Rat für
Informations
Infrastrukturen

RfII Berichte No. 5

Datentreuhänder:
Potenziale für wissenschaftskonformes Datenteilen – Herausforderungen für die institutionelle Ausgestaltung

Analysen, Begriffsbestimmungen und Stellungnahmen

Juni 2023

Datentreuhänder:
Potenziale für wissenschaftskonformes Datenteilen –
Herausforderungen für die institutionelle Ausgestaltung

IMPRESSUM

Verabschiedet im Juni 2023

Rat für Informationsinfrastrukturen (RfII)
Geschäftsstelle
Papendiek 16
37073 Göttingen

Tel. 0551-3927050
E-Mail info@rfii.de
Web www.rfii.de

DRUCK

Klartext GmbH, Göttingen

ZITIERVORSCHLAG

RfII – Rat für Informationsinfrastrukturen: Datentreuhänder: Potenziale für wissenschaftskonformes Datenteilen – Herausforderungen für die institutionelle Ausgestaltung, RfII Berichte No. 5, Göttingen 2023, 87 S.

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über URN urn:nbn:de:101:1-2023021714 abrufbar.

INHALT

ABKÜRZUNGSVERZEICHNIS

B2B	Business to Business
B2G	Business to Government
BMBF	Bundesministerium für Bildung und Forschung
BMWK	Bundesministerium für Wirtschaft und Klimaschutz
DA	Data Act
DGA	Data Governance Act
DSGVO	Datenschutz-Grundverordnung
DSP	Data sharing providers
DSS	Data sharing services
FAIR	Findable, Accessable, Interoperable, Reusable
FDZ	Forschungsdatenzentrum
KMU	Kleine und mittlere Unternehmen
MII	Medizininformatikinitiative
PIMS	Personal Information Management Systeme
RatSWD	Rat für Sozial- und Wirtschaftsdaten
RfII	Rat für Informationsinfrastrukturen
TMF	Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.
vzbv	Verbraucherzentrale Bundesverband

ZUSAMMENFASSUNG

Bestrebungen auf nationaler wie europäischer Ebene zielen darauf ab, das Teilen von digitalen Daten zu vereinfachen. Dies soll einerseits in einzelnen gesellschaftlichen Bereichen wie beispielsweise dem Gesundheitswesen oder im Mobilitätssektor geschehen. Andererseits soll das Datenteilen auch über Bereiche und Domänengrenzen hinweg gefördert und Daten aus der öffentlichen Verwaltung, der Wissenschaft, der Wirtschaft oder Zivilgesellschaft besser zwischen den Akteuren in diesen Sektoren zugänglich gemacht werden. Hierfür fehlen allerdings noch einheitliche Standards, Dateninfrastrukturen und vertrauenswürdige Datenmittlerstrukturen (Intermediäre). Außerdem bestehen bislang Unsicherheiten, welche Daten auf welche Weise verfügbar gemacht und von Dritten weiterverwendet werden dürfen. Rechtliche Rahmensetzung und auch die konkreten Datenschutzanforderungen sind nicht immer klar oder werden uneinheitlich interpretiert.

Datentreuhänder stellen in diesem Kontext einen vielfach diskutierten Lösungsansatz dar: Sie sollen dazu beitragen, unter Datengebern und Datennutzern ein Vertrauensverhältnis aufzubauen, indem sie als markt- und interessensneutrale Instanzen fungieren, den Datenzugang vermitteln und eine rechtmäßige Datennutzung und -weiterverwendung zu fairen und transparenten Bedingungen gewährleisten. Sinnvoll erscheint der Aufbau und Einsatz von Datentreuhändern unter anderem dort, wo sich potenzielle Konflikte um den Zugang zu Daten ergeben, insbesondere in Bezug auf den Schutz von personenbezogenen Daten oder von Betriebsgeheimnissen.

Das Konzept der Datentreuhänderschaft ist aus dem Blickwinkel wissenschaftlicher Akteure von hoher Relevanz, da sie

- aufgrund ihrer umfangreichen Erfahrung hinsichtlich der innerwissenschaftlichen Nutzung bzw. Verfügbarmachung sensibler und schützenswerter Daten an der Erarbeitung geeigneter Lösungsansätze sowohl für bereichsspezifisches als auch bereichsübergreifendes Datenteilen mitwirken können;
- das Anliegen verfolgen, mit den vorhandenen Daten aus anderen gesellschaftlichen Teilbereichen – insbesondere der öffentlichen Verwaltung, des Gesundheitssystems, aber auch aus Unternehmen – im Gemeinwohlinteresse zu forschen;
- unter den Stichworten „Datensouveränität“ und „Wissenschaftsfreiheit“ nicht die Kontrolle über die Nutzung und Verwertung von Daten aus der eigenen Forschung verlieren und zugleich legitime externe Zugangsansprüche fair regeln und umsetzen möchten.

Der Rat für Informationsinfrastrukturen (RfII) spricht als Beratungsgremium aus der Perspektive des Wissenschaftssystems Empfehlungen zur Weiterentwicklung wissenschaftlicher und wissenschaftsrelevanter Informationsinfrastrukturen sowie zum digitalen Wandel in der Wissenschaft aus und hat sich in diesem Zusammenhang auch mit

dem Thema Datentreuhänderschaft intensiv auseinandergesetzt. Der vorliegende Arbeitsbericht fasst die Ergebnisse einer vom RfII eingesetzten Arbeitsgruppe zu Datentreuhänderschaft zusammen.

Der Arbeitsbericht behandelt Fragen des sektorenübergreifenden Datenteilens, insbesondere im Kontext der Schnittstelle von Wissenschaft und Wirtschaft. Hierzu werden aus Perspektive des Wissenschaftssystems handhabbare Begriffsbestimmungen vorgeschlagen. Mit Blick auf die zentralen Begriffe Digitale Souveränität und Datensouveränität werden wissenschaftspolitische Implikationen nachgezeichnet. Ein Workshop und ein Fachgespräch haben wichtige außerwissenschaftliche Expertise für die Arbeit und Arbeitsergebnisse des RfII zur Datentreuhänderschaft nutzbar gemacht. Mehrere Gesetzgebungsprozesse auf europäischer Ebene, die im Zusammenhang mit der Digitalstrategie der EU und der Etablierung eines digitalen Binnenmarktes stehen, setzen die Rahmenbedingungen für den Aufbau von Datenmittlerstrukturen (Data Governance Act) und den Zugang zu Daten (Data Act). Der RfII hat hierzu Anregungen in Form von Stellungnahmen verabschiedet und in Konsultationsprozessen der Europäischen Union vermittelt. Sie finden sich am Ende dieses Berichts.

Als Ergebnis der Befassung des RfII mit dem Themenkreis Datentreuhänderschaft lässt sich festhalten, dass mit der Etablierung von Datentreuhändern große Herausforderungen verbunden sind. Dies betrifft insbesondere die Frage nach der Konzeption sowohl öffentlicher als auch kommerziell tragfähiger und zugleich wissenschaftsfreundlicher Geschäftsmodelle sowie deren rechtssicherer Ausgestaltung. Erste Erprobungen von Datentreuhandmodellen können wertvolle Erkenntnisse für faires und wissenschaftskonformes Datenteilen liefern.

Der RfII empfiehlt in dem hier vorliegenden Bericht unter anderem:[1]

- das Sammeln von Erfahrungen in weiteren Pilotvorhaben;
- Begleitforschungen zu bereits pilotierten Datentreuhandmodellen;
- eine Fortsetzung und Intensivierung des Austauschs verschiedener Akteure zu neuen Intermediären, unter anderem aus der Wissenschaft, Wirtschaft und Zivilgesellschaft;
- die Schaffung von Rahmenbedingungen, die den Aufbau und die Nutzung von Datentreuhändern für die Praxis erleichtern (z. B. mit Blick auf Haftungsfragen).

1 S. hierzu S. 20-25. Vgl. auch die bereits veröffentlichten Stellungnahmen des RfII zum Themenfeld Datentreuhänderschaft im Anhang, Abschnitt C.

EXECUTIVE SUMMARY

National and European efforts strive for simplifying the sharing of digital data in various areas of society. On the one hand, this is intended in single social sectors such as the health and mobility sector. On the other hand, data sharing should also be promoted across sectors and domain boundaries. Data from public administration, science, business or civil society should be made more accessible between the actors in these sectors. For these purposes however, uniform standards, data infrastructures and trustworthy data intermediary structures (intermediaries) are still missing. Moreover, there are uncertainties so far about which data may be made available, in which form, and how these would be eventually used by third parties. Legal frameworks and also the concrete data protection requirements are not always clear or are getting interpreted in an inconsistent manner. In this context, data trusts are often discussed as a solution: They can help to build trust between data holders and data users by acting as neutral bodies, mediating access to data and guaranteeing the lawful use and re-use of data under fair and transparent conditions. The establishment and use of data trusts makes sense, among other things, where potential conflicts arise over access to data, especially with regard to the protection of personal data or trade secrets.

From the perspective of scientific actors, the concept of data trusteeship is highly relevant because they

- are able to contribute to the development of suitable solutions for both sector-specific and cross-domain data sharing due to their extensive experience in the use and availability of sensitive data within the scientific community,
- pursue the aim of conducting research in the public interest using existing data from other social sectors and domains – especially from public administration, the health system, but also from private companies,
- do not want to lose control over the use and re-use of data from their own research (keywords here are “data sovereignty” and “academic freedom”) but also have an interest in a regulation and implementation of legitimate and fair external access to research data.

The German Council for Scientific Information Infrastructures (RfII) gives recommendations as an advisory body from the view point of the scientific system on the further development of research and science-related information infrastructures as well as on the digital turn in science in general. In this context the Council has also discussed intensively the topic of data trusteeship. The present report aggregates the main results of a RfII working group on this subject.

The report picks up questions of cross-sectoral data sharing especially on the interface of science and economy. For this purpose, definitions of the terms digital sovereignty and data sovereignty are proposed from the perspective of the science system. In addition, a workshop and a hearing with external experts were held to make non-

scientific insights fruitful for the discussions of the working group and the results of the RfII on data trusteeship. Several legislative processes at the European level, which are related to the EU's digital strategy and the establishment of a digital single market, set the framework conditions for the development of data intermediation services (via the Data Governance Act) and access to data (via the Data Act). The RfII has made suggestions on these legislative approaches in the form of statements which were fed into the European Union's official consultation processes. They can be found in the annex of this report.

In summary, the establishment of data trusts is associated with major challenges. This concerns particularly the question of developing business models that are both publicly and commercially viable and at the same time science-friendly. But also questions of their legally secure design are touched. Pilot projects can provide valuable insights into fair data sharing which is compliant with scientific needs.

The RfII recommends in this report:[2]

- gathering more experience in further pilot projects,
- accompanying research on already conducted pilots,
- continuation and intensification of the exchange between various actors from science, business and civil society on new intermediaries,
- the creation of framework conditions that facilitate the establishment and use of data trusts in practice (e.g. with regard to liability issues).

2 See p. 20-25. Cf. also the already published statements of the RfII on the topic of data trusteeship in the annex, section C.

1 EINLEITUNG

Die Arbeitsgruppe Datentreuhänderschaft wurde auf der 16. Ratssitzung des RfII im November 2019 eingesetzt. Insgesamt traf sich die Arbeitsgruppe zu mehr als zwanzig Arbeitstreffen und veranstaltete einen Workshop im September 2020 sowie ein Fachgespräch im März 2022.

Der thematische Zuschnitt wie auch die erzielten Ergebnisse der AG weisen zusammengefasst folgende Besonderheiten auf:

- Das Themenfeld Datentreuhänderschaft ist erstens generischer Art. Es greift über den Fokus des RfII hinaus, Empfehlungen für Informationsinfrastrukturen in der bzw. für die Wissenschaft im engeren Sinne zu formulieren. So wurden unter anderem Fragen des Datenzugangs an der Schnittstelle von Wissenschaft und Wirtschaft adressiert und Herausforderungen für das Datenteilen auch in den Sektoren Mobilität, Gesundheit, Privatwirtschaft und Finanzsystem untersucht.
- Zweitens stellte sich die Arbeitsgruppe durch die europäischen Gestaltungsvorhaben im digitalen Binnenmarkt der Europäischen Union rasch aktuellen politischen Herausforderungen, die zwar nicht explizit auf die Wissenschaft abzielen, aber in ihren Folgen Konsequenzen für den wissenschaftlichen Umgang mit Daten und den Zugang zu Daten haben. Hier hat sich die Arbeitsgruppe im Auftrag des RfII anhand von Stellungnahmen in die Diskussion rund um das Thema Datentreuhänderschaft eingebracht. Dies betraf insbesondere die Begleitung der legislativen Prozesse, sofern – wie im Data Governance Act (DGA) und Data Act (DA) – Belange des Wissenschaftssystems zumindest mittelbar betroffen waren bzw. sind.

Der vorliegende Bericht führt in das Thema Datentreuhänderschaft ein und skizziert den Diskurs rund um das Konzept in Großbritannien und Deutschland (Kapitel 2). Deutlich wird, dass sich in beiden Ländern in den letzten Jahren ein intensiver Austausch über verschiedene Datentreuhänderansätze entwickelt hat und Datentreuhänder erprobt wurden bzw. werden. Aus Sicht der Arbeitsgruppe haben sich vier Aspekte (Kapitel 3) herauskristallisiert, die in der Beschäftigung und Weiterentwicklung des Konzepts Datentreuhänderschaft relevant sind. Diese betreffen das Setzen von Anreizen in Bezug auf den Aufbau von Datenvermittlungsdiensten bzw. Datentreuhändern, deren rechtssichere Ausgestaltung, die Verankerung von weiteren Mechanismen der Qualitätssicherung sowie die Berücksichtigung des Datenzugangs für Wissenschaft und Forschung. Die Ergebnisse, die aus der AG-Arbeit hervorgegangen sind, werden unter Kapitel 3 mit ihren jeweiligen Kernaussagen jeweils kurz dargelegt. Als Einzelbeiträge sind sie als Stellungnahmen und Workshopberichte vorab veröffentlicht worden. Gemeinsam mit den bislang unveröffentlichten Begriffsklärungen finden sich diese Dokumente im Anhang dieses Berichts.

2 DER DISKURS RUND UM DAS KONZEPT DER DATENTREUHÄNDERSCHAFT

Allgemein lassen sich im Diskurs um Datentreuhänder hinsichtlich der Zielvorstellungen verschiedene Ansätze erkennen:[3] Mit Datentreuhändern wird unter anderem das Potenzial verbunden, Individuen eine bessere Kontrolle über ihre personenbezogenen Daten zu verschaffen. Hierzu werden Softwarelösungen wie Personal Information Management Systeme (PIMS) diskutiert, die unter anderem die Übersicht über erteilte Datenfreigaben und deren Verwaltung erleichtern sollen.[4]

Ein weiterer Ansatz zielt dagegen auf die Schaffung eines Intermediärs, der als neutraler Dritter fungiert und dort Datenaustausch befördern soll, wo sich dieser beispielsweise aufgrund von Rechtsunsicherheiten oder durch konkurrierende Marktpositionen im Bereich des Business to Business (B2B) schwierig gestaltet. Diesem Verständnis nach entscheidet die Datentreuhand über Datenzugangsfragen, führt gegebenenfalls bei widerstreitenden Interessen zwischen Datengebern und potenziellen Nutzern einen Ausgleich herbei und gewährleistet für alle Beteiligten einen rechtssicheren und nach klaren Regeln festgelegten auch sektorenübergreifenden Datenaustausch. Dabei wird über die Ausgestaltung von Datentreuhandmodellen (darunter die Aufgaben eines solchen Intermediärs, mögliche Geschäftsmodelle etc.) als auch die Möglichkeiten, Datentreuhänder im bestehenden Rechtsrahmen aufbauen zu können, noch intensiv diskutiert.

Kurzer Überblick über die Entwicklung des Diskurses in Großbritannien und in Deutschland

Mit Blick auf die Verwendung und mögliche Ausgestaltung von Datentreuhändern ist – unabhängig von der jeweiligen Rechtslage – die Perspektive auf Diskussionsansätze in Großbritannien auch für deutsche Überlegungen von Interesse, da hier vergleichbare inhaltliche Zielsetzungen von Datentreuhändern diskutiert werden und bereits 2019

---

3 Zur weiteren Einordnung s. den Beitrag von Christiane Wendehorst im Bericht des Datentreuhänder-Workshops der AG Datentreuhänderschaft (Rat für Informationsinfrastrukturen (2021) – Workshop-Bericht der AG Datentreuhänderschaft – Datentreuhänder: Potenziale, Erwartungen, Umsetzung, S. 4); Christiane Wendehorst; Sebastian Schwamberger; Julia Grinzinger: Datentreuhand – wie hilfreich sind sachenrechtliche Konzepte?, in: Tereza Pertot, Hg. (2020) – Rechte an Daten, S. 103–121; sowie Specht-Riemenschneider et al. (2021) – Datentreuhand. Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierungserfordernisse für Datentreuhandmodelle, MMR-Beilage, 25.

4 Zu PIMS vgl. u.a. Verbraucherzentrale Bundesverband (2020) – Neue Datenintermediäre. Anforderungen des vzbv an „Personal Information Management Systems“ (PIMS) und Datentreuhänder; edps.europa.eu/sites/default/files/publication/21-01-06_techdispatch-pims_en_0.pdf; Datenethikkommission der Bundesregierung (2019) – Gutachten der Datenethikkommission, S. 133ff.; Stiftung Datenschutz (2017) – Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen (Studie Gesamtfassung); darunter u.a.: Nicola Jentzsch (2017) – Die persönliche Datenökonomie: Plattformen, Datentresore und persönliche Clouds. Ökonomische Rahmenbedingungen innovativer Lösungen zu Einwilligungen im Datenschutz (Gutachten).

erste Erprobungen von Datentreuhandmodellen erfolgten und ausgewertet wurden. Wendy Hall und Jerome Pesenti brachten *data trusts* (Datentreuhänder) durch ihren Bericht „Growing the Artificial Intelligence Industry in the UK" von 2017 ins Gespräch, um Unternehmen, die Künstliche Intelligenz entwickeln, den Zugang zu Daten zu erleichtern.[5] Hierin empfahlen Hall und Pesenti, dass die britische Regierung und die Industrie ein Programm zur Entwicklung von *data trusts* vorlegen sollten, um einen vertrauenswürdigen Austausch von Daten zu gewährleisten. Dieses Konzept, Datentreuhänder einzuschalten, um das Teilen von Daten zwischen Unternehmen/Organisationen zu erleichtern und zu fördern, ist im britischen Diskurs auch mit dem Begriff der *functional data trusts* verbunden.[6] Weitere Impulse in diese Richtung stammen vom britischen Open Data Institute. Datentreuhänder werden als ein mögliches rechtliches Konstrukt verstanden, um das Teilen von Daten vor allem zwischen Unternehmen und Regierungen zu erhöhen und den daraus entstehenden gesellschaftlichen und ökonomischen Wert besser erschließen zu können. Gleichzeitig sollen Datentreuhänder auch die Risiken begrenzen, die beim vermehrten Austausch von Daten auftreten. Datentreuhänder werden definiert als eine rechtliche Struktur zur unabhängigen, treuhänderischen Verwaltung von Daten („a legal structure that provides independent, fiduciary stewardship of data").[7] Das Open Data Institute hat zudem erste Erprobungen von Datentreuhändern, angelegt an drei konkrete Anwendungsbereiche[8], durchgeführt und die Ergebnisse im Jahr 2019 veröffentlicht. Zudem hat es im Rahmen eines Projekts unter Mitwirkung von Pinsent Masons Anregungen hinsichtlich der Gestaltung der Governance-Strukturen von Datentreuhändern gegeben.[9] Hinsichtlich der Diskussion um geeignete Governance-Strukturen wird auch hinterfragt, inwieweit Erfahrungen aus der partizipativen Einbindung der Datengeber bei Biobanken für Datentreuhandmodelle fruchtbar gemacht werden können.[10]

Eine Facette der Diskussion über Datentreuhänder dreht sich unter anderem um Ideen, Individuen darin zu unterstützen, ihr Recht auf informationelle Selbstbestimmung besser durchsetzen zu können. Hiermit ist auch der Begriff der *bottom up data trusts* verbunden. Sylvie Delacroix und Neil D. Lawrence argumentieren in diesem Zusammenhang, dass Datentreuhänder aus drei Gründen ein vielversprechender Ansatz seien.[11] In ihrem Beitrag argumentieren sie, dass Datentreuhänder aus drei Gründen ein vielversprechender Ansatz seien: Erstens seien regulatorische Bestrebungen nicht

---

5 Hall und Pesenti erstellten die unabhängige Begutachtung auf Anfrage des britischen Wirtschafts- und Kulturministeriums; online verfügbar unter: gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk.

6 Kieron o'Hara (2020) – Data Trusts.

7 Jack Hardinges (2020) – Data Trusts. theodi.org/article/data-trusts-in-2020/. Jack Hardinges legt hierin dar, dass die Arbeitsdefinition von 2018 um treuhänderische Pflichten des Datentreuhänders erweitert wurde.

8 ODI (2019) – Data Trusts: Lessons from Three Pilots; docs.google.com/document/d/118RqyUAWP3WIyy-CO4iLUT3oOobnYJGibEhspr2v87jg/edit.

