansatz für Probleme des Datenzugangs dar. Datentreuhänder müssen beiden Seiten gegenüber Verantwortung für die Rechtmäßigkeit der Datennutzung übernehmen. Herausforderungen würden hier in Mandaten zur Ausübung von Datenrechten und in der Vermeidung von Interessenkonflikten liegen. Schließlich seien Dienste zu nennen, bei denen die Aufgabe eines vertrauenswürdigen Dritten eher darin liegt, zu weitgehende Befugnisse und Zugriffsmöglichkeiten anderer Parteien zu beschränken (z.B. als Verwahrer eines Schlüssels bei pseudonymisierten Daten). Diese Form der Datentreuhand werde auch jenseits des Datenschutzes immer wichtiger, da mit ihrer Hilfe teils Konflikte mit dem Kartellrecht vermieden werden könnten. In diesem Zusammenhang seien Standards, unter anderem im Wettbewerbsrecht notwendig.

In der anschließenden Diskussion wurde erörtert, inwieweit regulatorische Maßnahmen, ausgerichtet an den jeweiligen Grundformen beziehungsweise Kategorien von Datentreuhändern, als sinnvoll betrachtet werden können. Wie Lina Ehrig problematisierte, haben sich in den letzten eineinhalb Jahren viele als Datentreuhänder bezeichnet, die primär kommerzielle Interessen verfolgen und demnach keine neutrale Position einnehmen. Regulatorische Leitplanken seien notwendig, dabei sei aber nicht jede Kategorie in gleicher Weise regulierungsbedürftig. Christiane Wendehorst schlug vor, den Begriff Regulierung zu vermeiden und stattdessen von Rechtsrahmen zu sprechen. Hierdurch komme die einschränkende, aber auch ermöglichende Funktion zum Ausdruck. Es brauche zum Teil auch einen übergreifenden europäischen Rechtsrahmen. Eine Regulierung dürfe aber, so gab Robert Schmitt zu bedenken, nicht dazu führen, dass die Kreativität von Datenerzeugern und -nutzern eingeschränkt werde. Stefan Bender unterstrich, dass in vielen Punkten weiterer Klärungsbedarf besteht. Er schlug vor, Leitplanken zu formulieren, inwieweit beispielsweise eigene Forschungstätigkeiten mit der Neutralitätsverpflichtung des Datentreuhänders in Einklang gebracht werden könnten – ein Problem, das sich in den Forschungsdatenzentren in besonderer Weise stelle.

SESSION II - ZUGANGSMODELLE

Die zweite Session beschäftigte sich mit der Frage, wie mehreren Akteuren ein bedarfsgerechter und gleichberechtigter Datenzugang ermöglicht werden kann. Bei der Ausgestaltung von Zugangsmodellen müssen insbesondere die Zugangswege und Bedingungen hinsichtlich der Weitergabe der Daten geklärt werden.

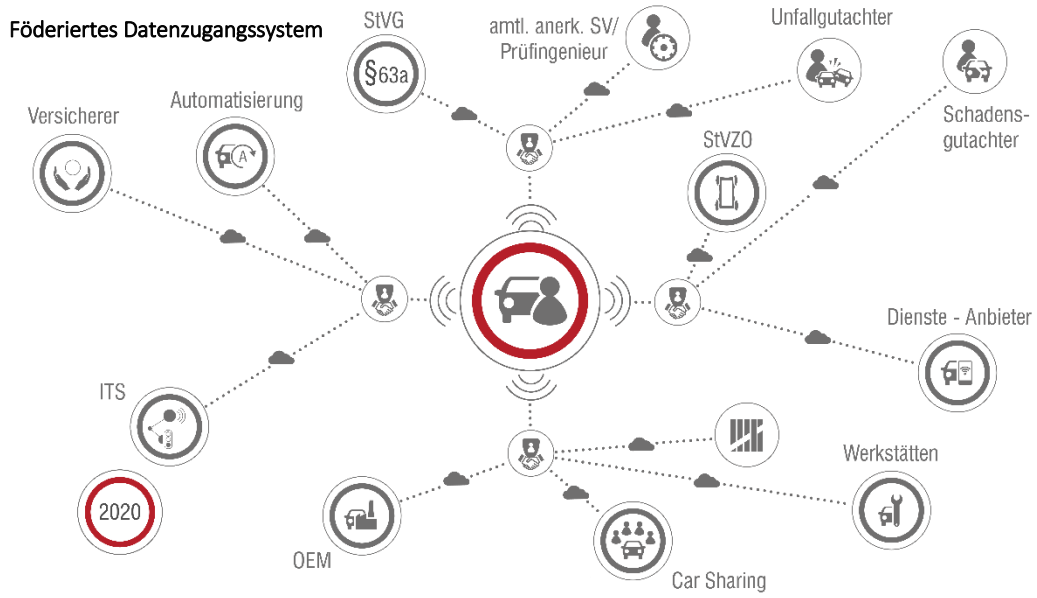
Einen Überblick über die Initiativen im Bereich medizinischer Daten und Bemühungen eines verbesserten Datenzugangs für die Forschung gab **Sebastian Semler**, Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF). Anhand der Medizininformatik-Initiative zeigte er auf, wie Daten aus der Krankenversorgung durch den