9 Pinsent Masons (2019) – Data Trusts Legal and Governance Considerations; theodi.org/article/data-trusts-legal-report.

10 Richard Milne et al. (2022) – What Can Data Trusts for Health Research Learn from Participatory Governance in Biobanks?, in: Med Ethics 2022;48:323–328, DOI: doi:10.1136/medethics-2020-107020.

ausreichend, um der bestehenden Machtambivalenz entgegenzuwirken, die zwischen Unternehmen, die Daten sammeln (und ihr Geschäftsmodell darauf aufbauen), und Betroffenen bestehen. Aufgrund fehlender rechtlicher Mechanismen kumulierten sich die Risiken für die Datensubjekte bzw. Betroffenen, gänzlich die Kontrolle über ihr „soziales Selbst" (social self) zu verlieren und vielmehr ihrer „maschinenlesbaren Vergangenheit" ausgeliefert zu sein. Dies sei insofern problematisch, als Dritte auf Basis solcher „Datenspuren" weitreichende Entscheidungen wie beispielsweise über Hypothekenanträge fällen. Und drittens könnten Individuen bislang nicht unter Berücksichtigung ihrer Präferenzen zwischen verschiedenen Data-Governance-Ansätzen wählen.[12] Sie zeigen unter anderem anhand verschiedener personenbezogener Daten – darunter medizinischen Daten, Social-Media-Daten und Finanzdaten – auf, worin die Vorteile in der Einschaltung eines Datentreuhänders als neutralem Dritten liegen könnten.[13] Aus ihrer Sicht bestehen Herausforderungen vor allem in Bezug auf geeignete Aufnahme- und Ausstiegsverfahren: Das Interesse an solchen Lösungen könnte in der Bevölkerung zu gering sein, sodass sich die Implementierung schwierig gestalte.

Unter dem Begriff der *civic data trusts* werden Ansätze diskutiert, den Zugriff auf Daten zu ermöglichen oder Daten, die im Kontext von Smart Cities entstehen, im Sinne des Gemeinwohls verfügbar zu machen. In diesem Zusammenhang wird vielfach ein Projekt aus Toronto erwähnt. Nach Ansicht von Kieron o`Hara handele es sich hier nicht um einen Datentreuhänder.[14] In Großbritannien stammen wesentliche Impulse zum Datentreuhänder-Diskurs zudem aus dem Umfeld des Alan Turing Institutes, des Ada Lovelace Instituts sowie der Anwaltskanzlei Pinsent Masons.[15] Das Alan Turing Institute legt den Fokus auf den Beitrag von Datentreuhandlösungen zur Verbesserung des Zugangs zu Trainingsdaten für die Entwicklung Künstlicher Intelligenz.

Im deutschsprachigen Diskurs wird der Begriff des „Datentreuhänders" ebenfalls sehr vielschichtig verwendet und mit zum Teil ganz unterschiedlichen Erwartungen verbunden. Eine Intensivierung des Diskurses um Datentreuhandlösungen lässt sich in Deutschland nahezu zeitgleich beobachten. In der Debatte werden Datentreuhänder häufig im Zusammenhang mit der Verbesserung des Datenaustausches zwischen Unternehmen,[16] der Stärkung von Verbraucherrechten und als Lösungsansatz bestehender Datenzugangsprobleme (u. a. im Bereich Mobilitäts- und Gesundheitsdaten) genannt.

---

11 Vgl. u.a. Sylvie Delacroix; Neil D. Lawrence (2019): Bottom-up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance, in: International Data Privacy Law 9, Nr. 4, S. 236-252. Sylvie Delacroix ist Professorin für Recht und Ethik an der Universität von Birmingham. Neil D. Lawrence ist DeepMind Professor für Maschinelles Lernen an der Universität Cambridge und Senior AI Fellow am Alan-Turing-Institut.

12 Delacroix; Lawrence (2019) – Bottom-up Data Trusts, S. 240.

13 Ebd., S. 248ff.

14 Kieron o'Hara ist Philosoph und Informatiker sowie außerordentlicher Professor im Fachbereich Elektronik und Informatik an der Universität Southampton.

15 Zum Fokus des Alan Turing Institutes auf data trusts: turing.ac.uk/news/can-data-trusts-be-backbone-our-future-ai-ecosystem.

Die Datenethikkommission hat sich in ihrem Gutachten von 2019 ausführlich mit Datenmanagement- und Datentreuhandsystemen, darunter auch PIMS, befasst. Dabei hat sie deutlich auf das Risiko der Fremdbestimmung durch PIMS und unter anderem auf die notwendige Einführung eines Zertifizierungssystems hingewiesen.[17] Mit Diensten zur Einwilligungsverwaltung hat sich beispielsweise auch die Stiftung Datenschutz intensiv auseinandergesetzt.[18] Einen weiteren wesentlichen Ausgangspunkt des Diskurses stellt der Bericht der Kommission Wettbewerbsrecht 4.0 dar. Diese hat in ihrem Bericht vom September 2019 auf das Potenzial von Datentreuhändern verwiesen und hiermit vor allem das Ziel angesprochen, Verbraucherrechte zu stärken und den Datenzugang für Unternehmen zu verbessern.[19] Die Nutzung von Datenmanagement- und Einwilligungssystemen wie PIMS ist aus Sicht der Kommission nicht ausreichend, da hierdurch keine Lösung für die Bedarfe der datennachfragenden Unternehmen geschaffen werde. Daher plädiert sie dafür, eine „neue Form von Datentreuhändern" zu entwickeln. Mit Fokus auf die Perspektive der Verbraucherinnen und Verbraucher wurde das Thema Datentreuhänderschaft zudem in der Veranstaltungsreihe „Zu treuen Händen" der Verbraucherzentrale Nordrhein-Westfalen aufgegriffen.[20]

Es findet sich eine große Breite an Zielvorstellungen und Funktionen, die an Datentreuhänder herangetragen werden.[21] Dies wurde beispielsweise bei der Expertenanhörung deutlich, die am 23. Januar 2020 im Rahmen der Datenstrategie stattfand.[22] So unterstrich Boris Otto, dass Datentreuhänder das Datenteilen zwischen Unternehmen fördern könnten, indem sie als vertrauenswürdige Dritte agieren, zu Datentransparenz beitragen oder auch beim Umgang mit Daten helfen.[23] In der Anhörung wurde ein weiterer Diskursstrang thematisiert. So artikulierte Regina Riphahn, dass Datentreuhänder auch aus Sicht der Wissenschaft und Forschung Potenziale besitzen.[24] Sie könnten unter anderem einen geregelten Zugang zu privatwirtschaftlichen Daten

16 Vgl. das Ergebnisprotokoll des ZVEI-Workshops vom 3.11.2021, zvei.org/themen/ergebnisse-des-zvei-workshops-datentreuhaender-welche-rolle-spielt-er-im-industriellen-kontext. Als Hemmnisse des B2B-Datenteilens werden v.a. fehlende Standards, unterschiedliche Schnittstellen oder Daten-Monetarisierung gesehen. Der Einsatz von Datentreuhändern biete im industriellen Kontext allerdings, wie das Ergebnisprotokoll ausführt, kaum einen Mehrwert.

17 Datenethikkommission der Bundesregierung (2019) – Gutachten der Datenethikkommission, S. 133f.

18 Stiftung Datenschutz (2017) – Neue Wege bei der Einwilligung im Datenschutz.

19 BMWi (2019) – Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft. Bericht der Kommission Wettbewerbsrecht 4.

20 Eine Dokumentation der Veranstaltung ist verfügbar unter: verbraucherforschung.nrw/zu-treuen-haenden-tagungsreihe-datenintermediaere-datentreuhaender-60831.

21 Siehe hierzu Aline Blankertz (2020) – Datentreuhandmodelle.

22 Transkript zur Anhörung im Rahmen der Datenstrategie unter bundesregierung.de.

23 Ebd., S. 25. Boris Otto leitet das Fraunhofer-Institut für Software- und Systemtechnik ISST und ist Inhaber des Lehrstuhls Industrielles Informationsmanagement an der Technischen Universität Dortmund. Zudem ist er in das Projekt Gaia-X involviert, das er seit seiner Entstehung in verschiedenen Rollen begleitet.

24 Regina Riphahn ist Professorin für Statistik und empirische Wirtschaftsforschung an der Friedrich-Alexander-Universität Erlangen-Nürnberg und war von 2014 bis 2020 Vorsitzende des Rates für Sozial- und Wirtschaftsdaten (RatSWD).

ermöglichen und darüber hinaus die Datenverknüpfbarkeit verbessern.[25] Die von der Europäischen Kommission eingesetzte High-Level Expert Group hat in ihrem Bericht 2020 dargelegt, dass vor allem Strukturen und Anreize fehlen, um die Potenziale des B2G-Datenaustausches auszuschöpfen.[26] Die Expertengruppe hat daher als Empfehlung formuliert, dass öffentliche Stellen wie private und zivilgesellschaftliche Positionen für *data stewards* einrichten sollen. Ebenso sollte die Europäische Kommission hier fördernd tätig werden und prüfen, mit Blick auf die Weiterverwendung von privatwirtschaftlichen Daten einen EU-Rechtsrahmen zu schaffen. Zudem sollten nach Ansicht der Expertengruppe Kooperationen zum B2G-Datenaustausch in Pilotprojekten *(sandboxes)* erprobt werden.[27]

In der Datenstrategie der Bundesregierung, die im Januar 2021 veröffentlicht wurde, wird entsprechend ein breites Feld an Ausgestaltungsmöglichkeiten aufgezeigt.[28] Dies betrifft das Ziel der Nutzung (u.a. zur Stärkung der Verbraucherrechte, zur Erleichterung des Zugangs zu privatwirtschaftlichen Daten) als auch die mögliche Trägerschaft/ Rechtsform einer Datentreuhand (privatwirtschaftlich, gemeinnützig, genossenschaftlich oder staatlich). Angekündigt wird hierin unter anderem, einen Rechtsrahmen für PIMS zu schaffen sowie Forschungsdatenzentren weiter auszubauen. Zunächst sollen Datentreuhänder laut Datenstrategie projektförmig erprobt werden. Entsprechend zielt eine im Januar 2021 veröffentlichte Förderrichtlinie des BMBF auf eine solche Erprobung von Datentreuhandmodellen.[29] Die geförderten 18 Projekte decken ein breites Anwendungsspektrum ab. Sie reichen von Projekten zur besseren Nutzbarmachung medizinischer Daten und Mobilitätsdaten bis hin zu Umwelt-, Forst- und Landwirtschaftsdaten.[30]

Zur Bundestagswahl 2021 wurde in einigen Wahlprogrammen ebenfalls auf das Potenzial von Datentreuhändern Bezug genommen.[31] Das Zielvorhaben, Datentreuhänder aufzubauen, findet sich auch im Koalitionsvertrag der Ampelfraktionen von 2021. So beabsichtigt die Bundesregierung, Datentreuhänder neben anderen Instrumenten zur Verbesserung der Datennutzung „gemeinsam mit Wirtschaft, Wissenschaft und

25 Transkript zur Anhörung im Rahmen der Datenstrategie, S. 26.
26 Ebd., S. 31ff.
27 High-Level Expert Group on Business-to-Government Data Sharing (2020) – Towards a European Strategy on Business-to-Government Data Sharing for the Public Interest, digital-strategy.ec.europa.eu/en/news/commission-appoints-expert-group-business-government-data-sharing.
28 Bundesregierung (2021) – Datenstrategie der Bundesregierung. Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, bundesregierung.de/breg-de/suche/datenstrategie-der-bundesregierung-1845632.
29 bmbf.de/bmbf/shareddocs/bekanntmachungen/de/2021/01/3292_bekanntmachung.html.
30 Überblick über die geförderten Projekte: bildung-forschung.digital/digitalezukunft/de/technologie/daten/datentreuhandmodelle_pilotvorhaben/datentreuhandmodelle_pilotvorhaben_node.html.
31 S. Bundestagswahlprogramm der SPD sowie der Partei Bündnis 90/die Grünen, spd.de/fileadmin/Dokumente/Beschluesse/Programm/SPD-Zukunftsprogramm.pdf, https://cms.gruene.de/uploads/documents/Wahlprogramm_DIE_GRUENEN_Bundestagswahl_2021.pdf.

Zivilgesellschaft auf den Weg zu bringen."[32] Hiermit sind auch Pläne verknüpft, in Deutschland ein Dateninstitut zu gründen. Dies soll die Aufgabe wahrnehmen, Datentreuhandmodelle und auch die Datenverfügbarkeit und -standardisierung voranzutreiben.[33] In den Diskurs um Datentreuhänder haben sich unter anderem auch die Bundesdruckerei, der Deutsche Dialogmarketingverband (DDV), die Konrad-Adenauer-Stiftung, die Stiftung Datenschutz und die Verbraucherzentrale mit unterschiedlichen Akzenten eingebracht.[34]

Neben Überlegungen zum Aufbau geeigneter Geschäftsmodelle und möglicher Anwendungsbereiche wird die Frage gestellt, wie Datentreuhänder juristisch fundiert werden können. So hat sich in den letzten Jahren ein rechtswissenschaftlicher Diskurs entwickelt, inwieweit Datentreuhänder in der bestehenden Rechtslage überhaupt ausgestaltet werden können oder gegebenenfalls auch Anpassungen der Datenschutz-Grundverordnung (DSGVO) notwendig sind.[35] In diesem Zusammenhang wurde vielfach dargelegt, dass Rechtsunsicherheit vor allem in Bezug auf die Einspeisung von Daten in die Datentreuhand und deren Verarbeitung besteht. Entsprechend wird die Einführung von Erlaubnistatbeständen vorgeschlagen, um Datentreuhänder rechtssicher aufbauen zu können. Wie Michael Funke aufzeigt, lassen sich Datentreuhänder auf unterschiedliche Weise begründen, im Sinne einer Rechtsübertragung oder einer Stellvertretung.[36] In der aktuellen Rechtslage ist die Schaffung von Datentreuhändern *(data trusts)*, wie das Gutachten von Michael Funke darlegt, zwar möglich, aber mit Risiken verbunden. Ein Lösungsansatz könnte darin bestehen, in der Datenschutz-Grundverordnung ausdrücklich die Möglichkeit einer Stellvertretung zu adressieren, und zwar umfasse dies die Ebene der Erlaubnistatbestände (Art. 6 DSGVO), die Ebene der Betroffenenrechte (Art, 12 ff.) und der gerichtlichen Geltendmachung (Art. 77–79 DSGVO). Sinnvoll sei auch eine Stellungnahme des Europäischen Datenschutzausschusses zur Frage der Stellvertretung.[37] Eine weitere Möglichkeit, Datentreuhänder rechtssicher aufbauen zu können, bestehe darin, eine neue rechtliche Position einzuführen. So könnte in der DSGVO neben Verantwortlichem und Auftragsverarbeiter eine Rolle vorgesehen werden, die die Rechte Dritter wahrnehmen könnte.[38]

---

32 Koalitionsvertrag 2021–2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), BÜNDNIS 90 / DIE GRÜNEN und den Freien Demokraten (FDP), S. 17.

33 Inzwischen liegen hierzu erste Empfehlungen der Gründungskommission vor, bmi.bund.de/SharedDocs/pressemitteilungen/DE/2022/12/dateninstitut.html.

34 S. u.a. Webtalk des DDV, ddv.de/aufzeichnung-webtalk-datentreuhaender-modelle.html; Vortragsreihe „Zu treuen Händen" der Verbraucherzentrale Nordrhein-Westfalen, Beiträge können heruntergeladen werden unter: verbraucherforschung.nrw/zu-treuen-haenden-tagungsreihe-datenintermediaere-datentreuhaender-60831.

35 Siehe u.a. Michael Funke (2020) – Die Vereinbarkeit von Data Trusts mit der Datenschutzgrundverordnung (DSGVO), algorithmwatch.org/de/gutachten-data-trusts-dsgvo/; Jürgen Kühling; Florian Sackmann; Hilmar Schneider (2020) – Datenschutzrechtliche Dimensionen Datentreuhänder. Kurzexpertise im Auftrag des Bundesministeriums für Arbeit und Soziales.

36 Michael Funke ist Fachanwalt für Informationstechnologierecht und für die Kanzlei JBB Rechtsanwälte tätig.

37 Funke (2020) – Die Vereinbarkeit von Data Trusts, S. 29.

38 Ebd.

Auch wurde über die notwendige Regulierung und die Schaffung eines geeigneten, auch EU-weiten Rechtsrahmens hinsichtlich der Entstehung dieser neuen Intermediäre diskutiert. Unter anderem wurde seitens Louisa Specht-Riemenschneider und Aline Blankertz ein risikobasierter Regulierungsansatz vorgeschlagen, der sich an vier Grundmodellen der Datentreuhand orientiert.[39] Berücksichtigt werden sollte demnach, inwieweit die Datenhaltung zentral beim Datentreuhänder oder dezentral erfolgt sowie ob der Datentreuhänder freiwillig oder obligatorisch genutzt wird.[40] Demgegenüber hat die EU mit dem Data Governance Act (DGA) eine Rechtsverordnung auf den Weg gebracht, die einen horizontal angelegten Ansatz wählt und Rahmenbedingungen für Datenintermediäre schafft. Kritikpunkte am DGA bezogen sich vor allem darauf, dass dieser zu wenig Anreize für potenzielle Anbieter setze, Geschäftsmodelle aufzubauen und sich auf dem Markt zu etablieren. Als ein weiterer Aspekt, der sich hinderlich auf den Aufbau von Datentreuhändern auswirkt, wurden die großen Haftungsrisiken adressiert, die auf Datentreuhänder zukommen.[41] Dies bezieht sich auf drohende Bußgelder bei datenschutzrechtlichen Verstößen als auch auf die Geltendmachung von Schadensersatzansprüchen.[42]

Angesichts der nach wie vor bestehenden rechtlichen, aber auch technischen Herausforderungen und der Frage nach geeigneten Geschäftsmodellen zielt eine weitere im Januar 2023 veröffentlichte Förderrichtlinie des BMBF auf die „Erforschung oder Entwicklung praxisrelevanter Lösungsaspekte („Bausteine“) für Datentreuhandmodelle“.[43]

Ausführliche Überlegungen zum Einsatz von Datentreuhändern und erste Pilotprojekte finden sich für verschiedene Anwendungsbereiche. Diese stehen u.a. im Zusammenhang mit der BMBF-Förderrichtlinie zur Erprobung von Datentreuhandmodellen sowie dem Gaia-X-Förderwettbewerb des BMWK. Beispielhaft werden kurz einige Datentreuhänderansätze für Medizin-, Mobilitätsdaten sowie Finanzdaten dargelegt:[44]

---

39 Aline Blankertz; Louisa Specht-Riemenschneider (2021) – Neue Modelle ermöglichen. Regulierung für Datentreuhänder. Louisa Specht-Riemenschneider ist Inhaberin des Lehrstuhls für Bürgerliches Recht, Informations- und Datenrecht (seit 2023 umbenannt in Lehrstuhl für Bürgerliches Recht, Recht der Datenwirschaft, des Datenschutzes, der Digitalisierung und der Künstlichen Intelligenz) und Vorstandsvorsitzende der Forschungsstelle für Rechtsfragen neuer Technologien sowie Datenrecht (ForTech). Aline Blankertz ist Ökonomin, wirtschaftswissenschaftliche Beraterin und war u.a. als Leiterin des Projekts „Datenökonomie“ bei der Stiftung Neue Verantwortung tätig.

40 Ebd., S. 5f.

41 Kühling et al. (2020) – Datenschutzrechtliche Dimensionen Datentreuhänder, S. 52.

42 Ebd.

43 bmbf.de/bmbf/shareddocs/bekanntmachungen/de/2023/01/2023-01-20-Bekanntmachung-Datentreuhandmodelle.html.

44 Siehe u.a. Louisa Specht-Riemenschneider; Wolfgang Kerber (2022) – Designing Data Trustees – A Purpose-Based Approach.

Medizindaten

Im Bereich der Medizindaten bestehen zahlreiche nationale Entwicklungen zur Verbesserung des Datenzugangs bzw. Datenteilens für Wissenschaft und Forschung, u. a. vorangebracht durch die Medizininformatik-Initiative, aber auch durch privatwirtschaftliche Projekte wie z. B. Honic.[45] Ein Hindernis des Datenteilens stellen u. a. die Rechtsunsicherheit bei der Verknüpfung von Datensätzen sowie uneinheitliche Normen und Spezifikationen für die Speicherung und den Austausch von Daten dar.[46]

Auch liegen viele Gesundheitsdaten nicht digital vor. Bestrebungen gehen in die Richtung, unter anderem die Interoperabilität, die Auffindbarkeit von Daten in den verschiedenen Registern, die rechtlichen Rahmenbedingungen durch die Harmonisierung der Landeskrankenhausgesetze und den Aufbau (fachspezifischer wie interdisziplinär ausgerichteter) Plattformen, Datenräumen bzw. Infrastrukturen zu verbessern:

Durch die im Rahmen der Medizininformatik-Initiative gegründeten Datenintegrationszentren werden beispielsweise Forschungs- und Versorgungsdaten der deutschen Universitätsklinika erschlossen und zugänglich gemacht.[47] Zudem entsteht das Forschungsdatenzentrum Gesundheit am Bundesinstitut für Arzneimittel und Medizinprodukte, das der Wissenschaft und Forschung den Zugang zu Abrechnungsdaten aller gesetzlich Krankenversicherten in Deutschland ermöglichen soll.[48] Ein spezifisches Beispiel zur besseren Vernetzung und Auswertung medizinischer Daten stellt das Molekulare Tumorboard an der Universitätsklinik Freiburg dar, das als „Datenraum“ zur interdisziplinären Auswertung von Daten und Erschließung personalisierter Therapiemöglichkeiten dienen soll.[49] Darüber hinaus gibt es Projekte, die auf die Verbindung von Daten aus dem primären und sekundären Gesundheitssektor zielen, darunter Honic und HEALTH-X dataLOFT. Unter Förderung des BMWK konzipiert das Gaia-X-Projekt HEALTH-X dataLOFT einen „Gesundheitsdatenraum“.

Auf europäischer Ebene schreiten die Vorbereitungen im Aufbau des European Health Data Space (EHDS) weiter voran. Ziel des EHDS ist es, einen Datenraum zu schaffen, um die Primär- als auch Sekundärnutzung von Gesundheitsdaten zu erleichtern. Darüber hinaus streben fachspezifische Projekte einen länderübergreifenden und leichteren Zugang zu Gesundheitsdaten an, wie zum Beispiel die europaweite Datenbank zu bildgebenden Daten zum Zwecke der Krebsforschung.[50]

---

45 Honic strebt den Aufbau einer Plattform zur Verfügbarmachung von Versorgungsdaten mittels eines Datentreuhänders und zur Verknüpfung verschiedener Datenbestände an. Laut Tagesspiegel Background sollten im Oktober 2022 Forschungsprojekte starten. Die Bundesdruckerei ist hier als Datentreuhänder beteiligt; honic.eu/de/.

46 S. u.a. Beiträge und Diskussion auf der vom Digital Health Hub Greifswald organisierten Veranstaltung „EHDS, MII, THS & DIZ – Leicht erklärt. Gesundheitsdaten für die Versorgung nutzbar machen“, 18.08.2022; Video unter: youtube.com/watch?v=PA7RHCfpxxU.

47 medizininformatik-initiative.de/de/konsortien/datenintegrationszentren.

48 Das FDZ Gesundheit befindet sich aktuell noch im Aufbau; bfarm.de/DE/Das-BfArM/Aufgaben/Forschungsdatenzentrum/_node.html, https://www.forschungsdatenzentrum-gesundheit.de.

49 aerztezeitung.de/Medizin/Uniklinik-Freiburg-und-Roche-haben-gemeinsamen-Datenraum-im-Visier-422784.html.

Als ein Lösungsansatz in Bezug auf Datenzugangsprobleme im Bereich der Medizindaten wird auch die Nutzung von neuen Intermediären in Form von Datentreuhändern in Erwägung gezogen. So wird unter anderem diskutiert, hierdurch Datenzugangsmöglichkeiten zu bestehenden Registern zu erweitern als auch Erleichterungen im Bereich der Datenspende zu erreichen (ggf. über die elektronische Patientenakte).[51] Ein Vorschlag setzt dabei auf das Zusammenwirken von europäischen/nationalen Koordinierungsstellen, die Datenzugangsanträge abwickeln, sowie flexiblen Datentreuhandstrukturen, die eine Datenteilungs- und Datenspendefunktion übernehmen könnten.[52] Um dies rechtssicher umsetzen zu können, schlagen Louisa Specht-Riemenschneider und Wolfgang Kerber eine datenschutzrechtliche Verantwortlichkeitszuweisung vor sowie eine „Klärung der datenschutzrechtlichen Verarbeitungsgrundlage zur Einspeisung von Daten in die Treuhand und zur Datenverarbeitung in der Treuhand". Diese soll in Form einer Erlaubnisnorm umgesetzt werden können.[53]

Zu Medizindaten laufen zudem mehrere Projekte im Zusammenhang mit der BMBF-Förderrichtlinie zur Erprobung von Datentreuhändern, darunter Entwicklung und Erprobung von Datentreuhandmodellen am Beispiel der verteilten künstlichen Intelligenz in der Medizin (TreuMed), Datentreuhandverbund biomedizinische Forschungsdaten Land Sachsen-Anhalt (DaTHMed-LSA), GesundheitsDAtentreuhand-Reallabor zur Entwicklung und Erprobung der Ökosystemintegration datengetriebener Gesundheitsforschung (DaRE), Datenschutzrechtliches Reallabor für eine Datentreuhand in der Netzwerkmedizin (TrustDNA), Vertrauenswürdiges Datentreuhandmodell zur souveränen Verwaltung und effektiven Nutzung von medizinischen Daten in der Schlafforschung (SouveMed). Die Projekte sind meist auf die Verfügbarmachung von Daten bestimmter Fachbereiche ausgerichtet (wie Daten aus der Radiologie oder Schlafforschung), aber beispielsweise auch auf den Zugang zu verschiedenen medizinischen Datenbanken. Neben der Konzeption eines Datentreuhandmodells werden Schwerpunkte beispielsweise auf die Einbindung von Patientinnen und Patienten oder auch die Datenqualität gelegt.

50 euractiv.de/section/gesundheit/news/eu-kommission-will-kampf-gegen-krebs-mit-neuer-datenbank-vorantreiben/.
51 Specht-Riemenschneider; Kerber (2022) – Designing Data Trustees, S. 44f.
52 Ebd.
53 Ebd. Wolfang Kerber ist Professor für Wirtschaftspolitik an der Philipps-Universität Marburg.

Erprobung von Datentreuhändern im Bereich Medizindaten: Projektziele

Das Projekt TreuMed zielt auf die Entwicklung einer technischen Lösung, das den Umgang mit Datenschutzanforderungen in Bezug auf Patientendaten erleichtern soll. Es handelt sich um ein „Ampelsystem für Datentreuhänder", das je nach Identifizierbarkeit der Patientendaten verschiedene Privacy-Ebenen und Schutzvorkehrungslevel anzeigte. Diese Lösung soll am Beispiel der „verteilten künstlichen Intelligenz" im Bereich der molekularen Epidemiologie und der Biomarkerforschung erprobt werden. Es handelt sich um ein Gemeinschafts-Projekt von der Universität Hamburg und der Universität Greifswald unter Beteiligung der ePrivacy GmbH.

Beim Projekt DaTHMed-LSA geht es um den Aufbau einer standortübergreifenden Datentreuhandstelle in Sachsen-Anhalt, die einen Zugang zu verschiedenen medizinischen Datenbanken über ein Web-Portal gewährleisten soll. Im Rahmen des Projekts wird unter anderem ein neues Herzinfarktregister erstellt. Die Universität Magdeburg und die Universität Halle-Wittenberg setzen dieses Projekt um.

Das Projekt DaRE konzipiert ein Datentreuhandmodell für medizinische Daten am Beispiel der Radiologie. In den Fokus wird unter anderem die Einbindung von Patientinnen und Patienten in die Datenfreigabe gerückt. Das Datentreuhandmodell soll in einem Reallabor durchgeführt und evaluiert werden. Beteiligt sind an diesem Projekt das Fraunhofer-Institut für Software- und Systemtechnik ISST, das Fraunhofer-Zentrum für Internationales Management und Wissensökonomie, die Universität Bonn sowie die Universitätsklinik Bonn.

Auf Daten aus der Netzwerkmedizin ist das Projekt TrustDNA ausgerichtet. So sollen Daten aus dem Deutschen Netzwerk für angewandte Präzisionsmedizin für nationale und internationale Initiativen wie das Europäische Humangenom-Phenomarchiv verfügbar gemacht werden. Das Projekt entwickelt ein Datentreuhandmodell, das eine Einbindung der Patientinnen und Patienten in Forschungsvorhaben vorsieht. Es wird geleitet durch die Universität Heidelberg in Zusammenarbeit mit dem European Molecular Biology Laboratory und der Charité-Universitätsmedizin Berlin.

Das Projekt SouveMed des FZI Forschungszentrums Informatik, des Universitätsklinikums Freiburg und der Hochschule für Technik und Wirtschaft strebt ein Datentreuhandmodell zur Verwaltung und Nutzung von medizinischen Daten in der Schlafforschung an. Darüber hinaus sollen die Datenqualität erhöht und Anreizmechanismen zur Steigerung der Teilnahme von Patientinnen und Patienten evaluiert werden.

Privatwirtschaftliche Daten

Die Datenstrategie der Bundesregierung hat die Anwendung von Datentreuhändern als einen Lösungsansatz formuliert, um den B2B-Datenaustausch zu fördern. Angesichts der sektorspezifischen Bedarfe und Herausforderungen des Datenteilens wird die Anwendung verschiedener, flexibler Datenteilungsmodelle als sinnvoll eingeschätzt.[54] In Bezug auf das Teilen von Daten zwischen Unternehmen gilt die Fähigkeit der Unternehmen, überhaupt am Datenaustausch mitwirken zu können (Stichwort Data Readiness), als eine wesentliche Herausforderung. Ebenso wird die Notwendigkeit betont, Anreize für Unternehmen zu schaffen, Daten mit anderen zu teilen. Einige,

54 S. u.a. Ergebnisprotokoll ZVEI-Workshop.

allerdings laut einer Studie des BMWK nur wenige und meist größere Unternehmen, nutzen bereits B2B-Plattformen, um Daten zu teilen, während ein Großteil gar keine Möglichkeiten hierfür sieht.[55] Darüber hinaus werden Potenziale von Datenmarktplätzen erschlossen, um den Datenaustausch zwischen Unternehmen zu erhöhen.[56] Auch laut einer Umfrage des Verbands Bitkom teilen lediglich 8 Prozent der deutschen Unternehmen (Stand Mai 2022) ihre Daten mit anderen und setzen ebenfalls die Daten anderer ein.[57] Als ein wesentliches Hemmnis geben Unternehmen mangelnde Kompatibilität in Bezug auf die Daten sowie die Rechtsunsicherheit an.[58]

Um Voraussetzungen für das Datenteilen zu verbessern, ist u.a. die Standardisierung von Datenformaten und Schnittstellen wichtig, aber auch Maßnahmen zur Stärkung des Vertrauens in das Datenteilen.[59] Wie die Studie im Auftrag des BMWK darlegt, sollten angesichts der EU-Rechtsetzungsvorhaben weitere Regulierungsinitiativen nur mit Vorsicht angegangen werden, um nicht die Komplexität zu erhöhen oder gar Inkohärenzen zwischen den verschiedenen Rechtstexten und Unsicherheiten seitens der Unternehmen zu evozieren. Auch sollten sektorspezifische Regelungen nur bei Vorliegen eines Marktversagens erfolgen. Zentral sei, dass die Regulierungen aufgrund des sich erst im Entstehen begriffenen Markts für das Teilen von Daten sowohl Reflexivität als auch Agilität aufweisen, um je nach Marktentwicklung auch Anpassungen vornehmen zu können.[60] Empfohlen wird der Einsatz regulatorischer „Sandkästen" vor allem in sektorspezifischen Kontexten, bevor ein horizontaler Rechtsrahmen geschaffen wird. In Bezug auf Datenintermediäre sollten einerseits die Auswirkungen des DGA analysiert und ggf. Verbesserungen an der Rechtsverordnung vorgeschlagen werden. Auch sollten die EU-Gesetzgeber, die nationalen Gesetzgeber und die Wettbewerbsbehörden darauf hinwirken, Datenschutzvorschriften zur „wirksamen Integration von Datenmittlern in die Marktordnung für die gemeinsame Nutzung von Daten" zu entwerfen.

Der Zugang der Wissenschaft und Forschung zu privatwirtschaftlichen Daten gestaltet sich meist schwierig, da geregelte Zugänge fehlen und Zugangsbedingungen meist einzeln ausgehandelt werden.[61] Initiativen wie das Projekt Fair Data Spaces erschließen dabei Möglichkeiten, den Datenaustausch zwischen Wirtschaft und Wissenschaft

55 Heike Schweitzer et al. (2022) – Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy. A legal, economic and competition policy angle, S. 4.

56 S. u.a. Bundesministerium für Wirtschaft und Energie (2020) – Datenmarktplätze in Produktionsnetzwerken (Impulspapier der Arbeitsgruppe „Digitale Geschäftsmodelle" der Plattform Industrie 4.0).

57 bitkom.org/Presse/Presseinformation/Unternehmen-oeffnen-sich-Datenoekonomie.

58 Ebd.

59 Schweitzer et al. (2022) – Data access and sharing in Germany and in the EU.

60 Ebd., S. 303f.

61 RatSWD (2019) – Big Data in den Sozial-, Verhaltens- und Wirtschaftswissenschaften: Datenzugang und Forschungsdatenmanagement. RatSWD Output 4 (6), DOI: 10.17620/02671.39. Vgl. allgemein zu den Herausforderungen im Hinblick auf den B2G-Datenaustausch u.a. High-Level Expert Group (2020) – Towards a European strategy on business-to-government data sharing.

durch den Aufbau eines Datenraumes und der Gestaltung klarer rechtlicher Rahmenbedingungen zu erleichtern.

Das Projekt MANDAT

Im Rahmen des BMBF-geförderten Projekts MANDAT (Methoden zum Austausch von unternehmensbezogenen Daten in treuhänderbasierten Datenökosystemen), das gemeinsam von der Friedrich-Alexander-Universität Erlangen-Nürnberg, dem Karlsruher Institut für Technologie KIT und der DATEV eG geleitet wird, soll ein dezentral aufgebautes Datenökosystem zum Austausch von Unternehmensdaten entwickelt werden. Das Projekt baut auf offenen Standards auf.

Mobilitäts- bzw. Fahrzeugdaten

Im Hinblick auf Mobilitätsdaten finden sich zahlreiche Ansätze zur Verbesserung des Datenaustauschs, darunter u.a. die durch Unternehmen der Automobilindustrie getriebene Initiative Catena-X[62], die inzwischen als Verein organisiert ist, sowie Projekte zum Aufbau eines deutschen Datenraums Mobilität. Darüber hinaus strebt die EU die Gründung des European Mobility Data Space an. Die Zugangsmöglichkeiten zu bestimmten Daten, wie im Kontext des vernetzten bzw. automatisierten Fahrens, gestalten sich allerdings je nach Akteursrolle unterschiedlich. Zwischen den verschiedenen Akteuren zeichnen sich in Bezug auf Fahrzeugdaten seit Jahren Konflikte um deren Zugang und Weiterverwendung ab.

In diesem Zusammenhang stehen sich verschiedene Konzepte gegenüber. Aus den Reihen der Fahrzeughersteller wurde das Nevada- bzw. Adaxo-Konzept entwickelt, das auch als Extended Vehicle-Konzept bezeichnet wird.[63] Dies sieht die Übertragung der im Kontext des vernetzten Fahrens generierten Daten an einen Server der Hersteller vor.[64] Dies bedeutet, dass die Kontrolle über den Zugang zu diesen Daten bei den Herstellern verbleibt, welches beispielsweise bei der Aufklärung von Unfällen problematisch sein kann.[65] Kritik an diesem Konzept äußerten unter anderem Versicherungsunternehmen und Verbraucherschützer.[66] Der Gesamtverband der Deutschen Versicherungswirtschaft hat in seinem Positionspapier vom August 2018 bereits die Schaffung eines Datentreuhänders vorgeschlagen, und zwar zusammen mit der Politik, Verwaltung und mehreren Stakeholdern. Eingefordert wird eine stärkere Kontrolle der Fahrzeugnutzer über die erzeugten Daten als auch Regelungen, die weiteren Beteilig-

62 catena-x.net/de/ueber-uns/rolle-des-vereins.
63 Siehe u.a. Verband der Automobilindustrie (2022) – Adaxo: Automotive Data Access – Extended and Open. VDA-Konzept für den Zugriff auf fahrzeuggenerierte Daten.
64 Siehe u. a. Specht-Riemenschneider; Kerber (2022) – Designing Data Trustees, S. 59ff.
65 Ebd.
66 U.a. Tibor Pataki (2021) – Autonomes Fahren und Datentransfer, in: DAR 2021/ Heft 9, S. 481f.; Tibor Pataki (2016) – Die automobile Revolution gelingt nur gemeinsam, Kommentar online verfügbar unter: versicherungsbote.de/id/4847410/Automobile-Revolution-gelingt-nur-gemeinsam/.

ten (u.a. Werkstätten) einen ungehinderten Datenzugang ermöglichen. In diesem Zusammenhang wird auch der Einsatz von Datentreuhandlösungen diskutiert.[67]

Ein Lösungsansatz in Bezug auf den Zugang zu Fahrzeugdaten setzt dabei auf die Verbindung von Datentreuhandstrukturen und dem Einsatz von Personal Management Systems (PIMS). So empfiehlt der Verbraucherzentrale Bundesverband (vzbv) eine Datentreuhand sowie einen Mobilitätsdatenwächter einzuführen, der als „Autorisierungsstelle" fungieren solle.[68] Nach diesem Konzept würde der Fahrzeughalter Festlegungen über die Weitergabe der Daten treffen, die in einem vom Mobilitätsdatenwächter betriebenen PIMS hinterlegt werden. Der vzbv schlägt eine Aufgabentrennung zwischen Datenwächter und Datentreuhand vor, sodass der Datenwächter über Art und Umfang der Weiterverwendung der Daten entscheide, aber keinen physischen Zugang zu den Daten besitze. Hierüber verfüge nur der Datentreuhänder.[69]

Die Projekte TreuMoDa und MobiDataSol

Im Kontext des autonomen Fahrens wird zurzeit ein Datentreuhänder entwickelt und erprobt, der als „gemeinnützige Schnittstelle" Daten aus dem Bereich des autonomen Fahrens für Wissenschaft, Wirtschaft und Gesellschaft nutzbar machen soll. Es handelt sich um das vom BMBF-geförderte Projekt TreuMoDa (Konzeptionierung und prototypische praxisnahe Erprobung einer Treuhandstelle für Mobilitätsdaten im Anwendungsfeld Automatisiertes Fahren unter Nutzung des Testfelds für Autonomes Fahren Baden-Württemberg). Das Projekt wird durchgeführt vom Karlsruher Institut für Technologie in Kooperation mit dem Forschungszentrum Informatik (FZI) und dem FIZ Karlsruhe.

Auf die Verfügbarmachung von Mobiliätsdaten (und auch Umweltdaten) auf kommunaler Ebene zielt beispielsweise das Projekt MobiDataSol (Intelligente Datenprodukte für die Urbane Mobilitätswende mittels Ökosystem Data Governance in der Smart City Solingen), das von der Stadt Solingen und der Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., der Universität Stuttgart und dem Institut für Energie- und Umweltforschung (ifeu) ausgeführt wird.

Finanzdaten

Ein konkretes Anwendungsbeispiel eines Datentreuhänders, das sich nicht unter dem Dach des BMBF, sondern für das GAIA-X-Ökosystem in der Erprobung befindet, ist das vom BMWK geförderte Projekt EuroDaT. Dieses Projekt im Rahmen des Gaia-X-Förderwettbewerbs konzentriert sich auf die Entwicklung eines Datentreuhänders zur

67 Specht-Riemenschneider und Kerber zeigen die Vorteile von Datentreuhandstrukturen gegenüber dem Extended Vehicle-Konzept und dem Zugang zu Daten unter FRAND-Bedingungen auf. Diese liegen ihrer Ansicht nach v. a. in der Unfallaufklärung als auch einem Datenzugang für öffentliche Stellen sowie für Wissenschaft und Forschung. Specht-Riemenschneider; Kerber: Designing Data Trustees; Verbraucherzentrale Bundesverband (2021) – Fahrerlos alle mitnehmen.

68 Verbraucherzentrale Bundesverband (2022) – Mobilitätsdatenwächter – Digitale Privatheit bei vernetzten Fahrzeugen für alle Verbraucher:innen gewährleisten. Positionspapier des Verbraucherzentrale Bundesverbands (vzbv) zu einem verbrauchergerechten und fairen Zugang zu Fahrzeugdaten.

69 Ebd., S. 9.

Nutzung und Verwendung von Finanzdaten. Hiermit verbunden sind Überlegungen zum Konzept der transaktionsbasierten Datentreuhand. Dieses Modell zielt zunächst auf Verbesserungen der Analyse von Kreditinstituten zur Geldwäscheverdachtserkennung, die Anwendungsmöglichkeiten können aber auch darüber hinausreichen.[70] Der Datentreuhänder stellt nach diesem risikominimierenden Ansatz keine Daten zur Verfügung, sondern nur Ergebnisse der Datenauswertung in geschützter Umgebung. Der Datentreuhänder hält die Daten demnach nicht physisch vor, er fordert diese nur punktuell an, verknüpft diese und wertet sie aus.

Use Cases des EuroDat-Projekts

Im Rahmen des Projekts EuroDat werden vier Use Cases umgesetzt: zur föderativen Erkennung von Betrug und Finanzkriminalität, zu Sustainable Finance, zum Haushaltsbarometer sowie zur Bereitstellung von Daten zu Forschungszwecken. So soll ein standardisierter Zugang zu Mikrodaten geschaffen werden, die der wirtschaftswissenschaftlichen Forschung häufig nur eingeschränkt zur Verfügung stehen und insbesondere zur Evaluierung von Verteilungswirkungen geldpolitischer Maßnahmen benötigt werden. Das Projekt zielt auch darauf, anonymisierte Datenanalysen zu ermöglichen, die zur Entwicklung neuer Geschäftsmodelle beitragen.

70 Johannes Buchheim; Steffen Augsberg; Petra Gehring: Transaktionsbasierte Datentreuhand. Nutzungsszenarien, Kennzeichen und spezifische Leistungen eines neuen Modells gemeinsamer Datennutzung, in: JZ 23/2022, S. 1139–1147.

3 ERGEBNISSE

Die AG Datentreuhänderschaft des RfII hat die in Kapitel 2 skizzierte Diskussion um Datentreuhandlösungen aufmerksam verfolgt und hierin eigene Akzente gesetzt, die insbesondere folgende vier inhaltliche Aspekte umfassen:

Anreize zum Aufbau von Datentreuhändern fördern

Der bereits in Kraft getretene Data Governance Act (DGA) der EU setzt die Rahmenbedingungen für den Aufbau von „Datenvermittlungsdiensten", darunter auch für – altruistisch wie nicht-altruistisch ausgerichtete – Datentreuhänder. Aus Sicht der AG Datentreuhänderschaft sollten auf europäischer wie nationaler Ebene weitere Maßnahmen erfolgen, die neben den rechtlichen Anforderungen auch auf die Förderung von Anreizen zur Erprobung und zum Aufbau von Datentreuhändern setzen. Hinsichtlich der Finanzierbarkeit von Datentreuhändern stellt sich aufgrund der Neutralitätsverpflichtung laut DGA die Frage, wie Datentreuhänder nachhaltig aufgebaut und genutzt werden können. So ist aus Sicht der AG ggf. auch der Einsatz öffentlicher Fördergelder in als prioritär erachteten Anwendungsfeldern zu erwägen.

Datentreuhänder rechtssicher ausgestalten

In Bezug auf die vielfach angesprochene Rechtsunsicherheit bei der Ausgestaltung von Datentreuhändern (u. a. hinsichtlich der Übertragung von Entscheidungskompetenzen zum Datenzugriff Dritter gemäß DSGVO) sollten Bemühungen in Richtung einer Harmonisierung der Rechtsauslegung seitens der Aufsichtsbehörden und Prüfungen weiterer rechtlicher Klarstellungen bzw. Anpassungen erfolgen. Als wesentlich erachtet die AG Datentreuhänderschaft in diesem Zusammenhang die Adressierung und Klärung von Haftungsfragen. Auch ließe sich in zukünftigen Rechtsetzungsinitiativen auf nationaler Ebene (u. a. Mobilitätsdatengesetz, Gesundheitsdatennutzungsgesetz) ggf. prüfen, inwieweit Fragen der Haftung beim Einsatz von Datentreuhandlösungen hierin adressiert werden können.