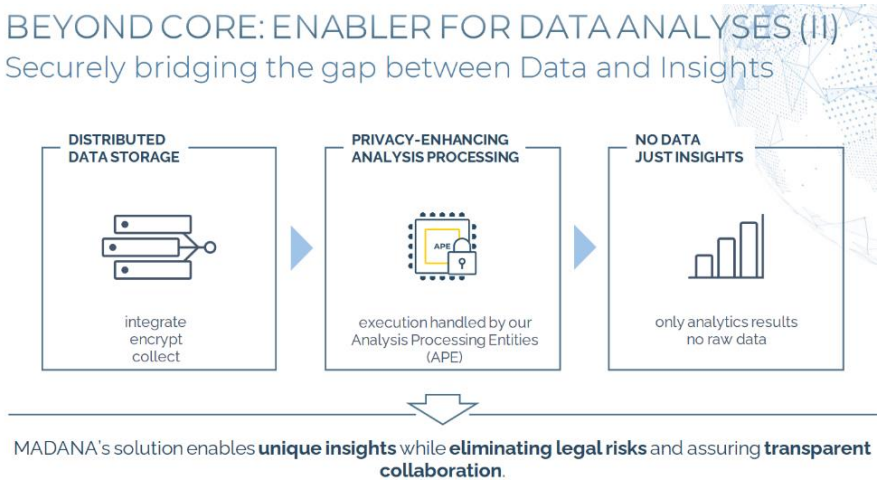
Aufbau von Datenintegrationszentren nachnutzbar gemacht werden. Er verwies zudem auf generische Datenschutzkonzepte, die seit 2001 von der TMF fortlaufend und im Dialog mit Datenschutzbeauftragten erarbeitet werden und die eine strikte Trennung von identifizierenden und medizinischen Nutzdaten vorsehen (Konzept der informationellen Gewaltenteilung). Die Vertrauenswürdigkeit und rechtliche Unabhängigkeit seien zentrale Anforderungen an eine solche Datentreuhandstelle. Ebenso müsse eine hohe IT-Kompetenz und auch für die spezifische

Wissenschaftsdomäne eine entsprechende Fachkompetenz vorhanden sein. Empfehlenswert sei auch die Durchsetzung von klaren Use- & Access-Verfahren. Die Nationale Kohorte (NAKO) und auch die technologiegestützte Treuhandlösung der Bundesdruckerei führte er als Best-Practice-Beispiele an.

Im Bereich Mobilitätsdaten wird sichtbar, welche Anstrengungen notwendig sind, um einen fairen und gleichberechtigten Datenzugang sicherzustellen. Welche Folgen sich für den Verbraucher aufgrund der zunehmenden Vernetzung von Fahrzeugen und der Gatekeeper-Rolle der Fahrzeughersteller ergeben, führte **Fred Blüthner**, FSD Fahrzeugsystemdaten – Zentrale Stelle nach StVG, aus. Im Grunde werden die – auch personenbeziehbaren – Mobilitätsdaten der Fahrzeugnutzer, von dem Unternehmen, welches das Fahrzeug hergestellt hat, exklusiv verwaltet. Sofern sich die Daten ausschließlich über Server des Fahrzeugherstellers beziehen lassen, habe dies Nachteile für das Angebot wettbewerbsfähiger und unabhängiger Dienste. Es bestünde auch die Gefahr der Datenmanipulation. Dass Fahrzeugdaten wie zum Beispiel die des Unfalldatenspeichers (EDR) beim Fahrzeughersteller verbleiben und dem Fahrzeughalter, dessen Versicherung oder einem Sachverständigen nicht direkt und unabhängig zugänglich sind, habe unter anderem Auswirkungen auf die vertrauenswürdige und transparente Aufklärung und Nachverfolgung von Unfällen. Blüthner argumentierte dagegen für ein föderiertes Datenzugangssystem, das den Nutzer in den Mittelpunkt rückt. Aus seiner Sicht soll der Fahrzeughalter selbst entscheiden können, an wen er seine Daten geben möchte, gegebenenfalls solle er auch daran verdienen können.