Qualitätssicherung stärken

In ihren Arbeiten hat die AG Datentreuhänderschaft wiederholt vorgeschlagen, neben der Berücksichtigung der FAIR-Prinzipien erweiterte Maßnahmen der Qualitätssicherung vorzusehen, und zwar in Bezug auf den Aufbau von Datentreuhändern (beispielsweise durch die Einführung geeigneter Zertifizierungsverfahren bzw. eines Labels) als auch die Daten selbst betreffend. So wäre es aus Sicht der AG förderlich, wenn der Datentreuhänder zumindest Informationen über die Qualität der Daten vorhält, zu denen er Zugang vermittelt. In weiteren (u.a. sektorspezifischen) Rechtsetzungsinitiativen seitens der EU, z. B. im Zusammenhang mit den European Data Spaces, aber auch der späteren Evaluierung zentraler Regulierungsansätze wie des DGA, sollte darauf hingewirkt werden, dass Qualitätssicherungsaspekte (hinsichtlich des Aufbaus neuer Infrastrukturen als auch der Daten selbst) stärker verankert werden bzw. in den Fokus rücken.

Zugang für Wissenschaft und Forschung sichern

Die bisherigen Regulierungsansätze bzw. Vorhaben der EU in Bezug auf die Schaffung eines Rechtsrahmens für Datenintermediäre bzw. den B2B-/B2G-Datenaustausch sind mit Blick auf den Datenzugang für Wissenschaft und Forschung zu unspezifisch. Aus Sicht der AG Datentreuhänderschaft sollten freiwillige Ansätze des Datenteilens zwischen Wissenschaft und Wirtschaft gefördert, aber auch darüber hinausgehende Regulierungsansätze geprüft werden. Verlässliche Formate des sektorenübergreifenden Austausches können dazu beitragen, Win-win-Situationen zu gestalten. Dies umfasst auch, Lösungsansätze hinsichtlich der auf beiden Seiten bestehenden Schutzinteressen an den Daten und Potenziale von Datentreuhändern bzw. anderen neuen Intermediären in diesem Kontext zu erschließen.

Ausgangspunkt der Arbeit der AG war es zunächst, den Begriff „Datentreuhänder/ Datentreuhand“ zu definieren. Hieraus ist eine Begriffsklärung entstanden, die vom Plenum auf der 25. Ratssitzung verabschiedet wurde. Hierin werden als wesentliche Charakteristika der Datentreuhand vor allem dessen Vermittlungsrolle wie auch dessen Pflichten (darunter Sorgfaltspflichten sowie die Verpflichtung zur Wahrung der Neutralität) ausgewiesen. Zudem stünden verschiedene Anwendungsbereiche (u.a. im Kontext der Stärkung von Verbraucherinteressen oder zur Verbesserung des B2G-Datenaustausches) zur Diskussion. Hervorgehoben wird die Rolle der Wissenschaft in der Diskussion um Datentreuhandlösungen. Diese könne mit Blick auf die Verwendung sensibler Daten Anregungen liefern, zudem sei die Wissenschaft selbst Interessentin am Zugang zu Daten aus Wirtschaft und Gesellschaft. Der RfII sieht in Datentreuhändern ferner das Potenzial, den Aufbau sektorenübergreifender Datenzugänge zu ermöglichen.

Die AG Datentreuhänderschaft hat im Laufe ihrer Tätigkeit zentrale digitalpolitische Zielsetzungen und laufende Rechtsetzungsinitiativen (u.a. Datenstrategie, das geplante Mobilitätsdatengesetz) auf nationaler wie internationaler Ebene (Data Act, Data Governance Act), die im Zusammenhang mit der Datentreuhänder-Thematik stehen, verfolgt.

Insgesamt sind aus der AG-Arbeit **fünf Stellungnahmen und zwei Berichte** hervorgegangen.[71] Inhaltlicher Auftaktpunkt war die Stellungnahme DATENTREUHANDSTELLEN GESTALTEN – ZU ERFAHRUNGEN DER WISSENSCHAFT[72], in der Reflexionen über den Begriffskontext und das Begriffsverständnis zu Datentreuhändern angestellt werden. Zudem hat der RfII hierin Empfehlungen zur weiteren Auseinandersetzung mit dieser Thematik gegeben: So hat der RfII angeregt, mögliche Anwendungsbereiche von Datentreuhändern zu prüfen und den Aufbau dieser Infrastrukturen neuen Typs gegebenenfalls auch durch öffentliche Förderung voranzubringen. Aus Sicht des RfII sollte zudem der öffentlich geförderten Wissenschaft ein Zugang zu Daten anderer gesellschaftlicher Sektoren (beispielsweise in Form von gesetzlichen Forschungsklauseln) eingeräumt werden. Des Weiteren hat er auf notwendige Qualitätssicherungsmaßnahmen durch die Einführung eines Siegels oder Zertifizierungen und den Bedarf an einem Austausch zwischen Politik, Wirtschaft, Verwaltung und Wissenschaft hingewiesen.

Sehr früh hat die AG festgestellt, dass ein großer Bedarf besteht, sich aus der Perspektive der Wissenschaft zu **Gesetzesinitiativen,** die auf europäischer Ebene im Zusammenhang mit der Datenstrategie laufen und das Themenfeld Datentreuhänderschaft berühren, mit prägnanten **Stellungnahmen** zu äußern. Die AG hat sich zum Teil in einem sehr raschen Sondierungs- und Reflexionsprozess zu Gesetzesvorhaben verhalten und auch Verbesserungsvorschläge aus Sicht der Wissenschaft in die Diskussion eingebracht. Der RfII hat sich hiermit auch an Konsultationsprozessen der EU-Kommission zum Data Governance Act als auch zum Data Act beteiligt.

In seiner **Stellungnahme zum Data Governance Act (DGA),** der einen Rechtsrahmen für Datenvermittlungsdienste und die Weitergabe von geschützten Daten des öffentlichen Sektors schafft, hat der RfII unter anderem Anregungen formuliert, die Bildung von Datenvermittlungsdiensten durch Anreize zu fördern, vor allem durch die Klärung von Haftungsfragen und der Förderung des Aufbaus von Versicherungslösungen. Der RfII hat auch angemerkt, dass im DGA neben der Berücksichtigung der FAIR-Prinzipien darüber hinausgehende Qualitätssicherungsmaßnahmen verankert werden sollten (u.a. Entwicklung von Standards hinsichtlich der Anonymisierungsverfahren sowie von Leitlinien für die Kontrolle und Klassifizierung der Qualität der Daten).

Zur Ausgestaltung des **geplanten Data Act** der EU-Kommission, der Regelungen bezüglich des B2G- sowie B2B-Datenaustausches vorsieht, hat der RfII in zwei Stellungnahmen auf den Bedarf eines geregelten Datenzugangs der öffentlich geförderten

71 Alle „Arbeitsprodukte“ der AG Datentreuhänderschaft sind im Anhang beigefügt.

72 Rat für Informationsinfrastrukturen (2020) – Stellungnahme Datentreuhandstellen gestalten – Zu Erfahrungen der Wissenschaft, https://rfii.de/?p=4259.

Wissenschaft zu privatwirtschaftlichen Daten aufmerksam gemacht.[73] Noch in der Folgenabschätzung hatte die EU-Kommission auf die Potenziale intermediärer Strukturen hingewiesen, dies allerdings im weiteren Rechtsetzungsverfahren nicht mehr aufgegriffen. Der RfII hat nachdrücklich dafür plädiert, Möglichkeiten zur Förderung von Datentreuhandlösungen (u. a. durch Harmonisierung bzw. Konkretisierung der Rechtsauslegung) weiter zu erschließen.

Eine weitere Stellungnahme hat die AG Datentreuhänderschaft zum Referentenentwurf hinsichtlich der **nationalen Umsetzung des DGA** verfasst und Anfang Februar 2023 beim BMWK eingereicht. Hierin regt der RfII zwei Änderungen des Gesetzes zur Durchführung der Verordnung über europäische Daten-Governance an: Zum ersten die explizite Verankerung der Ausnahmeregelung für die öffentlich geförderte Wissenschaft hinsichtlich der Weiterverwendung von Daten öffentlicher Stellen (und zwar kostenfrei bzw. zu reduzierten Gebühren). Zweitens die Aufnahme einer Evaluierungsklausel in das Gesetz, um die Wirksamkeit der nationalen Umsetzung in einem Turnus von ca. vier Jahren überprüfen zu können. Darüber hinaus regt die AG weitere Maßnahmen zur Anreizsetzung und Qualitätssicherung an, sodass die Potenziale, die der DGA bietet, auch bestmöglich ausgeschöpft werden können.[74]

Die Arbeitsgruppe hat zudem **Expertise von außen** eingeholt, und zwar einerseits in Form eines größeren Workshops mit 15 Sachverständigen im September 2020 und eines kleineren Austauschs im März 2022 mit insgesamt sechs Sachverständigen. Die AG hat im Nachgang die wichtigsten Ergebnisse jeweils in einem Bericht[75] zusammengefasst:

Workshop

Zielsetzung des Workshops war es zunächst, das Thema zu eruieren und basierend auf grundlegenden Fragen zum Konzept der Datentreuhänderschaft einen Austausch zwischen Vertretern aus unterschiedlichen Sektoren zu schaffen. Als Sachverständige haben teilgenommen:

- Robert Schmitt (RWTH Aachen)
- Stefan Bender (Forschungsdaten- und Servicezentrum der Deutschen Bundesbank)

---

73 Rat für Informationsinfrastrukturen (2022) – Stellungnahme zum Vorschlag der EU-Kommission für eine „Verordnung über harmonisierte Vorschriften für den fairen Zugang zu Daten und deren Verwendung“ (Data Act), https://rfii.de/?p=7629.

74 Rat für Informationsinfrastrukturen (2023) – Stellungnahme zum Entwurf eines Gesetzes zur Durchführung der Verordnung über europäische Daten-Governance und zur Änderung der Verordnung (Daten-Governance-Rechtsakt), https://rfii.de/?p=8461.

75 Rat für Informationsinfrastrukturen (2021) – Workshop-Bericht der AG Datentreuhänderschaft – Datentreuhänder: Potenziale, Erwartungen, Umsetzung, https://rfii.de/?p=4652; RfII – Rat für Informationsinfrastrukturen (2022) – Datentreuhandmodelle: Qualitätsanforderungen – Ermöglichungsbedingungen – Haftungsfragen. Bericht zum Fachgespräch der AG Datentreuhänderschaft, https://rfii.de/?p=7603.

- Thomas Zurek (SAP)
- Lina Ehrig (Verbraucherzentrale Bundesverband)
- Christiane Wendehorst (Universität Wien)
- Sebastian Semmler (Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V., TMF)
- Fred Blüthner (FSD Fahrzeugsystemdaten Zentrale Stelle nach StVG)
- Christian Junger (MADANA)
- Henning Schwabe (BASF)
- Louisa Specht-Riemenschneider (Universität Bonn)
- Jan Schallaböck (iRIGHTS)
- Ralf Wehrspohn (Vorstand der Fraunhofer-Gesellschaft)
- Rolf Schwartmann (TH Köln)
- York Sure-Vetter (Direktor der NFDI)
- Monika Jungbauer-Gans (Deutsches Zentrum für Hochschul- und Wissenschaftsforschung, DZHW und Vorsitzende des Rates für Sozial- und Wirtschaftsdaten, RatSWD)

Allgemein wurde deutlich, dass über verschiedene Sektoren hinweg eine große Nachfrage besteht, sich mit Datentreuhandlösungen zu beschäftigen. Diskutiert wurden u.a. Ansätze der Modellbildung sowie Aspekte der Qualitätssicherung von Datentreuhändern. Der Workshop gliederte sich in drei Sessions. Thematisiert wurden zunächst **mögliche Aufgaben eines Datentreuhänders.** Hervorgehoben wurde, dass Datentreuhänder dazu beitragen könnten, den notwendigen Vertrauensprozess zwischen Datenerzeugern und -nutzern aufzubauen und zu stärken. Diskutiert wurde auch über den Bedarf eines möglichst europäischen Rechtsrahmens, der genügend Raum für Kreativität lasse. Zweitens wurde die Frage der **Ausgestaltung von Zugangsmodellen** erörtert. Deutlich wurde der Bedarf an sektorspezifischen Lösungsansätzen. So zeigten sich in den jeweiligen Anwendungsbereichen spezifische Herausforderungen: Im Bereich der Mobilitätsdaten fehle es beispielsweise noch an Aushandlungsprozessen, die einen fairen Datenaustausch ermöglichen. Ebenfalls sollte das Zusammenwirken rechtlicher Rahmenbedingungen und technischer Lösungen bedacht werden. Drittens beschäftigte sich der Workshop mit der Frage der **Qualitätssicherung von Datentreuhändern.** Vorgeschlagen wurde unter anderem eine Zertifizierung sowie kontinuierliche Evaluierung. Zudem wurde hervorgehoben, dass mit Blick auf Qualitätskriterien sowohl Anforderungen an den Datentreuhänder als auch Anforderungen an die Daten zu berücksichtigen seien.

Fachgespräch

Das Fachgespräch zielte darauf, Input eines kleinen Kreises an Sachverständigen einzuholen und zwar zu wesentlichen Fragen, die sich aus der weiteren Arbeit der AG ergeben haben. So lag der inhaltliche Schwerpunkt des Fachgesprächs auf der Frage nach den **Ermöglichungsbedingungen** von Datentreuhändern (also welche Faktoren entscheidend dafür sind, dass Datentreuhänder aufgebaut und auch genutzt werden). Regulierungsansätze wie z.B. der DGA wurden dabei als nicht ausreichend eingeschätzt. So sollten weitere **Anreize** gesetzt werden, Intermediäre wie Datentreuhänder aufzubauen. Diskutiert wurde auch die Frage, wie mit den hohen **Haftungsrisiken** umgegangen werden sollte, die auf Datentreuhänder zukommen. Und drittens wurden **Aspekte der Qualitätssicherung** vertieft. Als Sachverständige haben teilgenommen:

- Franziska Boehm (FIZ Karlsruhe/KIT Karlsruhe)
- Thomas Ganslandt (Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V., TMF)
- Egbert Schark (d-fine)
- Matthias Spielkamp (AlgorithmWatch)
- Rainer Böhme (Universität Innsbruck)
- Tibor S. Pataki (Gesamtverband der Deutschen Versicherungswirtschaft, GDV)

In Anknüpfung an den ersten Workshop wurde die Frage nach den Qualitätskriterien, die an den Datentreuhänder als auch die Daten selbst anzulegen sind, diskutiert. Sektorspezifische – und zwar rechtliche wie technische – Qualitätskriterien und bestenfalls **europaweit einheitliche Standards** sollten entwickelt werden. In Bezug auf die Qualitätsanforderungen an Daten wurde untermauert, dass diese über die FAIR-Kriterien hinausgehen und die Metadaten auch Angaben unter anderem über die rechtlichen Möglichkeiten bzw. Limitierungen der Nachnutzung umfassen sollten. Auch wurde u.a. herausgearbeitet, dass Erkenntnisse aus der Medizininformatik-Initiative (Tools für die Datenauswertung, Governance-Prozesse) dabei für andere Sektoren nutzbar gemacht werden können. Des Weiteren wurden Ermöglichungsfaktoren hinsichtlich des Aufbaus und der Nutzung von Datentreuhändern diskutiert. **Klare rechtliche Rahmenbedingungen** und die **Entwicklung tragfähiger Geschäftsmodelle** wurden als wesentliche Faktoren genannt. Ein weiterer Schwerpunkt lag auf der Frage, inwieweit der Aufbau von Versicherungslösungen für die Haftungsproblematik (z.B. bei Datenmissbrauch, Datenverlust oder Daten-Leak) förderlich für die Entwicklung von Datentreuhändern sein kann. Langfristig sei mit auf Datentreuhänder zugeschnittenen Versicherungsprodukten zu rechnen. Allerdings sei zu erwarten, dass **Versicherungsangebote** mit einer umfangreichen Haftungsbegrenzung entstehen. Als notwendig wurden klare rechtliche Rahmenbedingungen erachtet, aus denen deutlich hervorgeht, wofür der Datentreuhänder haften solle.

LITERATURVERZEICHNIS

Blankertz, Aline et al. (2020): Datentreuhandmodelle. Themenpapier, ip.mpg.de/de/publikationen/details/datentreuhand-modelle-themenpapier.html.

Blankertz, Aline; Specht-Riemenschneider, Louisa (2021): Neue Modelle ermöglichen. Regulierung für Datentreuhänder, Berlin, boell.de/de/2021/07/09/neue-modelle-ermoeglichen.

BMWi – Bundesministerium für Wirtschaft und Energie (2019): Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft. Bericht der Kommission Wettbewerbsrecht 4.0, Berlin, bmwk.de/Redaktion/DE/Publikationen/Wirtschaft/bericht-der-kommission-wettbewerbsrecht-4-0.html.

BMWi – Bundesministerium für Wirtschaft und Energie (2020): Datenmarktplätze in Produktionsnetzwerken (Impulspapier der Arbeitsgruppe „Digitale Geschäftsmodelle" der Plattform Industrie 4.0.

Buchheim, Johannes; Augsberg, Steffen; Gehring, Petra (2022): Transaktionsbasierte Datentreuhand. Nutzungsszenarien, Kennzeichen und spezifische Leistungen eines neuen Modells gemeinsamer Datennutzung, in: JuristenZeitung 77, Nr. 23, S. 1139–1147.

Bundesregierung (2021): Datenstrategie der Bundesregierung. Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, bundesregierung.de/breg-de/suche/datenstrategie-der-bundesregierung-1845632.

Datenethikkommission der Bundesregierung (2019): Gutachten, Berlin, bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.html.

Delacroix, Sylvie; Lawrence, Neil D. (2019): Bottom-up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance, in: International Data Privacy Law 9, Nr. 4, academic.oup.com/idpl/article/9/4/236/5579842.

Funke, Michael (2020): Die Vereinbarkeit von Data Trusts mit der Datenschutzgrundverordnung (DSGVO), Berlin, algorithmwatch.org/de/gutachten-data-trusts-dsgvo/.

Hardinges, Jack (2020): Data Trusts in 2020, theodi.org/article/data-trusts-in-2020/.

High-Level Expert Group on Business-to-Government Data Sharing (2020): Towards a European Strategy on Business-to-Government Data Sharing for the Public Interest, digital-strategy.ec.europa.eu/en/news/commission-appoints-expert-group-business-government-data-sharing.

Jentzsch, Nicola (2017): Die persönliche Datenökonomie: Plattformen, Datentresore und persönliche Clouds. Ökonomische Rahmenbedingungen innovativer Lösungen zu Einwilligungen im Datenschutz, Berlin, stiftungdatenschutz.org/praxisthemen/abgeschlossene-projekte/einwilligung-und-pims.

Kühling, Jürgen et al. (2020): Datenschutzrechtliche Dimensionen Datentreuhänder. Kurzexpertise im Auftrag des Bundesministeriums für Arbeit und Soziales. IZA Research Report No. 104, iza.org/publications/r/221/datenschutzrechtliche-dimensionen-datentreuhander.

Milne, Richard et al. (2022): What Can Data Trusts for Health Research Learn from Participatory Governance in Biobanks?, in: Med Ethics 48, S. 323–328, DOI: doi:10.1136/medethics-2020-107020.

O'Hara, Kieron (2020): Data Trusts, in: EDPL 4, S. 484–491. DOI: 10.21552/edpl/2020/4/4.

Open Data Institute (2019): Data Trusts: Lessons from Three Pilots, docs.google.com/document/d/118RqyUAWP3WIyy-CO4iLUT3oOobnYJGibEhspr2v87jg/edit.

Pataki, Tibor (2016): Die automobile Revolution gelingt nur gemeinsam, https://www.versicherungsbote.de/id/4847410/Automobile-Revolution-gelingt-nur-gemeinsam/.

Pataki, Tibor (2021): Autonomes Fahren und Datentransfer, in: DAR, Nr. 9.

Pinsent Masons (2019) – Data Trusts Legal and Governance Considerations, theodi.org/article/data-trusts-legal-report.

RatSWD (2019) – Big Data in den Sozial-, Verhaltens- und Wirtschaftswissenschaften: Datenzugang und Forschungsdatenmanagement. RatSWD Output 4 (6). Berlin, Rat für Sozial- und Wirtschaftsdaten (RatSWD). DOI: 10.17620/02671.39.

Schweitzer, Heike et al. (2022): Data Access and Sharing in Germany and in the EU: Towards a Coherent Legal Framework for the Emerging Data Economy.
A Legal, Economic and Competition Policy Angle, ip.mpg.de/de/publikationen/details/data-access-and-sharing-in-germany-and-in-the-eu-towards-a-coherent-legal-framework-for-the-emerging-data-economy-a-legal-economic-and-competition-policy-angle-final-report-expertenstudie-im-auftrag-des-bundesministeriums-fuer-wirtschaft-und-klimaschutz.html.

Specht-Riemenschneider, Louisa; Kerber, Wolfgang (2022): Designing Data Trustees. A Purpose-Based Approach, kas.de/en/single-title/-/content/designing-data-trustees-a-purpose-based-approach.

Specht-Riemenschneider, Louisa et al. (2021): Die Datentreuhand. Ein Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierungserfordernisse für Datentreuhandmodelle, in: MMR-Beilage 25.

Stiftung Datenschutz (2017): Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen, Leipzig, stiftungdatenschutz.org/praxisthemen/abgeschlossene-projekte/einwilligung-und-pims.