Christian Junger, MADANA, verdeutlichte das Potenzial, das in technischen Lösungen, insbesondere in Verschlüsselungstechnologien rund um Confidential Computing liegt, um einen vertrauensvollen und fairen Datenaustausch zu ermöglichen. Er stellte die Idee einer dezentralen, plattformbasierten Datenanalyse vor. Es ließe sich ein ganzes System an sogenannten „sicheren Enklaven“ aufbauen, die eine Vernetzung über gesicherte Kanäle ermöglichen und einen Zugriff Dritter ausschließen. Der Datenproduzent könne seine Daten über einen verschlüsselten Hardwarebereich (Trusted Execution Environment) zur Verfügung stellen. Die Datenanalyse erfolge automatisiert, sodass das Ergebnis verschlüsselt an den Käufer des Ergebnisses geschickt werde. Ein Rückschluss auf die Rohdaten sei so nicht möglich. Hiermit sei eine technische Möglichkeit von "Federated Learning" gegeben, Daten zu analysieren und anschließend mit neuen, aggregierten Daten zu arbeiten, ohne dass die Ursprungsdaten herausgegeben oder synthetisiert beziehungsweise verwässert werden müssen.



Aus der Perspektive der Wirtschaft seien – wie Henning Schwabe, BASF, aufzeigte – neue Dateninfrastrukturen notwendig, um zirkulares Wirtschaften oder auch verantwortungsvolle Lieferketten aufbauen zu können. Der Nachhaltigkeitsbericht, in dem Unternehmen unter anderem über die ökologischen Auswirkungen ihrer Tätigkeiten berichten, sei ein Beispiel für den B2B-Datenaustausch. Hier gebe es ISO-Standards, aber auch ein firmenspezifisches Reporting. Schwabe differenzierte mit Blick auf den Zugang zwischen der Möglichkeit eines unbegrenzten, anonymen Zugriffs sowie einem Datenaustausch zwischen Mitgliedern eines „Clubs“. Nahezu jede Branche experimentiere mit Datenplattformen, die lediglich bestimmten Nutzern offenstehen. Als dritte Variante nannte er den bilateralen Datenaustausch auf der Ebene bereits bestehender Geschäftsbeziehungen. Hier werden Nutzungs- und Schutzrechte untereinander vereinbart.

Aus Sicht von Louisa Specht-Riemenschneider, Universität Bonn, könnten Datentreuhänder dazu beitragen, dort den Datenzugang zu verbessern, wo Daten nicht freiwillig herausgegeben werden; sie hat dabei namentlich die globalen Internetunternehmen („Big Five“) im Blick. Es genüge aber nicht, einen Datentreuhänder oder Datenzugangsermittler einzuschalten, ohne dass in materiellrechtlicher Hinsicht Datenzugangsansprüche bestehen. Specht-Riemenschneider schlug vor, über abgeleitete Datenzugangsansprüche für die Wissenschaft nachzudenken, das heißt der Wissenschaft überall dort Datenzugangsansprüche zu gewähren, wo auch andere Dritte solche Zugangsansprüche haben.

Dabei sei zu diskutieren, wer Zugang erhalten soll, wie lange dieser gewährt wird und ob beziehungsweise wie Zugang im Sinne des Bereitstellers vergütet werden soll. Auch Zugangsbeschränkungen müssen für unterschiedliche Zugriffsinteressen geregelt werden, zum Beispiel zum Schutz von Geschäftsgeheimnissen. Von einer gesetzlichen Regelung könnten auch Konkurrenten im Wettbewerb um Daten profitieren. Hinsichtlich der Gestaltung eines Datentreuhänders seien sektorspezifische Regelungen wichtig, darüber hinaus empfahl sie horizontale Leitplanken, also übergreifende gesetzliche Rahmenbedingungen. Ein Datentreuhänder sollte dezentral eingerichtet sein, es sollte auch eine Zertifizierung und gegebenenfalls Haftungsprivilegierungen geben. Hinsichtlich der Stellung des Datentreuhänders zeigte sie drei mögliche Varianten auf: Dieser könnte als Host für die ihm anvertrauten Daten, als Host mit Verarbeitungsbefugnissen (d.h. der die Daten auch hält und ggf. veredeln kann) oder als Zugangsberechtigter (in Form eines neutralen Dritten, der Einblick in die Daten erhält) ausgestaltet werden.

In der Diskussion fanden die Ansätze einer Modellbildung für Datentreuhänder, die Frau Wendehorst und Frau Riemenschneider präsentiert hatten, große Zustimmung. Es sei zudem deutlich, dass es konkrete sektorspezifische Lösungsansätze geben müsse, die aber gegebenenfalls entlang einiger sektorübergreifender horizontaler Leitlinien ausgerichtet sein könnten, entsprechende Modelle seien weiter zu konkretisieren. Es wurde zudem herausgearbeitet, dass allein technische Lösungen nicht ausreichten, um genug Vertrauen zu organisieren. Vielmehr sei es wichtig, dass Technik und rechtliche Rahmenbedingungen miteinander verbunden werden. Sichtbar wurden auch die sektorspezifischen Herausforderungen. Im Bereich der Medizindaten bestehe, wie Herr Semler darlegte, ein großer Personalbedarf, um das Einwilligungsmanagement übernehmen und gegebenenfalls auch bündeln zu können. Herr Blüthner machte darauf aufmerksam, dass für Mobilitätsdaten erst noch Aushandlungsprozesse und entsprechende Geschäftsmodelle etabliert werden müssten, die einen fairen Datenaustausch ermöglichen. Abschließend wurde herausgearbeitet, dass dies letztlich die grundsätzliche Frage berühre, wie ein europäisches Modell der kollaborativen Wertschöpfung ausgestaltet werden könne.

SESSION III - QUALITÄTSSICHERUNG

Thema der dritten Session war die Frage, welche Qualitätskriterien an Datentreuhänder angelegt werden können, um das Vertrauen der Datengeber in einen solchen Intermediär zu stärken. Auch stand zur Diskussion, welche Qualitätssicherungsmaßnahmen in Form von Zertifizierungsverfahren oder Regeln/Standards sinnvoll erscheinen.

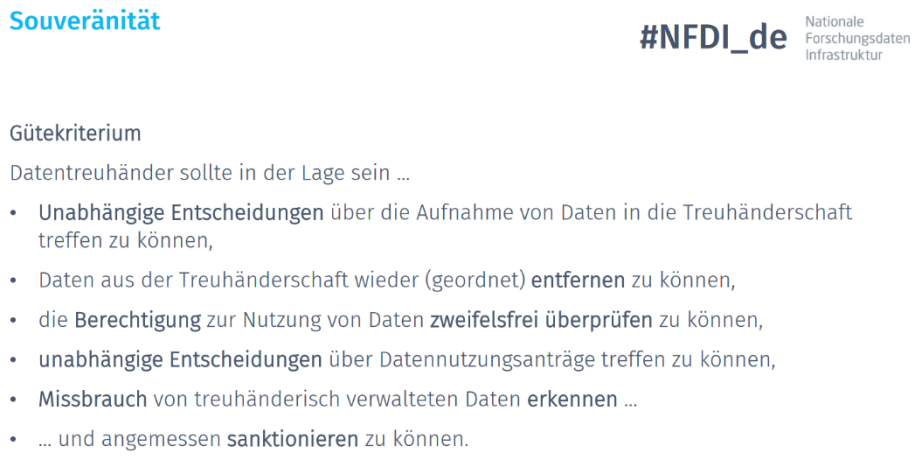
Gütekriterien seien aus Sicht von Jan Schallaböck, iRIGHTS, vor allem hinsichtlich Transparenz und Rechenschaftspflicht anzulegen, dies umfasse unter anderem die Pflichten und Zwecke der Weitergabe sowie die technischen Systeme und Schutzmaßnahmen. Vertraulichkeit sei ein weiterer möglicher Bereich, der beim Entwurf von Gütekriterien zu berücksichtigen sei. Die Qualität der Kuratierung, der Anonymisierung und Pseudonymisierung sowie der Schutzmaßnahmen seien hier relevant. Schallaböck führte die Vielfalt an Zertifizierungsmechanismen vor Augen (darunter u.a. ein- bzw. zweistufige Verfahren sowie die Datenschutzfolgeabschätzung) und skizzierte die bereits bestehenden internationalen Standards, beispielsweise mit Blick auf die Definition von personenbezogenen Daten. Abschließend argumentierte er für die Einführung eines zentralen Registers von Datensammlungen. Dies eröffne Zugangswege für die wissenschaftliche Forschung und erhöhe den gesellschaftlichen Einblick in bestehende Datenverarbeitungen.