Verband der Automobilindustrie (2022) – Adaxo: Automotive Data Access – Extended and Open. VDA-Konzept für den Zugriff auf fahrzeuggenerierte Daten. vda.de/de/aktuelles/publikationen/publication/adaxo--automotive-data-access---extended-and-open.

Verbraucherzentrale Bundesverband e. V. (2020): Neue Datenintermediäre. Anforderungen des vzbv an „Personal Information Management Systems“ (PIMS) und Datentreuhänder, vzbv.de/publikationen/datenintermediaere-gesetzlich-regeln.

Verbraucherzentrale Bundesverband e.V. (2021): Fahrerlos alle mitnehmen. Automatisierte und vernetzte Mobilität aus Verbrauchersicht. vzbv.de/pressemitteilungen/gesetz-zum-autonomen-fahren-muss-alle-mitnehmen.

Sämtliche URL wurden zuletzt geprüft am 28.05.2023.

Verbraucherzentrale Bundesverband e.V. (2022): Mobilitätsdatenwächter – Digitale Privatheit bei vernetzten Fahrzeugen für alle Verbraucher:innen gewährleisten. Positionspapier des Verbraucherzentrale Bundesverbands (vzbv) zu einem verbrauchergerechten und fairen Zugang zu Fahrzeugdaten. vzbv.de/pressemitteilungen/verbraucherinnen-sollen-ueber-nutzung-von-mobilitaetsdaten-entscheiden.

Wendehorst, Christiane: Datentreuhand - wie hilfreich sind sachenrechtliche Konzepte?, in: Tereza Pertot (Hg.), Rechte an Daten, Tübingen 2020, S. 103–121.

ANHANG

A. BEGRIFFSKLÄRUNGEN

Datentreuhänder, Datentreuhand

[data trustee]

Bei einem Datentreuhänder handelt es sich um einen Intermediär, der unter festgelegten Rahmenbedingungen eine Vermittlungsrolle zwischen einem Datengeber und einem Datennutzer einnimmt. In der Regel unterliegt der Datentreuhänder dabei besonderen Pflichten, beispielsweise Sorgfaltspflichten und der Pflicht zur Wahrung der Neutralität. Datentreuhänder sollen für unterschiedliche Akteure einen fairen, von sachfremder Bevorzugung freien Zugriff auf Daten gewährleisten. Als neutrale Vermittler nehmen sie ggf. auch die Aufgabe wahr, hinsichtlich der Ausgestaltung des Datenzugriffs bzw. der Datennutzung einen Interessensausgleich zwischen Datengebern und Datennutzern herbeizuführen. Dies bedeutet, dass der Datentreuhänder lediglich eine vermittelnde Rolle einnehmen soll und die verwalteten Daten nicht für einen dem Neutralitätsgebot entgegenstehenden Zweck verwenden darf.

Der Begriff „Datentreuhänder" wird in aktuellen Diskussionen und Papieren in vielfältigen Bedeutungen verwendet und auf unterschiedliche Anwendungsbereiche bezogen. So findet sich das Konzept der Treuhänderschaft unter anderem verbunden mit der Idee einer treuhänderischen Verwaltung von Verbraucherdaten (ein Beispiel sind hier die *Personal Information Management Systems,* kurz genannt PIMS). Überdies gelten Datentreuhänder auch als Lösungsansatz, Daten unter Konkurrenzbedingungen zu teilen, z. B. zwischen Wirtschaftsunternehmen, aber auch an der Schnittstelle von Wissenschaft und Wirtschaft. In ausdifferenzierten Sphären, wie z. B. zwischen Wissenschaft und Wirtschaft, soll ein Datentreuhänder gewährleisten, dass die sog. „Datensouveränität" im Sinne von Verfügungsrechten und ggf. Schutzinteressen der Datengeber erhalten bleibt. Datengeber können Wirtschaftsunternehmen, öffentliche Stellen oder natürliche Personen sein – bei Letzteren können Daten in einem breiten Spektrum von Rollen unter anderem als Kunde, Patient oder Nutzer von Geräten und Diensten erfasst werden. Datennutzer sind jeweils im konkreten Fall genauer zu definierende Gruppen oder Kreise. Der Datentreuhänder kann je nach Anwendungsbereich und Bedarf verschiedene Aufgaben übernehmen (u. a. Anonymisierung von Daten, Datenveredelung), die seine Neutralität nicht gefährden sollen. Mitunter ermöglicht der Datentreuhänder den Dateninteressenten eine Auswertung von Daten/Datenbeständen, ohne die Daten selbst herauszugeben (auch bezeichnet als „transaktionsbasierter Datentreuhänder")[1]. Für die jeweiligen Anwendungsbereiche sind unterschiedliche Geschäftsmodelle denkbar. Hinsichtlich der Trägerschaft kommen die öffentliche Hand als auch kommerzielle Akteure oder nicht eigens dafür finanzierte Institutionen (z. B. mit spezieller Expertise und einem unter Vertrauensgesichtspunkten hinreichend anerkannten Status für spezialisierte Bereiche) in Frage.

Mit Blick auf die diskutierte Einrichtung von Datentreuhändern bzw. bereits institutionalisierten Datentreuhandstellen kommt die Wissenschaft in zwei eng miteinander verknüpften Rollen ins Spiel: Zum einen als Vorbild für „Best Practice" im Management sensibler Daten, der Einbin-

1 Buchheim, Johannes; Augsberg, Steffen; Gehring, Petra: Transaktionsbasierte Datentreuhand, in: JuristenZeitung Jahrgang 77 (2022) Heft 23, S. 1139–1147.

dung von Stakeholdern (Datensouveränität) in die Governance der Nachnutzung und in der Qualitätssicherung der Daten. Die Wissenschaft kennt seit längerem eine Datenbereitstellung im Sinne von „Vertrauensstellen“ für die Pseudonymisierung oder Anonymisierung von personenbezogenen Daten, die man als „treuhänderisch“ interpretieren kann, z. B. in sozialwissenschaftlichen, klinischen und epidemiologischen Studien. Der (nicht immer so bezeichnete) „Datentreuhänder“ kann beispielsweise zu diesem Zweck die Identitätsdaten einer zu Studienzwecken erfassten Person durch ein Pseudonym ersetzen, um Identitätsrechte des Datengebers bei Weitergabe der Daten zu schützen. Zum anderen ist die Wissenschaft Interessentin am Zugang zu Daten aus Wirtschaft und Gesellschaft, die z. B. über ein Treuhandmodell rechtmäßig und qualitätsgesichert zur Verfügung gestellt werden. Hinsichtlich der Verfügbarmachung von sensiblen Daten für die Wissenschaft können beispielsweise die Datenintegrationszentren der Medizininformatik-Initiative und die vom RatSWD akkreditierten Forschungsdatenzentren (FDZ) Erfahrungen liefern.

Während in Datenrepositorien die Datensätze häufig öffentlich sind, unterliegen die Daten bei Datentreuhändern besonderen Zugangsregimes. Dabei ist der Datenzugang nicht – wie es beispielsweise bei „Datengenossenschaften“ der Fall ist – auf die Datengeber beschränkt. Datentreuhänder lassen sich demnach als Dateninfrastrukturen besonderen Typs verstehen, die aufgrund ihrer Wahrung von Sorgfalts- und Neutralitätspflichten als auch ihrer Rolle als neutrale Dritte die Schaffung sektorenübergreifender Datenzugänge unterstützen können.

Quellen

Blankertz, Aline et al.: Datentreuhandmodelle (Themenpapier), o. O. 2020.

Datenethikkommission: Gutachten der Datenethikkommission, Berlin 2019.

RatSWD: Big Data in den Sozial-, Verhaltens- und Wirtschaftswissenschaften: Datenzugang und Forschungsdatenmanagement, Berlin 2019, DOI: 10.17620/02671.39.

RfII – Rat für Informationsinfrastrukturen: Stellungnahme Datentreuhandstellen gestalten – Zu Erfahrungen der Wissenschaft, Göttingen 2020, URN: urn:nbn:de:101:1-20200430091124055685O3.

Specht-Riemenschneider, Louisa et al.: Die Datentreuhand. Ein Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierungserfordernisse für Datentreuhandmodelle, Multimedia und Recht, Beilage Heft 6/ 2021, S. 25–48.

Specht-Riemenschneider, Louisa; Kerber, Wolfgang: Designing Data Trustees – A Purpose-Based Approach, Berlin 2022.

Wendehorst, Christiane; Schwamberger, Sebastian; Grinzinger, Julia: Datentreuhand – wie hilfreich sind sachenrechtliche Konzepte? In: Tereza Pertot (Hg.), Rechte an Daten, Tübingen 2020, S. 103–122.

Digitale Souveränität / Datensouveränität

[digital sovereignty / data sovereignty]

„Digitale Souveränität“[2] wird als Oberbegriff eines interdisziplinär und in Deutschland seit 2013 intensiv geführten Diskurses rund um Digitalisierungsthemen unter dem Gesichtspunkt des selbstbestimmten Handelns von Individuen, Unternehmen oder auch Staaten verstanden. Dies bezieht sich sowohl auf die Kontrolle über die Speicherung und Verwendung ihrer Daten als auch auf die Sicherung ihrer Entscheidungs- und Gestaltungsräume im Hinblick auf die Entwicklung bzw. Nutzung von digitalen Technologien und Diensten. Im politischen, zivilgesellschaftlichen und wissenschaftlichen Diskurs findet sich eine weite, unscharfe Begriffsverwendung. Dementsprechend wird der Begriff mitunter als „Projektionsfläche für zahlreiche digitalpolitische Befürchtungen und Wünsche“ wahrgenommen (Fraunhofer Kompetenzzentrum Öffentliche IT 2017).

Auf europäischer Ebene bündelt der Begriff der „digitalen Souveränität“ verschiedene Handlungsfelder, Politiken und Regelungen oder Regelungsvorschläge, u.a. zu digitalen Märkten und digitalen Diensten, zur europäischen Industriestrategie, zur künstlichen Intelligenz, zur Cybersicherheit und zum Umgang mit Daten (s. näher Europäische Kommission, Ein Europa für das digitale Zeitalter). Zunächst wurde er im Bereich der Cybersicherheit herausgestellt, hatte aber bereits hier übergreifende Implikationen, sodass er insbesondere als Fähigkeit der EU verstanden wurde, die Kontrolle über die von ihr genutzten Systeme zu bewahren (ENISA 2017, S. 11, 19). Auch über die Gestaltung eines europäischen digitalen Binnenmarktes, kompetenzbedingt ein zentrales Paradigma der EU, reicht der Begriff hinaus. Bezüge auf die „digitale Souveränität“ in ihrer übergreifend-bündelnden Bedeutung finden sich mittlerweile häufiger im Kontext der Digital- und Datenpolitik der EU. So galt der „Ausbau der digitalen Souveränität“ 2020 als wesentliches Leitmotiv der deutschen EU-Ratspräsidentschaft. Die Idee eines „europäischen Weges“ für die Digitaltechnologie und Digitalwirtschaft ist dabei mehr oder weniger eng mit dem Begriff „Datensouveränität“ verbunden.

Die Datenethikkommission der Bundesregierung hat den Begriff der „digitalen Souveränität“ primär in seiner Bedeutung im Verhältnis völkerrechtlicher Akteure zueinander aufgegriffen: „digitale Souveränität Deutschlands und Europas“ (DEK [Bericht] 2019, S. 20, 24, 32, 69, 95, 123, 141) sowie „digitale Souveränität Deutschlands“ (142). Ähnlich hat auch der RfII den Begriff der „Souveränität über Forschungsdaten“ u.a. mit Blick auf europäische Datenschutzstandards und im Sinne einer Warnung vor völliger „Offenheit“ von Forschungsdaten (vgl. RfII 2016, S. 35) interpretiert.

2 Die hier vorliegende Begriffsbestimmung stellt keine durch den RfII festgelegte Definition im engeren Sinne dar. Vielmehr steckt sie das Feld der unterschiedlichen, auf Digitalität bezogenen Souveränitätssemantiken ab, in denen sich der RfII in seiner Beratungstätigkeit aktuell bewegt.

Die vielschichtige Begriffsverwendung spiegelt sich unter anderem in der Digitalstrategie der Bundesregierung vom August 2022. „Digitale Souveränität“ wird als Leitmotiv der Digital- und Innovationspolitik der Bundesregierung formuliert. Sie wird dabei sowohl auf Aspekte der digitalen Kompetenz des Einzelnen als auch in der übergeordneten Begriffsdimension beispielsweise auf den Ausbau von Kompetenzen in Schlüsseltechnologien und die Anwendung von Open-Source-Lösungen durch die öffentliche Verwaltung bezogen.

Im politischen Raum taucht der Begriff der „digitalen Souveränität“ u. a. im Diskurs um Abhängigkeitsstrukturen insbesondere in Bezug auf digitale Technologien und Dienstleistungen außereuropäischer Anbieter und um daraus resultierende Konsequenzen staatlichen Handelns auf. Dabei wird unter anderem auch der umfangreiche Import von Hardware-Produkten durch deutsche Unternehmen thematisiert. Der Begriff markiert zugleich eine Situationsbeschreibung wie auch eine Zielvorstellung. Es geht hierbei nicht um Autarkie oder Unabhängigkeit, sondern um die Fähigkeit, in relevanten Feldern „digitale Technologien selbst zu entwickeln oder ohne einseitige Abhängigkeit von anderen Wirtschaftsräumen zu beziehen“ (Fraunhofer-Institut für System- und Innovationsforschung ISI 2020). So dient der Begriff unter anderem dazu, aus der Perspektive von Unternehmen oder Staaten technische oder technologische Abhängigkeiten zu problematisieren und die hiermit verbundenen potenziellen Auswirkungen und Risiken zu diskutieren. Dies speist sich meist aus einer Sorge um die Wahrung von Handlungs- und Gestaltungskompetenzen, den Erhalt der Wettbewerbsfähigkeit oder die Gewährleistung der Cybersicherheit. Darüber hinaus umfasst der Diskurs um „die digitale Souveränität“ mehrere – wie z. B. verbraucher-, industrie- und sicherheitspolitische? Aspekte, die unter anderem als „Datensouveränität“, „Verbrauchersouveränität“ oder „technologische Souveränität“ verhandelt werden.

Soweit mit Blick auf Individuen der Begriff der individuellen „digitalen Souveränität“ thematisiert wird, geht es neben der Stärkung der Medienkompetenz bzw. „digitalen Kompetenz“ u.a. darum, die Position von Verbraucherinnen und Verbrauchern durch technologische (z.B. durch die Umsetzung der Prinzipien *Data Protection by Design* und *Data Protection by Default* in den Voreinstellungen von Kommunikations- und anderen digitalen Diensten) oder regulatorische (wie der Forderung nach Offenlegung von Algorithmen) Maßnahmen zu verbessern (vgl. Sachverständigenrat für Verbraucherfragen 2017).

Der Begriff der **„Datensouveränität“** ist mit dem der „digitalen Souveränität“ eng verknüpft. Beispielsweise gehen in der aktuellen Datenstrategie der Bundesregierung beide Begriffe ineinander über (Gehring 2022, S. 33 ff.). „Data sovereignty“ (in englischer Sprache) bezeichnet zunächst die Hoheit von Nationalstaaten über die im eigenen Land anfallenden und gesammelten Daten. In dieser gegen transnationale Übergriffe auf die eigenen Staatsbürger gerichteten Bedeutung kam der Begriff in Gebrauch (vgl. Irion 2012, S. 40: „Cloud services are virtual, dynamic, and potentially stateless, which has triggered governments‘ concern for data sovereignty“). Anlässe für die Begriffsprägung sind Konflikte von Regierungen mit global operierenden Datenkonzernen, aber auch Überwachungssysteme wie das US-amerikanische PRISM, das weit über die eigenen Staatsgrenzen hinaus Massendaten erhebt und damit die Datensouveränität anderer Nationalstaaten verletzt.

Im Kontext der Digital- und Datenstrategie der Europäischen Union ist dieser Ausgangspunkt erweitert und wiederum mit einem übergreifend-bündelnd verstandenen Begriff der „digitalen Souveränität“ verbunden worden. Der Europäischen Kommission geht es darum, einen „eigenen, europäischen Weg [zu] finden, indem wir den Austausch und die breite Nutzung von Daten kanalisieren und gleichzeitig hohe Datenschutz-, Sicherheits- und Ethik-Standards wahren“ (Europäische Kommission 2020, S. 4). Die EU-Datenstrategie zeichnet sich durch eine Reihe neuer Ansätze und Konzeptionen aus, die den Datenschutz gewährleisten und zugleich, soweit dies als sinnvoll eingeschätzt wird, Datenzugänge und ein Datenteilen durch passende Regulierungskonzepte ermöglichen sollen.

Im deutschsprachigen Raum hat das Stichwort Datensouveränität auf mehreren Pfaden Sichtbarkeit erlangt. Es wird:

- im Sinne des grundrechtlichen Datenschutzes diskutiert, um das Recht auf informationelle Selbstbestimmung zu unterstützen oder zu konkretisieren. Die Befähigung der betroffenen Person, ihre Rechte in Bezug auf die personenbezogenen Daten wahrzunehmen (bspw. das Recht darauf, dass die personenbezogenen Daten nur in dem für den jeweiligen Zweck erforderlichen Umfang verarbeitet werden, oder die Rechte auf Auskunft, Berichtigung oder Löschung), gehörte auch zu den Zielen der europäischen Datenschutzreform und hat Eingang in die Datenschutz-Grundverordnung gefunden.
- teilweise so verstanden, dass Bürger „souverän“ über ihren eigenen „Datenreichtum“ verfügen können sollen. Dabei wird der ökonomische Wert der personenbezogenen Daten in den Mittelpunkt gestellt und Bürgerinnen und Bürger sollen frei darüber entscheiden können, ob sie den ökonomischen Wert ihrer Daten vermarkten wollen oder aber auf Vermarktung verzichten.
- teilweise auch als Weiterentwicklung informationeller Selbstbestimmung verwendet, sofern diese primär auf Abschottung und Ausschluss von Datenzugangs- und nutzungsmöglichkeiten ausgerichtet wird. Datensouveränität umfasst dann auf der Basis eines angemessenen Rechtsrahmens Entscheidungen, die das Datenteilen und erwünschte Datennutzungen im Sinn des jeweiligen Individuums ermöglichen (etwa Deutscher Ethikrat 2017, S. 251 ff.).
- neben dem Begriff eines (staatlichen) Datenschutzes ebenfalls für Unternehmen und andere gesellschaftliche Akteure verwendet und bezieht sich darauf, dass diese selbstbestimmt über die Verwaltung, Speicherung und Nutzung der eigenen Daten entscheiden können. Dies schließt die Kontrolle über ihre Daten ein; sie sollen selbst bestimmen, wie sie diese nutzen, wer darauf zugreifen darf und wie sie gespeichert werden. Dabei geht es nicht nur darum, dass natürliche Personen oder Unternehmen selbstbestimmt über ihre ökonomischen Daten verfügen können, sondern auch darum, dass sie die technischen Möglichkeiten haben, diese Souveränität auszuüben. Daher wird der Begriff der „Datensouveränität“ auch als Designprinzip für Datenräume angegeben (Nagel & Lycklama 2021, Curry et al. 2022, Otto et al. 2022) und in der europäischen Datenstrategie[3] als Zielvorstellung verstanden. Allerdings scheint der Begriff „Datensouveränität“ in diesem Zusammenhang häufig ohne eine genaue Klärung verwendet zu werden.

In der digitalpolitischen Debatte in Deutschland stehen in rechtlicher Hinsicht somit mehrere differente Bedeutungen des Begriffs „Datensouveränität“ nebeneinander: eine völkerrechtliche, die sich am Konzept des Schutzes der Staatsbürger orientiert, eine unionsrechtliche, die in die Digital- und Datenstrategie der EU eingebettet ist, eine grundrechtliche, die sich an Rechten und Freiheiten der betroffenen Personen orientiert und das Motiv informationeller Selbstbestimmung hervorhebt oder auch weiterentwickelt, sowie eine vertragsrechtliche, die unter dem Titelwort der Souveränität eine marktwirtschaftlich verstandene Individualfreiheit einschließlich der Ausübung von Verwertungs- und Vermarktungsrechten versteht. Die Pluralität an Begriffsverständnissen zu Datensouveränität hängt unter anderem damit zusammen, dass der Rechtsstatus von Daten kontextabhängig, vielschichtig, offen und im Fluss sowie teilweise noch nicht abschließend geklärt ist. Daher ist der Begriff bis auf Weiteres für vielfältige Zwecke verwendbar.

In der Summe bleiben beide Begriffe – digitale Souveränität wie Datensouveränität – in ihren Konturen noch verschwommen und erscheinen im Diskurs zum Teil austauschbar. Umso wichtiger ist es, beide Begriffe differenziert zu gebrauchen.

Verweise:

→ Datenschutz

Quellen:

Curry, Edward; Scerri, Simon; Tuikka, Tuomo: Data Spaces, Design, Deployment and Future Directions, 2022, DOI: 10.1007/978-3-030-98636-0.

Datenethikkommission der Bundesregierung: Gutachten der Datenethikkommission, Berlin 2019.

Deutscher Ethikrat: Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung. Stellungnahme, 2017.

Digitalstrategie der Bundesregierung „Gemeinsam digitale Werte schöpfen“, Berlin 2022.

ENISA (The European Union Agency for Cybersecurity): Principles and opportunities for a renewed EU cybersecurity strategy, 2017.

Europäische Kommission: Ein Europa für das digitale Zeitalter, commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_de.

Europäische Kommission: Eine europäische Datenstrategie, COM(2020) 66 final, 2020.

Fraunhofer-Institut für System- und Innovationsforschung ISI (Hg.): Technologiesouveränität. Von der Forderung zum Konzept, Karlsruhe 2020.

Gehring, Petra: Datensouveränität versus Digitale Souveränität. Wegweiser aus dem konzeptionellen Durcheinander, in: Augsberg, Steffen/ dies. (Hg.): Datensouveränität. Positionen zur Debatte, Frankfurt am Main 2022, S. 19-44.

Gräf, Eike; Lahmann, Henning; Otto, Philipp: Die Stärkung der digitalen Souveränität. Wege der Annäherung an ein Ideal im Wandel, 2018.

Hummel, Patrik et al.: Data sovereignty. A review, in: Big Data & Society Volume 8, Issue 1 (2021), S. 1-17.

Irion, Kristina: Government Cloud Computing and National Data Sovereignty", in: Policy & Internet. 4 (3–4): 40–71, DOI: 10.1002/poi3.10.

Kompetenzzentrum Öffentliche Informationstechnologie (Hg.): Digitale Souveränität als strategische Autonomie. Umgang mit Abhängigkeiten im digitalen Staat, Berlin 2020.

Kompetenzzentrum Öffentliche Informationstechnologie (Hg.): Digitale Souveränität, Berlin 2017.

3 In der europäischen Datenstrategie (eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066) wird der Begriff „data sovereignty“ nicht erwähnt. Die EU Webseite https://digital-strategy.ec.europa.eu/en/policies/strategy-data macht die Aussage: „The European strategy for data aims at creating a single market for data that will ensure Europe’s global competitiveness and data sovereignty.“

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: Digitale Souveränität der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen, Entschließung vom 22.09.2020, https://datenschutzkonferenz-online.de/media/en/TOP 8 Entschließung digitale Souveränität_final.pdf.

Nagel, Lars; Lycklama, Douwe: Design Principles for Data Spaces (1.0), 2021, DOI: 10.5281/zenodo.5244997.

Otto, Boris; ten Hompel, Michael; Wrobel, Stefan: Designing Data Spaces: The Ecosystem Approach to Competitive Advantage, 2022.

Pohle, Julia: Digital sovereignty. A new key concept of digital policy in Germany and Europe, Berlin 2020.

RfII – Rat für Informationsinfrastrukturen: Leistung aus Vielfalt. Empfehlungen zu Strukturen, Prozessen und Finanzierung des Forschungsdatenmanagements in Deutschland, Göttingen 2016.

Sachverständigenrat für Verbraucherfragen: Digitale Souveränität, Berlin 2017.

B. BERICHTE

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.

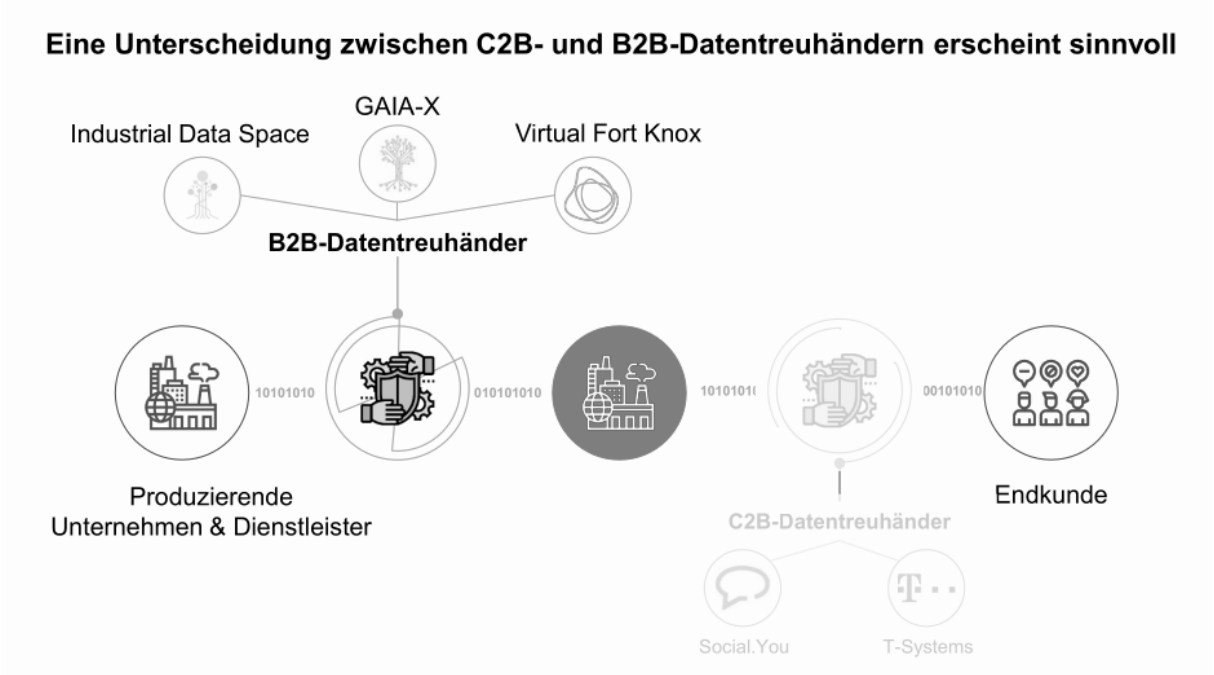
In ihrer Einführung verwies **Marit Hansen,** Landesbeauftragte für Datenschutz Schleswig-Holstein und Leiterin der Arbeitsgruppe Datentreuhänderschaft, auf den dynamischen Diskurs rund um das Thema Datentreuhänder und den thematischen Fokus des Workshops, der inhaltlich in drei Sessions gegliedert war: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

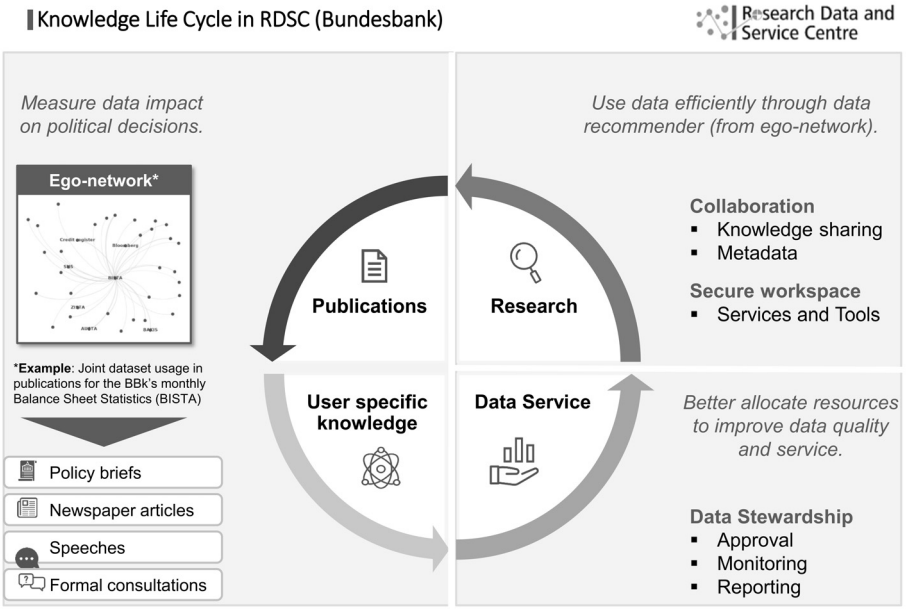
Dies beschrieb **Robert Schmitt,** RWTH Aachen, in seinem Vortrag „Datentreuhänder in der Produktion“ mit Blick auf mittelständische Unternehmen, die – wie er darlegte – die bei ihnen erzeugten Daten als Grundlage ihrer Wettbewerbsfähigkeit interpretieren. Insofern seien bei kleinen und mittleren Unternehmen (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.



Schmitt plädierte für eine Unterscheidung zwischen Business-to-Business (B2B-) und Custumer-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 nichtkommerzielle 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



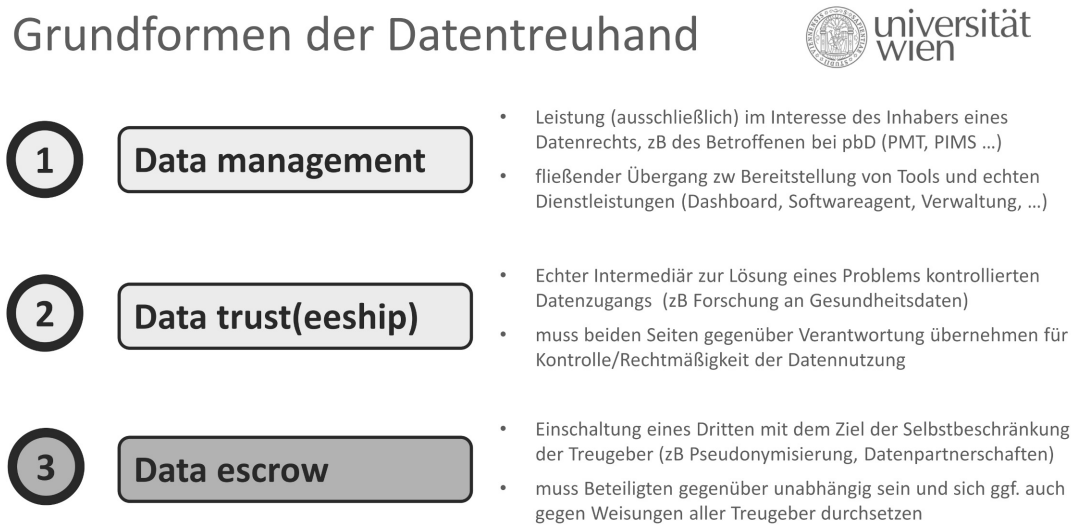
nachnutzbar sind. Mit Blick auf die Herausforderungen einer Datentreuhandstelle unterschied Bender drei Dimensionen, die zu berücksichtigen sind: Wissen (u.a. im Bereich Data Science, Programmierung, Anonymisierung), Rahmenbedingungen mit Blick auf den Datenzugang und Vertrauen (mit Blick auf die Datenerzeuger 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 im-

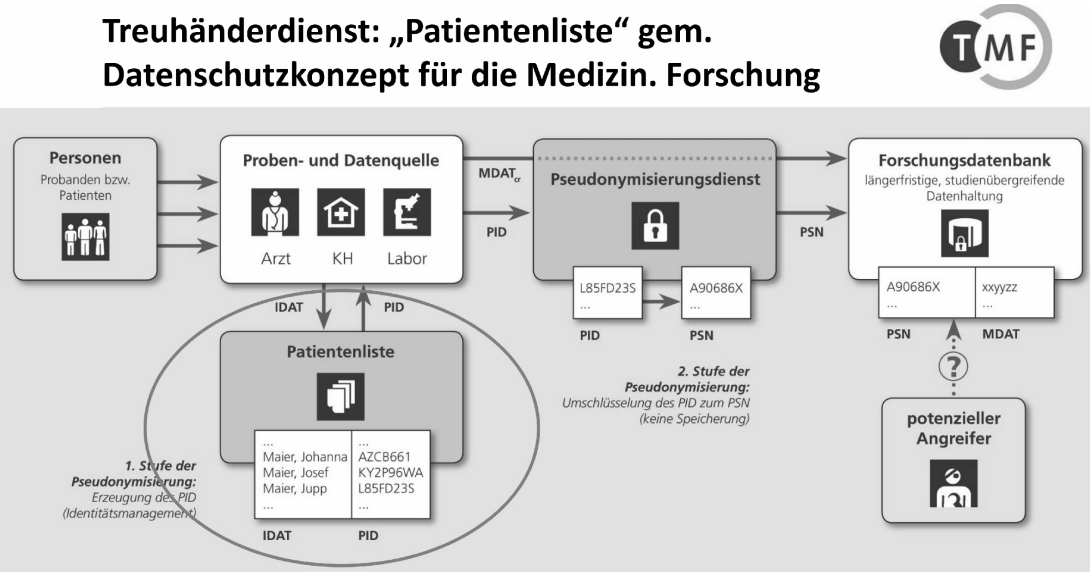
mer wichtiger, da mit ihrer Hilfe teils Konflikte mit dem Kartellrecht vermieden werden könnten. In diesem Zusammenhang seien Standards, unter anderem im Wettbewerbsrecht, notwendig.

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.

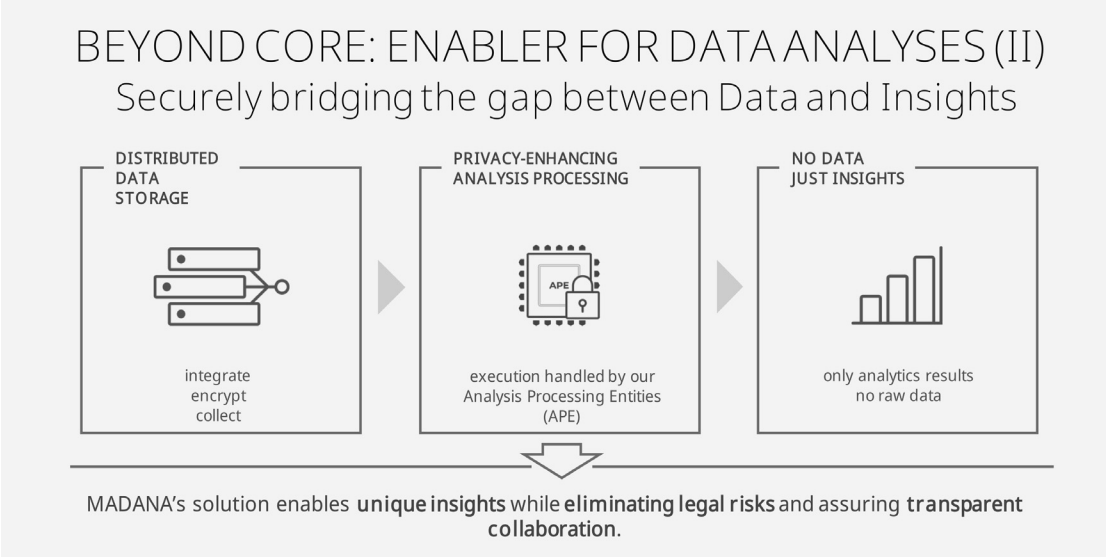
Einen Überblick über die Initiativen im Bereich medizinischer Daten und Bemühungen eines verbesserten Datenzugangs für die Forschung gab **Sebastian Semler,** Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF). Anhand der Medizininformatik-Initiative zeigte er auf,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

rung 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 gegebenenfalls 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 Einwilligungsmanage-

ment 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.

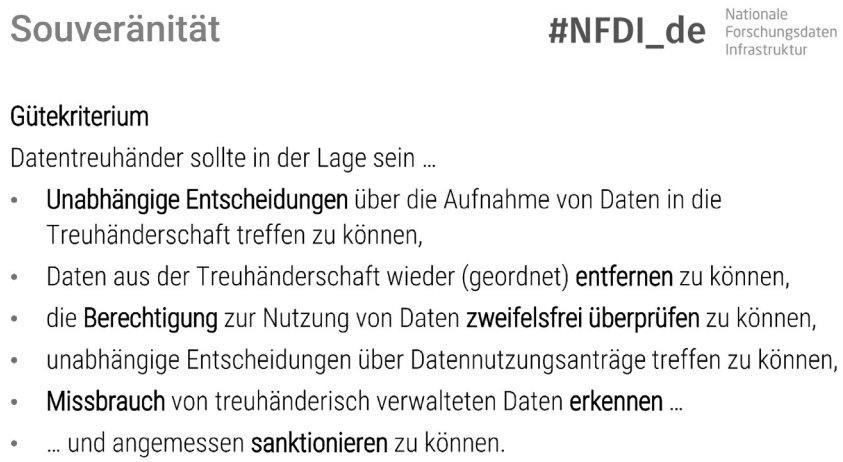
Gütekriterien seien aus Sicht von **Jan Schallaböck,** iRIGHTS, vor allem hinsichtlich Transparenz und Rechenschaftspflicht anzulegen, dies umfasse unter anderem die Pflichten und Zwecke der Weitergabe sowie die technischen Systeme und Schutzmaßnahmen. Vertraulichkeit sei ein weiterer möglicher Bereich, 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

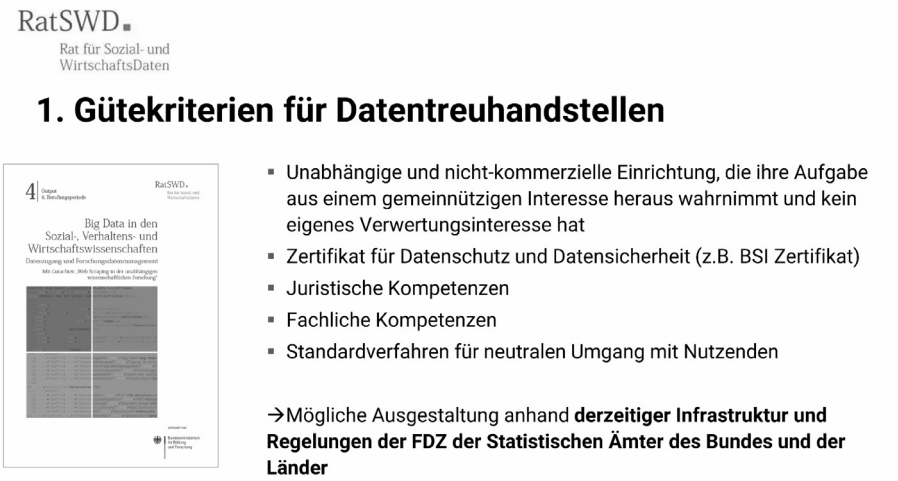
Anstrengungen auf europäischer Ebene in Bezug auf eine sichere europäische digitale Identität aus, die allen Bürgerinnen und Bürgern zur Verfügung stehen und ihnen mehr Kontrolle über ihre Daten ermöglichen soll.

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.

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, 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.

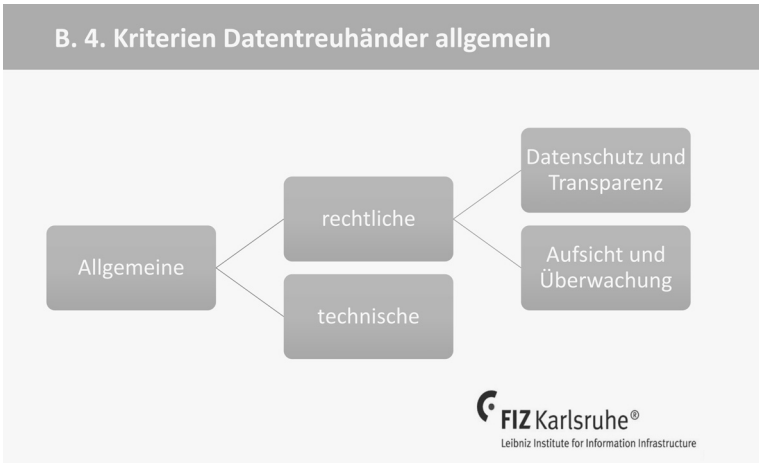
1 Koalitionsvertrag 2021–2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), BÜNDNIS 90/DIE GRÜNEN und den Freien Demokraten (FDP), S. 17.
2 Louisa Specht-Riemenschneider; Wolfgang Kerber (2022): Designing Data Trustees – A Purpose-Based Approach.

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[1]) zu berücksichtigen seien.



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 einheitli-

1 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).

che 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 Quellsyste-

men 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."

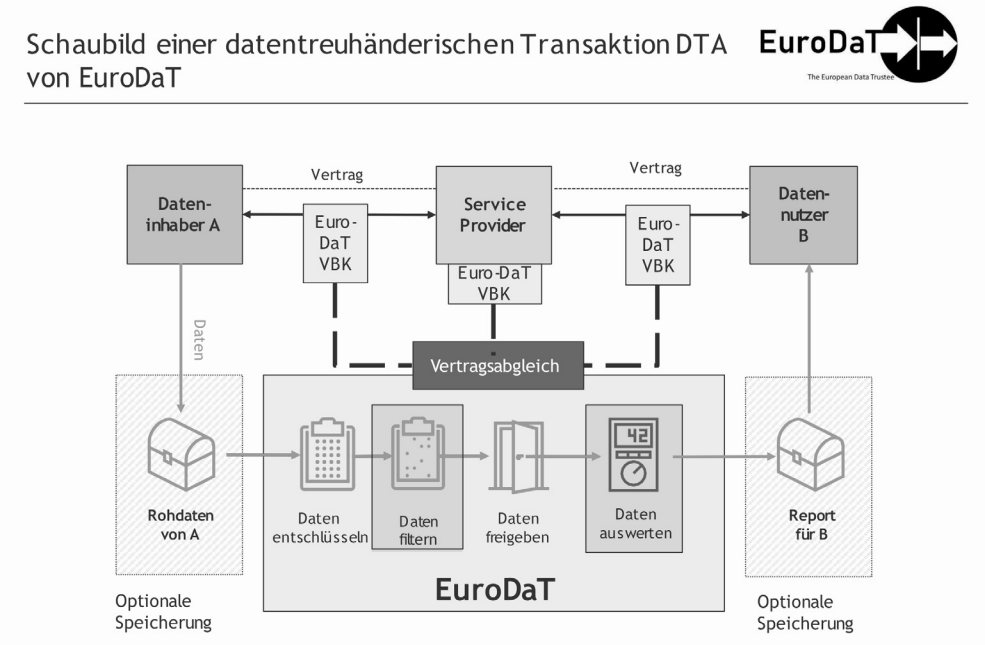
In Bezug auf die rechtlichen Rahmenbedingungen schätzten die Diskutantinnen und Diskutanten die derzeitige Rechtsgrundlage als nicht ausreichend ein. Der Data Governance Act der EU (DGA) wirke bislang eher einschränkend als anreizbildend. Ob durch den DGA Anreize für Datenintermediäre außerhalb des Rahmens 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 selbst 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.).