Hinsichtlich der Qualitätssicherung sei nach Ralf Wehrspohn, Vorstand der Fraunhofer-Gesellschaft, zwischen Anforderungen an den Datentreuhänder sowie Anforderungen an die Daten selbst zu unterscheiden. Beide Komponenten sollten in die Entwicklung eines Prüfkatalogs einfließen. Wehrspohn sprach sich für eine abgestufte Zertifizierung aus. Mit Blick auf die notwendigen Aufgaben des Intermediärs fügte er ergänzend die Gewährleistung für Datenportabilität, Interoperabilität und Datensouveränität hinzu. Dabei verwies er ebenfalls auf die zentrale Bedeutung der Neutralität des Datenintermediärs. Dieser dürfe keine wirtschaftlichen Eigeninteressen verfolgen.

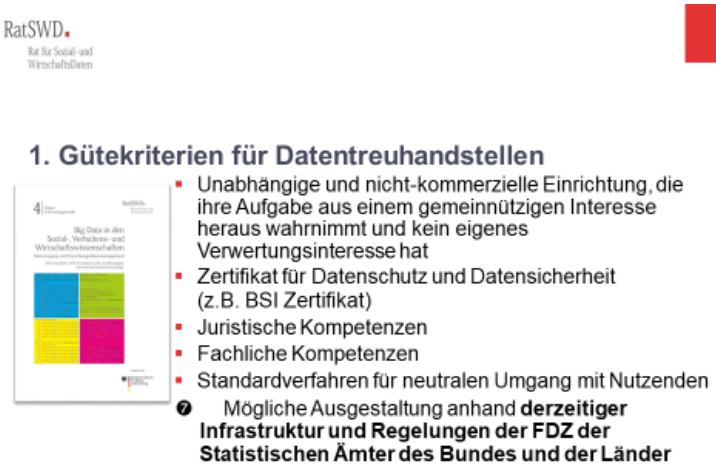
Rolf Schwartmann, TH Köln, erläuterte den Ansatz der Datenethikkommission, die bei Datenmanagement- und Datentreuhandsystemen zwischen zwei Modellen unterscheide: „technische Dashboards“ mit Einwilligungsmanagement sowie umfassende Dienstleistungen der Daten- und Einwilligungsverwaltung. Ausführlich stellte er den Referentenentwurf zu § 3 des Telekommunikations-Telemedien-Datenschutz-Gesetzes (TTDSG) vor, der auch auf Datentreuhänder Bezug nehme. Dargelegt werde hier, wie unter Vermeidung von Cookies, eine anonyme Nutzer-ID zur Verfügung gestellt werden könne. Dies ziele darauf, eine größere Unabhängigkeit gegenüber Login-Systemen großer Anbieter wie Google, Facebook, Amazon und somit ein Gleichgewicht für nationale/europäische Plattformen zu erreichen. Schwartmann führte auch Anstrengungen auf europäischer Ebene in Bezug auf eine sichere europäische digitale Identität aus, die allen Bürgerinnen und Bürgern zur Verfügung stehen und ihnen mehr Kontrolle über ihre Daten ermöglichen soll.

Weitere Erwartungen an einen Datentreuhänder formulierte York Sure-Vetter, Direktor der NFDI. Ein Datentreuhänder solle unter anderem unabhängige Entscheidungen über die

Aufnahme von Daten in die Treuhänderschaft treffen können und auch in der Lage sein, Daten wieder hieraus entfernen zu können. Ebenfalls sollte er Missbrauch von treuhänderisch verwalteten Daten erkennen und diesen sanktionieren können. Zusammenfassend zeigte Sure-Vetter drei zentrale Dimensionen auf, die bei der Ausgestaltung von Datentreuhändern eine Rolle spielen sollten: Die Befähigung, Daten zu speichern und zur Verfügung zu stellen, die Souveränität, unabhängige Entscheidungen treffen zu können, und die Vorteilsfreiheit. Es reiche aber nicht aus, diese Aspekte zu sammeln, es müssten auch erhebliche Anstrengungen unternommen werden, um diese in die Praxis umzusetzen.