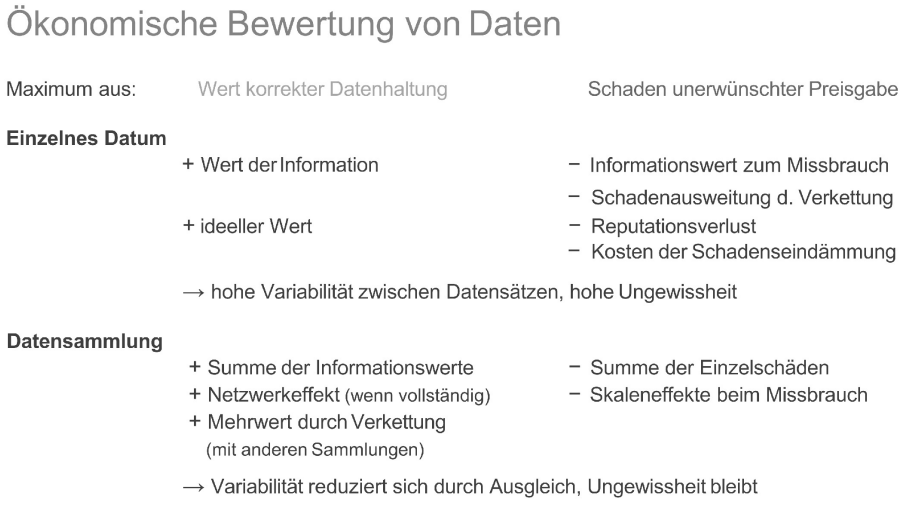
Ausgelotet wurden auch Ermöglichungsfaktoren im Zusammenhang mit Datenspenden und Einwilligungsverfahren. So wurde für eine breitere Anwendung des sogenannten *broad* oder *dynamic consent* plädiert, welcher in Deutschland noch kaum genutzt werde. Ein weiterer zen-

traler 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 aufwendig 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[1] 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 Etablie-

1 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.

rung 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 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 Entwicklung 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.

C. STELLUNGNAHMEN

Februar 2023

Stellungnahme zum Entwurf eines Gesetzes zur Durchführung der 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)

Die von der Europäischen Union auf den Weg gebrachte Rechtsverordnung über europäische Daten-Governance (Data Governance Act [DGA]) birgt nach Einschätzung des Rates für Informationsinfrastrukturen (RfII) große Chancen, das Datenteilen mittels Datenintermediären zu fördern. Die Legislation kann einen Mehrwert für das Gemeinwohl im Allgemeinen sowie für die wissenschaftliche Forschung im Besonderen schaffen. Die Potenziale des DGA werden aber nur wirksam, wenn sich entsprechende Anbieter auf dem Markt entwickeln und nachhaltig etablieren.

Der RfII hat in seiner Rolle als Beratungsgremium für den digitalen Wandel in der Wissenschaft im Januar 2021 zum Entwurf der Europäischen Kommission für einen DGA Stellung genommen. Er hat dabei angeregt, stärkere Anreize für die Erbringung von Datenvermittlungsdiensten zu setzen. Aus Sicht des RfII ist es für eine zielorientierte nationale Umsetzung des DGA wichtig, einen breiten Ermöglichungsraum für die Entstehung neuer Intermediäre, insbesondere für den Aufbau von Datentreuhändern, zu schaffen. Der RfII sieht Datentreuhänder als einen zentralen Baustein im Aufbau neuer Datenökosysteme an. Als neutrale Intermediäre können Datentreuhänder dazu beitragen, das Vertrauen auf Seiten der Datengeber als auch Datennutzer in eine rechtssichere und ggf. auch sektorenübergreifende Weitergabe und Nutzung von Daten unter Berücksichtigung notwendiger Schutzvorkehrungen zu stärken.

Akteure aus Wissenschaft und Forschung blicken aus mindestens drei Perspektiven auf die nationale Umsetzung des DGA: erstens als potenzielle Datennutzende, zweitens als genuine Anbieter von Datenvermittlungsdiensten und drittens vor dem Hintergrund umfangreicher Erfahrungen in der Wissenschaft mit dem Einsatz von Intermediären für ein effektives und vertrauensvolles Teilen von Daten. **Dementsprechend halten wir eine Änderung des Gesetzentwurfs in den folgenden Punkten für erforderlich:**

1. § 1 Abs. 3 des Gesetzentwurfs (Kostenregelung)

In Bezug auf die Weiterverwendung von Daten des öffentlichen Sektors sollte aus Sicht des RfII im § 3, Abs. 1 des nun geplanten deutschen Umsetzungsgesetzes die in Erwägungsgrund 25 des finalen europäischen Rechtstextes eröffnete Ausnahmeregelung für öffentlich geförderte Wissenschaftseinrichtungen konkret umgesetzt werden, damit Wissenschaft und Forschung wirkungsvoll Beiträge zu Innovation und Gemeinwohl leisten können. Daher sollten **wissenschaftlichen Nutzern Daten kostenfrei oder mindestens zu reduzierten Gebühren** bereitgestellt werden.

2. § 6 (Aufnahme einer Evaluierungsklausel in das Gesetz)

Der RfII spricht sich zudem nachdrücklich dafür aus, in das Gesetz eine Bestimmung zur **Evaluierung der nationalen Umsetzung des DGA** vorzusehen. Eine solche Evaluierung sollte in einem Turnus von ca. vier Jahren und unter Einbeziehung wissenschaftlicher Akteure erfolgen. Dies ermöglicht, die Wirksamkeit der Umsetzung zu prüfen und ggf. Anhaltspunkte für Nachsteuerungen geben zu können. Nur wenn die im DGA liegenden Potenziale auch genutzt werden, wird dieser nachhaltig zum Aufbau neuer Dateninfrastrukturen und einer für alle Seiten nutzbringenden Förderung des Datenaustausches beitragen können.

Des Weiteren empfiehlt der RfII bezüglich des Aufbaus von Informationsstellen, in der nationalen Umsetzung dafür Sorge zu tragen, dass – angesichts der bereits in Deutschland bestehenden Forschungsdatenzentren und auch Datenintegrationszentren – **keine institutionellen Doppelstrukturen** entstehen, die den Prozess des Datenteilens erschweren. Um seitens der Wissenschaft Angebote von Datenvermittlungsdiensten entwickeln und bereitstellen zu können, sind – wie für andere potenzielle Anbieter auch – Fragen der Rechtssicherheit und Nachhaltigkeit essenziell. Insofern sollten auch **über den DGA hinausgehend Maßnahmen** angestoßen werden, die sich förderlich auf die Entstehung neuer Intermediäre auswirken können. Dies umfasst beispielsweise Bestrebungen zu einer weiteren Harmonisierung der Rechtsauslegung, der Klärung von Haftungsfragen als auch der Förderung der Entwicklung geeigneter Geschäftsmodelle. Aus Sicht des RfII wären zukünftig auch weitere Anstrengungen im Bereich der Qualitätssicherung sinnvoll, d.h. die Einführung eines Labels oder einer Zertifizierung des Anbieters als auch eine stärkere Berücksichtigung von Datenqualitätsaspekten in Bezug auf die bereitgestellten Daten (u.a. Angaben zu ihrer Qualität oder Provenienz), sodass diese effektiv, transparent und rechtssicher genutzt werden können.

Der Gesetzgeber sollte die Gestaltungsspielräume, die der DGA ermöglicht, nutzen und Anreize schaffen, die den Aufbau neuer Intermediäre im gemeinsamen Dialog zwischen Wirtschaft, Verwaltung, Zivilgesellschaft und Wissenschaft voranbringen.

Mai 2022

Stellungnahme zum Vorschlag der EU-Kommission für eine „Verordnung über harmonisierte Vorschriften für den fairen Zugang zu Daten und deren Verwendung“ (Data Act)

Der Rat für Informationsinfrastrukturen (RfII) hat den Vorschlag der EU-Kommission für eine „Verordnung über harmonisierte Vorschriften für den fairen Zugang zu Daten und deren Verwendung“ vom 23. Februar 2022, auch bezeichnet als Data Act, mit Interesse zur Kenntnis genommen und möchte aus der Sicht der Wissenschaft und Forschung hierzu weitere Anregungen unterbreiten. Erste Empfehlungen zur Ausgestaltung eines Data Act hat der RfII bereits im September 2021 im Rahmen der Konsultation zur Folgenabschätzung (Inception Impact Assessment) gegeben.[1]

Der RfII bedauert, dass die Forderung einer grundsätzlichen „Datenzugangsklausel für die öffentlich organisierte Wissenschaft und Forschung“ zu privatwirtschaftlich gehaltenen Daten keinen Eingang in den vorliegenden Entwurf des Data Act gefunden hat. Von der Überzeugung getragen, dass von einem solchen Zugang sowohl die den Zugang gewährenden Unternehmen als auch das Gemeinwohl in hohem Maße profitieren würden, erneuert der Rat seine Vorschläge. Sie zielen darauf, den vorliegenden Entwurf (im Folgenden: DA-E) zu präzisieren, um die Potenziale, die in einem verbesserten Forschungszugang zu privatwirtschaftlich gehaltenen Daten liegen, besser auszuschöpfen.

Mit Blick auf das fünfte Kapitel des DA-E, das Regelungen zum B2G-Datenaustausch formuliert, schlägt der RfII zwei Modifizierungen vor und formuliert drittens eine allgemeine Anregung:

1. Forschungszugang ohne „außergewöhnlichen Bedarf“

Im DA-E wird ein Zugriff von Wissenschaft und Forschung auf privatwirtschaftlich gehaltene Daten dann ermöglicht, wenn eine Notfall- bzw. Krisensituationen eingetreten ist. Aus Sicht des RfII ist die Voraussetzung, dass für einen wissenschaftlichen Zugriff auf privatwirtschaftlich gehaltene Daten ein „außergewöhnlicher Bedarf“ ausgerufen werden muss, problematisch. Unklar bleibt, wer genau (im Entwurf: Staat, internationale Organisation), für welchen konkreten Anlass und ab welchem Schwellenwert einen „außergewöhnlichen Bedarf“ feststellt. Der RfII plädiert für eine Modifizierung im Data Act, die gewährleistet, dass der Wissenschaft ein eigener Zugriff auf privatwirtschaftliche Daten mit forschungsadäquaten Voraussetzungen eingeräumt wird, um allgemein zur Lösung großer gesellschaftlicher Herausforderungen (u.a. Pandemiebekämpfung, Anpassung an die Klimaerwärmung, demographischer Wandel etc.) beitra-

1 RfII (2021) – Stellungnahme zum geplanten Data Act der Europäischen Kommission auf Grundlage der Folgenabschätzung (Inception Impact Assessment) des Vorhabens; https://rfii.de/?p=6975 (zuletzt abgerufen am 10.05.2022).

gen zu können.[2] Aus Sicht des RfII ist es empfehlenswert, einen eigenen Datenzugang für Wissenschaft und Forschung auf der Grundlage eines öffentlichen Interesses bereits im Data Act – und nicht erst im Rahmen zukünftiger sektorspezifischer Regelungen – grundlegend zu verankern.

Dies könnte beispielsweise durch eine Änderung innerhalb des Data Acts erfolgen, indem unter Artikel 15 explizit hervorgehoben wird, dass öffentlichen Stellen und noch expliziter: öffentlich organisierten Wissenschaftsinstitutionen Datenzugriffe auf der Grundlage eines berechtigten allgemeinen „öffentlichen Interesses" ermöglicht werden.[3] Die Formulierung des „öffentlichen Interesses" ist in den Rechtsordnungen der Mitgliedstaaten der EU juristisch gängig. Sie kann staatlichen Einrichtungen ein ebenso flexibles wie angemessenes Zugriffsspektrum ermöglichen. Datenzugänge für Wissenschaft und Forschung sollten dabei sektorspezifisch über einschlägig legitimierte und qualitativ ausgewiesene Stellen, z. B. zertifizierte Datentreuhänder, gewährt werden (s. Abschnitt 3).[4] Datenanfordernde staatliche Stellen – einschließlich der öffentlich organisierten Wissenschaft – sollten in diesem Zusammenhang rechtsverbindlich gewährleisten, dass die angefragten Daten ohne ausdrückliche Ermächtigung der Datengeber weder an Dritte weitergeleitet, noch für gewerbliche Zwecke genutzt werden dürfen. Über die wissenschaftliche Datenverwendung ist auf Nachfrage Rechenschaft abzulegen.

Ebenso könnte an geeigneter Stelle im Data Act (beispielsweise in den Erwägungsgründen) stärker auf die – über konkrete Notfallsituationen hinausgehende – Bedeutung eines geregelten Zugangs der Wissenschaft und Forschung zu privatwirtschaftlichen Daten für die Förderung des Gemeinwohlinteresses hingewiesen werden. Auch könnte vor diesem Hintergrund klargestellt werden, dass über den Data Act hinausgehende Regelungen von Datenzugangsansprüchen (z. B. auf der Ebene der Mitgliedstaaten) möglich oder gar wünschenswert sind. Hierbei ist der Schutz von unternehmerischen Betriebsgeheimnissen und Geschäftsmodellen angemessen zu berücksichtigen (s. o.).

2. Kosten für den wissenschaftlichen Datenzugang begrenzen

Aus Sicht des RfII sollte mit Blick auf die Regelungen unter Artikel 20 dafür Sorge getragen werden, dass die öffentlich finanzierte Wissenschaft und Forschung privatwirtschaftlichen Datengebern höchstens eine Aufwandsentschädigung für die Datenbereitstellung erstatten muss,

2 Wissenschaftsrat (2015) – Zum wissenschaftspolitischen Diskurs über Große gesellschaftliche Herausforderungen; https://www.wissenschaftsrat.de/download/archiv/4594-15.html (zuletzt abgerufen am 10.05.2022).

3 Siehe in diese Richtung argumentierend auch: Open Future Policy brief #2.2 – Data Act: Business to Government Data Sharing.

4 Zur Regulierung von Datentreuhändern siehe unter anderem Louisa Specht-Riemenschneider; Wolfgang Kerber (2022) – Designing Data Trustees. A Purpose-Based Approach; https://www.kas.de/documents/252038/16166715/Designing+Data+Trustees.pdf/3523489b-2611-a12a-f187-3e770d1a9d94 (zuletzt abgerufen am 10.05.2022). Im deutschen Wissenschaftssystem nehmen akkreditierte Forschungsdatenzentren (FDZ) vergleichbare Funktionen wahr und regulieren beispielsweise den Zugang von Wissenschaftlerinnen und Wissenschaftlern zu Daten der Bundesbank, der Sozialversicherungsträger, der statistischen Ämter oder großer Panel-Studien. In diesem Zusammenhang entscheiden die FDZ auch je nach Forschungszweck und Begründung des Forschungsinteresses über Fragen der Ausgestaltung des Zugriffs (Remote oder lokal) und die Zugriffstiefe (Granularität und Grade der Anonymisierung und/oder Pseudonymisierung von Datensätzen). Der RfII hält diese im Bereich der Wirtschafts- und Sozialdaten praktizierte Lösung auch für andere Sektoren und wissenschaftliche Felder für übertragbar.

deren Kosten transparent nachzuweisen sind. Kostenneutralität für die datengebenden Unternehmen sollte hierbei das Ziel sein. Sollte die Anfrage auf Datenzugang nach dem Anwendungsbereich 15 b und c (d.h. unter anderem zur Prävention einer Notfallsituation) erfolgen, sollte rechtlich ausgeschlossen werden, dass Unternehmen für die Bereitstellung eine „Gewinnspanne“ *(reasonable margin)* ansetzen dürfen, die über eine reine Aufwandskompensation hinausgeht. Entsprechende Regelungen würden sowohl den geleisteten Aufwand seitens der Unternehmen kompensieren helfen, als auch den essentiellen Beitrag berücksichtigen, den Wissenschaft und Forschung für das Gemeinwohl leisten. Bei der im DA-E vorgesehenen Regelung sieht der RfII die Gefahr, dass Unternehmen mitunter prohibitiv wirkende Gebühren erheben könnten, die geeignet wären, Datenzugangsbegehren der Wissenschaft von vornherein abzuwehren, oder dass auf Basis privatwirtschaftlicher Daten, die potenziell von Gemeinwohlinteresse – und von Forschungsinteresse – sein könnten, lukrative Geschäftsmodelle zu Lasten der öffentlichen Hand entwickelt werden.

3. Berücksichtigung der Forschung auch in sektorspezifischen Regelungen

Der RfII regt an, für den Aufbau der European Data Spaces sektorspezifische Datenzugangsregelungen zu formulieren, die forschungsfreundlich ausgestaltet sind und freiwillige Anreize eines B2G-Datenaustausches fördern können. In diesem Zusammenhang begrüßt der RfII den Ansatz der EU-Kommission, im kürzlich veröffentlichten Verordnungsvorschlag zum European Health Data Space Zugang zu Gesundheitsdaten auf der Grundlage eines öffentlichen Interesses zu ermöglichen.[5] Der RfII wird die Entwicklungen rund um den Aufbau der European Data Spaces weiter beobachten.

In diesem Zusammenhang möchte der RfII auf die Regelungen des geplanten Data Governance Act (DGA) zu „new intermediaries“ hinweisen. Er sieht das Potenzial von Datentreuhändern, als neutrale Instanz, Datenzugangsanfragen zu sammeln und divergierende Interessen von Datengebern und Datennehmern auch im B2G-Bereich in einen Ausgleich bringen zu können. Dies wäre nach Ansicht des RfII auch für potenzielle privatwirtschaftliche Datengeber von Vorteil, da sie nicht mit einzelnen, ad hoc gestellten Anfragen öffentlicher Stellen auf Datenzugriff sowie mit deren Bearbeitung konfrontiert wären. Angeregt werden könnte zudem, mögliche Datentreuhandmodelle weiter zu erschließen bzw. zu erproben – darunter auch die bereits heute unter sehr hohen Sicherheitsstandards arbeitenden Forschungsdatenzentren der Wissenschaft und zahlreicher datenintensiver öffentlicher Einrichtungen.[6] Datentreuhänder können dazu beitragen, auch für private Unternehmen Standards im Bereich der Interoperabilität und Datenqualität zu entwickeln und zu setzen, die zugleich die Geschäftsmodelle und Betriebsgeheimnisse der datengebenden Firmen schützen. Daher möchte der RfII anregen, die in der Folgenabschätzung zum Data Act erwähnten Potenziale von Intermediären innerhalb des finali-

5 European Commission (2022) – Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space; ec.europa.eu/health/publications/proposal-regulation-european-health-data-space_en.

6 Siehe hierzu die Ausführungen in Fußnote 4.

sierten Data Acts an geeigneter Stelle wieder aufzugreifen.[7] Dies könnte dadurch geschehen, dass die potenzielle Rolle von Intermediären zumindest Eingang in die Erwägungsgründe des Acts findet.

7 "Intermediation structures or bodies could aggregate demand, support professionalization, convene public sector bodies interested in certain data as well as private sector data holders, including at sectoral level."; European Commission (2021) – Inception Impact Assessment, S. 5.

September 2021

Stellungnahme zum geplanten Data Act der Europäischen Kommission auf Grundlage der Folgenabschätzung (Inception Impact Assessment) des Vorhabens

Der Data Act soll dem öffentlichen Sektor im Gemeinwohlinteresse den Zugang zu privatwirtschaftlich gehaltenen Daten erleichtern (B2G). Ebenso zielt er darauf, den Datenaustausch Business to Business (B2B) zu fördern.

Mit Blick auf eine spätere konkrete Ausgestaltung des Acts regt der Rat für Informationsinfrastrukturen (RfII) an, dass die Kommission im geplanten Data Act

- grundsätzlich den Bedarf der Wissenschaft und Forschung an Zugangsansprüchen zu privatwirtschaftlich gehaltenen Daten anerkennt sowie
- diesen in den einzelnen Maßnahmen berücksichtigt.

Wissenschaft und Forschung sehen sich bislang mit teils erheblichen Hürden konfrontiert, Zugang zu privatwirtschaftlich gehaltenen Daten, insbesondere zu Daten von Unternehmen, zu erhalten. Nicht selten sind Forscherinnen und Forscher darauf angewiesen, Datenzugänge individuell mit Unternehmen auszuhandeln oder lediglich als so genannte „embedded researchers" einen Forschungszugang zu Unternehmensdaten zu erhalten, und das heißt dann: lediglich unter Einhaltung von durch die Unternehmen festgelegten Auflagen sowie oft auch ohne Kenntnis der unternehmensseitig für die Datenerzeugung und -verarbeitung verwendeten Algorithmen.[1] Diese und ähnliche Praktiken entsprechen nicht dem europäischen Verständnis guter wissenschaftlicher Praxis. Sie tragen nach Einschätzung des RfII auch nicht dazu bei, dass eine wissenschaftliche Verwertung dieser Daten im Gemeinwohlinteresse – z. B. als Beitrag zur Lösung großer gesellschaftlicher Herausforderungen – deutlich forciert werden könnte. Daher sollte eine **Datenzugangsklausel** für Zwecke der öffentlich organisierten **Wissenschaft und Forschung,** die zugleich der Unternehmensseite die Wahrung von Betriebsgeheimnissen bei wissenschaftlicher Nutzung der Daten garantiert, in den Data Act eingeführt werden.

Im ausformulierten Data Act sollte klar konturiert werden, inwiefern in Bezug auf die Business to Government (B2G)-Regelungen die öffentlich finanzierte Forschung unter den Anwendungsbereich fällt. Sofern Forschung allgemein einbezogen werden soll, ist es sinnvoll, sämtliche öffentlich finanzierten Forschungseinrichtungen hierunter zu fassen – und nicht nach Rechtsformen von Forschungsorganisationen zu differenzieren. Sollte der Aufbau neuer Intermediäre (gemäß Data Governance Act) im B2G-Bereich beabsichtigt werden, plädiert der RfII dafür, diese Intermediäre forschungsfreundlich auszugestalten. Mit Blick auf die bereits bestehenden

1 Diese Problematik hat u.a. die Arbeitsgruppe Datenzugang zu Big Data des RatSWD ausführlich dargelegt: RatSWD (2019) – Big Data in den Sozial-, Verhaltens- und Wirtschaftswissenschaften. Datenzugang und Forschungsdatemanagement. RatSWD Output 4 (6). Zu Datendiensten in diesem Bereich und Bestrebungen, Zugänge für Wissenschaft und Forschung zu schaffen bzw. zu erleichtern, vgl. beispielsweise auch RfII (2021) – Nutzung und Verwertung von Daten im wissenschaftlichen Raum, Kap. 2.4.

und im Rahmen der Datenstrategie der deutschen Bundesregierung weiter geplanten Forschungsdatenzentren in Deutschland sollten Doppelstrukturen oder unklare Zuständigkeiten bei der Einführung neuer Intermediäre auf europäischer Ebene vermieden werden.