Monika Jungbauer-Gans, Deutsches Zentrum für Hochschul- und Wissenschaftsforschung (DZHW) und Vorsitzende des Rates für Sozial- und Wirtschaftsdaten (RatSWD), hob die notwendige juristische und fachliche Kompetenz hervor, die in diesen Stellen vorhanden sein müsse. Forschungsdatenzentren seien Beispiele für ein dezentrales Modell, das variable Zugriffsmöglichkeiten biete, von Public Use Files bis hin zu differenzierten Daten, die nur On-Site genutzt werden können. Dazwischen gebe es zahlreiche Abstufungen. Mit Blick auf Zertifizierungsverfahren legte sie dar, dass ein Stufenmodell allein bemessen am Sensitivitätsgrad der Daten schwierig umzusetzen sei, da auch unterschiedliche Formen der Nachnutzung berücksichtigt werden müssten. Hier seien gegebenenfalls intransparente Einzelfallentscheidungen notwendig. Jungbauer-Gans veranschaulichte die jeweiligen Vorteile einer zentralen (u.a. die Möglichkeit der Stichprobenziehung) sowie föderierten Datentreuhandstruktur (community-nahes Beratungsangebot, inhaltliche/fachliche Spezialisierung zur Qualitätssicherung).



Zur Frage nach geeigneten Qualitätssicherungsmaßnahmen wurden in der anschließenden Diskussion weitere Anregungen gegeben. Aus Sicht von Herrn Wehrspohn sollte eine Zertifizierung in Form einer kontinuierlichen (und nicht nur einmaligen) Evaluierung beziehungsweise Prüfung bestehen, die neben den Prozessen auch die angewandte Technik berücksichtige. Das Kriterium der Gemeinnützigkeit des Datentreuhänders wurde von Herrn Schwartmann nachgeschärft: Dieser dürfe keine unternehmerischen Interessen verfolgen, das heißt nicht an der Nutzung der Daten verdienen können, er müsse sich aber durch die „Verwaltung“ der Daten refinanzieren können. Auf Seiten der Industrie bestehe – wie Herr Schwabe bekräftigte – ein dringlicher Handlungsbedarf, in den kommenden Jahren zügig Systeme oder neutrale Stellen zu schaffen, um das bestehende „Gefangenendilemma“ überwinden zu können, in welchem sich die derzeit vielfach abwartenden Unternehmen befänden. Dabei sollte unter anderem der Aspekt der Nutzungsketten bei der Konzeption von Datentreuhändern mitbedacht werden. In Bezug auf die Schaffung dieser Systeme wurde auch die Frage der Finanzierbarkeit gestellt. Gleichzeitig wurde der unmittelbare Handlungsbedarf hervorgehoben. Wichtig sei, Herrn Sure-Vetter zufolge, nicht nur zwischen verschiedenen Datentreuhandkategorien zu differenzieren, sondern auch einen Aktionsplan zu entwerfen, welche Ziele mit welcher Priorisierung angestrebt werden sollten. Abschließend plädierte Herr Schallaböck dafür, verstärkt die Frage zu betrachten, wie entsprechende Anreizmodelle zur Ausgestaltung von Datentreuhandstellen geschaffen werden können.

Zusammenfassend hob Frau Hansen zum Schluss hervor, dass durch die Vorträge und Diskussionen das weite Feld an Anwendungsbereichen und Perspektiven auf das Thema Datentreuhänderschaft deutlich geworden sei. Zugleich sei die Dringlichkeit des Bedarfs in sehr verschiedenen Sektoren eindrucksvoll sichtbar geworden. Frau Gehring unterstrich das Erkenntnispotenzial, das ein Gedankenaustausch bei der Ausgestaltung von Lösungsansätzen eröffne. Freilich zeigten sich aus Perspektive des RfII auch Grenzen, bestehende Erfahrungen aus der Wissenschaft mit treuhandähnlichen Stellen und Verfahren auf andere gesellschaftliche Bereiche zu übertragen.

Impressum

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