Der RfII plädiert dafür, den Data Act als Regulierungsinstrument zu nutzen, um sektorenübergreifend den Aufbau von Schnittstellen zwischen Wirtschaft, Gesellschaft und Wissenschaft voranzubringen. Dies könnte beispielsweise in Fördermaßnahmen zur Erprobung neuer Kooperationsformen wie Datentreuhandlösungen geschehen. Ebenso sollte die Europäische Datenschutzgrundverordnung so ausgelegt werden (oder ggf. so modifiziert werden), dass sie gemeinwohlorientierte, verantwortungsbewusste Datentreuhandlösungen unterstützt. Beispielsweise sollte die Möglichkeit einer pauschalen Einwilligung durch Datengeber in ein treuhandtypisches Verfügen über Daten und deren Weitergabe in einem hinreichend weit gefassten Rahmen bestehen.[2] Zudem könnten auf nationaler Ebene Datenschutzaufsichtsbehörden auf eine weitere Harmonisierung oder auch Konkretisierung der Rechtsauslegung hinwirken, die die Entstehung von Datentreuhandlösungen erleichtern würde. Nur so kann das in einem gesteigerten Datenaustausch liegende Innovationspotenzial zum Vorteil aller Beteiligten optimal ausgeschöpft werden. Dies zeigt sich beispielsweise bei der Erforschung Künstlicher Intelligenz (KI) und der Entwicklung innovativer Technologien und KI-Anwendungen. Der Aufbau geeigneter intermediärer Strukturen mittels Datentreuhandstellen kann einen Beitrag dazu leisten, faire Zugangsregelungen zu schaffen, die auf europäischen Werten bei Datenschutz und Wissenschaftsfreiheit aufbauen.

Weitere Anstrengungen der Europäischen Kommission zur Steigerung des Datenteilens sollten verstärkt mit Maßnahmen zur Qualitätssicherung einhergehen. Im Kontext von Open Data und Open Access hat der RfII bereits in einer Stellungnahme vom März 2019 auf die zu berücksichtigenden Qualitätsaspekte hingewiesen.[3] Er hat auch deutlich gemacht, dass das übergeordnete Regulierungsziel für das Datenteilen in der Förderung von hochwertigen Datenbeständen (high value data sets) liegen soll. In Bezug auf den Data Act erscheint es sinnvoll, dass auch für Daten aus dem privatwirtschaftlichen und kommerziellen Bereich mindestens die FAIR-Prinzipien als Orientierungsmaßstab vorgesehen werden sollten. Für eine wissenschaftliche Nutzung und Verwertung sind freilich auch die FAIR-Prinzipien lediglich eine Minimal-Anforderung, können aber als ein erster Schritt zur Forcierung eines sektorenübergreifenden Teilens von hochwertigen, auch wissenschaftlich nutzbaren Daten bewertet werden.

Der RfII begrüßt das Vorhaben der Kommission, durch die Schaffung von Rahmenbedingungen für faire und symmetrische Vertragsbeziehungen den Zugang kleinerer und mittlerer Unternehmen zu den Daten globaler, teils marktbeherrschender Unternehmen zu verbessern. Auch die vorgesehenen Maßnahmen bezüglich der Erleichterung eines Wechsels von Cloud-Diens-

2 Auf die hierbei entstehenden Haftungsfragen und die Notwendigkeit eines flankierenden Aufbaus tragfähiger Versicherungslösungen für Datentreuhänder hat der RfII bereits in einer Stellungnahme zum Entwurf eines Europäischen Data Governance Acts hingewiesen. Siehe hierzu RfII (2021) – Stellungnahme zum Vorschlag eines Data Governance Acts (DGA) durch die EU-Kommission.

3 RfII (2019) – Stellungnahme des Rates für Informationsinfrastrukturen (RfII) zu den aktuellen Entwicklungen rund um Open Data und Open Access.

ten und der Migrierbarkeit von Daten zwischen Diensten und Diensteangeboten werden vom RfII nachdrücklich begrüßt. Für die Forschung ist die Wechsel- und Migrationsmöglichkeit von Datenbeständen, die teilweise als Wissensspeicher auch das methodische Gedächtnis ganzer Disziplinen und Felder verkörpern, von existentieller Bedeutung. In seinem Positionspapier zur „Nutzung und Verwertung von Daten im wissenschaftlichen Raum“ hat der RfII ausgeführt, dass Akteure aus der öffentlich getragenen Forschung auch bei Einschaltung oder Nutzung kommerzieller Anbieter von Datendiensten dauerhaften Zugang zu den Daten, die sie einspeisen, behalten können müssen.[4] Deshalb dürfen die Nachhaltigkeit der Datenarchivierung und der Zugang zu Daten auch bei Verkauf oder Insolvenz eines kommerziellen Dienstleisters/Partners oder bei der Einstellung unprofitabler Dienste nicht verloren gehen. Der RfII ist sich sicher, dass diese Empfehlungen darüber hinausgehend auf die Anforderungen von B2B-Beziehungen übertragen werden können, in denen die Marktbeziehungen zurzeit nicht symmetrisch ausgestaltet sind.

4 Vgl. hierzu auch RfII (2021) – Nutzung und Verwertung von Daten im wissenschaftlichen Raum, Kap. 4.2 sowie Empfehlung 5.5 (S. 79f.).

Januar 2021

Stellungnahme zum Vorschlag eines Data Governance Acts (DGA) durch die EU-Kommission

Das Vorhaben der EU-Kommission, durch europaweite rechtliche Rahmenbedingungen zum Aufbau von Datenintermediären *(data sharing providers)* einen Impuls für das Teilen von Daten zu setzen, ist grundsätzlich zu begrüßen. Die EU-Kommission nimmt neue Akteure in den Blick, die ein effektiveres Teilen von Daten in Wirtschaft und Gesellschaft ermöglichen sollen. Um hierfür eine ebenso rechtssichere wie vertrauensstiftende Grundlage zu schaffen, formuliert die Kommission umfassende Anforderungen an die neuen Intermediäre. Der Rat für Informationsinfrastrukturen (RfII) hat hierzu aus der Perspektive eines Beratungsorgans zur Begleitung des digitalen Wandels in der Wissenschaft und der hierfür erforderlichen Informationsinfrastrukturen Stellung genommen.[1] Die nachfolgenden vier Empfehlungen zur weiteren Ausgestaltung des Entwurfs der DGA zielen darauf ab, dem Vorhaben insgesamt mehr Wirkung zu verleihen. Ebenso sollten aus Sicht des RfII wesentliche Belange der Forschung und der Hochschullehre bei der Etablierung von *data sharing providers* Berücksichtigung finden.[2]

***

Zu den Zielen des European Data Governance Acts (DGA) gehört es, das Teilen beziehungsweise die Nachnutzung auch von geschützten Daten – unter anderem Public-Sector-Daten – durch die Schaffung neuer Formen von treuhänderischen Datenintermediären *(data sharing providers,* im Folgenden DSP), welche die Daten nicht selbst auswerten, sondern bereithalten, gegebenenfalls für die verbesserte Nutzbarkeit passend aufbereiten und distribuieren, auf eine rechtlich verlässliche, aber auch ökonomisch attraktive Grundlage zu stellen.

- Zum einen wird dies die wissenschaftliche Datennutzung betreffen – hierzu hält der RfII unter Punkt A die Einführung einer Forschungs- bzw. Wissenschaftsklausel in den DGA für unabdingbar.
- Zum anderen können wissenschaftliche Einrichtungen sich als DSP im Sinne des DGA engagieren. Dies kann sowohl in ähnlicher Form wie ein gewinnorientiertes Unternehmen erfolgen als auch im Rahmen einer als gemeinnützig bzw. einer als „datenaltruistisch“ anerkannten Organisation. Hierzu nimmt der RfII in den Punkten B und C Stellung und empfiehlt, Präzisierungen vorzunehmen.

---

1 Die Stellungnahme wurde durch die AG Datentreuhänderschaft und den Vorsitz des RfII im Januar 2021 ausgearbeitet und am 29.01.2021 im Beteiligungsverfahren der EU-Kommission zum DGA eingereicht. Der RfII hat diese Stellungnahme in seiner 20. Sitzung am 18. März 2021 verabschiedet. Dabei hat er auch den Kompromissvorschlag der portugiesischen EU-Ratspräsidentschaft zum DGA vom 22.02.2021 gewürdigt, sieht aber in den Vorschlägen keinen Anlass, inhaltliche Änderungen seiner im Januar verfassten Stellungnahme vorzunehmen. Die hier formulierten Empfehlungen zur weiteren Ausgestaltung des DGA bleiben aus Sicht des RfII dringlich und geboten.

2 Siehe auch RfII (2020) – Stellungnahme Datentreuhandstellen gestalten – Zu Erfahrungen der Wissenschaft, http://www.rfii.de/?p=4318 (letzter Zugriff am 26.01.2021).

- Schließlich behandelt der DGA-Entwurf die Qualitätssicherung der Daten und entsprechende Aufgaben der DSP kaum. Datenqualität ist aber sowohl für die Motivation zum Datenteilen als auch für den effektiven Aufbau eines europäischen Datenökosystems zentral. Unter Punkt D führt der RfII aus, dass Qualitätsanforderungen im DGA über den Verweis auf die FAIR-Prinzipien noch hinausgehen müssen.[3]

A. Zugang für Forschung und Wissenschaft garantieren

Werden in Europa geschützte Daten des öffentlichen Sektors durch nicht exklusiv tätige Datentreuhänder zugänglich und nutzbar gemacht, so sollten auch diese neuen DSP bzw. *data sharing services (DSS)* dazu verpflichtet sein, Wissenschaftlerinnen und Wissenschaftlern (nur) zum Zweck der Durchführung von Forschungsprojekten ein unabdingbares Zugangsrecht zu den vorgehaltenen Daten zu gewähren und passende Zugangsregime einzurichten. Der RfII empfiehlt eine solche Forschungs- bzw. Wissenschaftsklausel mit Nachdruck.

Die Einführung einer Forschungsklausel ist aus Perspektive der Wissenschaft dringend notwendig. Die digitale Transformation darf die Randbedingungen für die wissenschaftliche Forschung nicht verschlechtern. Dies gilt konkret auch dann, wenn man das Zugangsmanagement für Daten auf eine intermediäre Ebene verlagert. Die öffentlich finanzierte Forschung ist auch in der Vergangenheit in den meisten Bereichen der public sector information (Medizin, öffentliches Archivwesen, Arbeitsmarktdaten, Umwelt- und Klimadaten, Kunst und Kulturgüter) aus gutem Grund beim Datenzugang privilegiert gewesen. Auch der DGA muss die Innovationsfähigkeit der Universitäten und öffentlich getragenen Forschungseinrichtungen in äquivalenter Weise sicherstellen. Hierfür bedarf es regulatorischer Leitplanken, die aber im Rahmen von Registrierungs- bzw. Akkreditierungsverfahren für DSP/DSS vereinbart werden können. Je nach Sensibilität der Daten können zwischen DSP/DSS und Forschungsakteuren unterschiedliche Zugangsregime greifen. Die Rolle der Wissenschaft – auch als Kooperationspartner für DSP/DSS – wird für den gelingenden Aufbau eines europäischen Datenökosystems von grundsätzlicher Bedeutung sein.

B. Anforderungen an Data Service Providers praxistauglich gestalten – Anreize setzen

Der Entwurf der DGA charakterisiert die neue Rolle eines DSP – sei dieser kommerziell oder datenaltruistisch – mittels der Fixierung von (Mindest-)Anforderungen an Unternehmen, die diese Funktion ausfüllen wollen: Zum Beispiel Registrierung, Verzicht auf Auswertung der Daten, Nutzung bestimmter Standardverträge etc. (vgl. Chapter III und IV DGA). Auch eine behördliche Überwachung ist geplant. Die vorgesehenen Anforderungen beschreiben Regeln, die das Handlungsfeld der DSP im Sinne der Gemeinwohlorientierung eingrenzen. Diese limitierenden Vorgaben stiften einerseits Rechtssicherheit und sind deshalb zu begrüßen. Andererseits fehlen im bisherigen Entwurf des DGA aber rechtliche Orientierungsmarken für die Ausgestaltung ökonomisch tragfähiger Geschäftsmodelle für DSP/DSS. Nur wenn DSP/DSS reale Chancen ha-

3 Zu den FAIR-Prinzipien siehe https://www.go-fair.org/fair-principles. Vgl. hierzu auch RfII (2020) – Herausforderung Datenqualität – Empfehlungen zur Zukunftsfähigkeit von Forschung im digitalen Wandel, S. 95ff.,http://www.rfii.de/?p=4203 (letzter Zugriff am 26.01.2021).

ben, sich am Markt dauerhaft zu etablieren, können sie das Teilen von Daten nachhaltig befördern. Der RfII plädiert erstens dafür, durch den DGA auch Anreize zu setzen, die potenziellen Anbietern den Eintritt in diesen Markt erleichtern und den Innovationswettbewerb fördern. Innovation kann nur auf Basis einer überprüfbaren, hochwertigen Datenbasis erzeugt werden, die hohen und höchsten Standards gerecht wird. Deshalb müssen zweitens im Rahmen des DGA konkretere Vorgaben für die Qualitätssicherung ergänzt werden, damit belastbares Vertrauen entstehen kann.

Der RfII regt zunächst an, datentreuhänderische Geschäftsmodelle, die mindestens kostendeckend, zum Beispiel im Rahmen einer bestehenden Einrichtung öffentlichen Rechts, gemeinnützig oder auch profitabel betrieben werden sollen, näher zu präzisieren und zur Etablierung von DSP bzw. DSS auch Anreize vorzusehen. Denn das Vertrauen von Datengebern in einen DSS wird nicht allein durch dessen Neutralität gesichert. Vielmehr zählen auch dessen nachhaltiger Datenumgang und seine ökonomische Stabilität. Die Rolle des neuen Intermediärs muss also unternehmerische Handlungsspielräume eröffnen. Dies gilt für kommerzielle wie für altruistische DSP gleichermaßen.

Da die Zwecke der Datenerhebung und Datenverwendung in Wirtschaft und Gesellschaft sehr differenziert sind, sollte ein europaweiter DGA aus Sicht des RfII keine One Size Fits All-Lösung anstreben. Vielmehr sollte ein Rechtsrahmen gesetzt werden, der den Bedürfnissen unterschiedlicher Sektoren und Akteure dient. Der RfII sieht hier zwei Anforderungsniveaus für DSP/DSS:

Für alle Daten, Dienste und Services, auf die sich der DGA erstreckt (siehe im Folgenden unter 1.), sollte ein allgemeinverbindlicher Rechtsrahmen gelten, der Mindeststandards für den datenbezogenen Vertrauensschutz (im Sinne der DSGVO)[4] und die Ermöglichung von nachhaltigen Geschäftsmodellen der Dienste und Services bietet. Die rechtlichen Anforderungen werden so gesetzt, dass sie zu einem Markteintritt einer Vielzahl von Diensten motivieren. Auch für kleine und mittlere Unternehmen sollten diese Anforderungen leicht umsetzbar sein. Auf einem zweiten Niveau (siehe im Folgenden unter 2.) verpflichten sich DSP und DSS, darüberhinausgehende Verpflichtungen einzugehen. Beispielsweise lassen sie sich bezüglich der Einhaltung besonders hoher Standards in der Datensicherheit und der Datenqualität zertifizieren. Beispiele für ein solches „Premiumsegment“ sind die akkreditierten Forschungsdatenzentren in der Wissenschaft. Mit einem solchen Stufenmodell kann je nach Datentyp, Verbraucherinteresse und Verwendungszweck ein breiter europäischer Wettbewerb entstehen.

1. Um die Etablierung von DSP in nachhaltiger Form grundsätzlich zu ermöglichen, empfiehlt der RfII als ergänzende Anforderungen für alle im Rahmen des DGA zu registrierenden Dienste und Services folgende Vorgaben zu berücksichtigen:

4 Siehe in diesem Sinne auch Verbraucherzentrale Bundesverband (2021) – Vertrauen stärken durch verbraucher-freundliche Daten-Governance, https://www.vzbv.de/sites/default/files/downloads/2021/01/13/21-01-12_vzbv-stellungnahme_data-governance-act.pdf (letzter Zugriff am 26.01.2021).

- Die Europäische Kommission und die Mitgliedstaaten setzen Impulse, um die Rahmenbedingungen für den Aufbau geeigneter Versicherungslösungen voranzutreiben, welche die Risiken für DSP absichern. Die Regelung von Haftungsfragen über Versicherungsmodelle fördert das öffentliche Vertrauen in die neuen Marktakteure. Zugleich müssten hier Lösungen gefunden werden, die auch für kleine und mittlere Unternehmen ebenso pragmatisch wie kostengünstig umsetzbar sind und ihnen den Aufbau nachhaltiger Geschäftsmodelle erleichtern. Mittelfristig prüfen die EU-Mitgliedstaaten die Voraussetzungen und Funktionsbedingungen für die eventuelle Einführung einer Pflichtversicherung für DSP.
- Bei Insolvenz eines DSP wie auch bei Geschäftsaufgabe und bei einer Geschäftsübergabe an ein Unternehmen anderen, nicht treuhänderischen Typs fallen die Daten an die öffentliche Hand. Beschließt diese die Löschung der Daten, besteht für sie keine Schadensersatzpflicht gegenüber den Datengebern.
- Wird ein DSS seitens einer öffentlichen Einrichtung betrieben, die ihre Rolle als DSP aufgibt, werden Haftungsregelungen für Datenverluste (analog zum unternehmerischen Insolvenzfall) begrenzt.
- Wird ein DSS durch eine wissenschaftliche Einrichtung zu wissenschaftlichen Zwecken betrieben, entfällt Artikel 11, Nr. 1 (die Metadatennutzung kann auch über die Weiterentwicklung des DSS hinausgehen).
- Die nationalen Behörden werden zusätzlich mit einer Beratungsfunktion ausgestattet, um Anbietern von Diensten für das Teilen von Daten eine Hilfestellung vor allem in Bezug auf die Klärung und Auslegung von Rechtsfragen zu ermöglichen, die im Zuge der Ausübung ihrer Tätigkeiten als DSP entstehen.
- Um eine weitgehend einheitliche Ausübung der Kontrollfunktion zu gewährleisten, sollte den nationalen Behörden hierzu ein Leitfaden bzw. Leitlinien an die Hand gegeben werden. Der Europäische Dateninnovationsrat (European Data Innovation Board) könnte mit der Aufgabe betraut werden, einen solchen Verständigungsprozess zu moderieren und für die Formulierung und Anwendung eines solchen Leitfadens Sorge zu tragen.
- Aufgrund der treibenden Rolle, die der öffentlich finanzierten Wissenschaft beim Aufbau eines europäischen Datenökosystems zukommt, müssen auch Akteure aus der Wissenschaft im Dateninnovationsrat angemessen repräsentiert sein.

2. Für DSP, die ihr Geschäftsmodell auch auf dem zweiten Niveau ansiedeln wollen (s.o.), gelten weitgehendere Regulierungen, deren Einhaltung Datengebern und -nutzern die Einhaltung höchster Standards bei der Weitergabe von Daten signalisieren. Für diese Kategorie von DSP empfiehlt der RfII folgende Ergänzungen im DGA:

- Die behördliche Aufsicht hat nicht nur eine Kontroll-, sondern auch eine Zertifizierungsfunktion, die der RfII als essentiell für die Frage der Qualitätssicherung von Daten und Diensten betrachtet. Diese kann auch – und aus wissenschaftlicher Perspektive: bevorzugt – im Rahmen eines noch zu entwickelnden, pragmatisch an den Erfordernissen der

unterschiedlichen Geschäftsmodelle ausgerichteten Akkreditierungsverfahrens ausgestaltet werden.

- Anbieter des zweiten Niveaus werden in einem öffentlich geführten Register aufgeführt, das Verbraucherinnen und Verbrauchern sowie weiteren Nutzerkreisen als Orientierung im Bereich der besonders vertrauenswürdigen und qualitativ hochwertigen Dienste dienen kann. Dies ist ein zusätzlicher Anreiz für DSP, sich um eine Zertifizierung zu bemühen.
- DSP bieten zum Beispiel für kritische oder besonders hochwertige Daten einen erhöhten Versicherungsschutz an, der sowohl Datengebern als auch Datennutzern als Orientierungsmarke für die Sensibilität dieser Daten sowie für besondere Anstrengungen bei der Datensicherheit und Qualitätsprüfung dienen kann.

C. Datenaltruismus klarer konturieren

Der Entwurf des DGA führt den Begriff des Datenaltruismus in die europäische Gesetzgebung zu Datenservices und Datennutzung ein – und zwar zum einen zur Beschreibung eines Motivs für Datensubjekte bzw. originäre Datengeber zur Weitergabe von Daten an DSP/DSS, zum anderen aber auch als Merkmal eines DSP, da diese sich als *data altruism organisation recognised* in the Union registrieren lassen können.

Der Entwurf der DGA beschreibt hierbei bislang als zentrales Kriterium für Datenaltruismus den Registrierungsvorgang. Die kennzeichnenden Merkmale, die eine datenaltruistische Organisation von anderen Organisationen unterscheiden, werden nicht benannt. Dies eröffnet weite Interpretationsspielräume im bisherigen Normentext. Was „Altruismus“ in diesem Zusammenhang bedeutet, muss geklärt werden

- bezüglich des Zweckes, für den die Daten gesammelt und zum Teilen bereitgestellt werden (z.B. Verwendung für die Medizinforschung, im Sport oder Kulturbereich etc.),
- hinsichtlich der Art des Datenhandelns (z.B. hohe Qualitätsstandards bzgl. Green-IT/ Klimaneutralität ihrer Datenhaltung),
- mit Blick auf die „Gemeinnützigkeit“ im Sinne eines Non-Profit-Geschäftsmodells.

Der RfII empfiehlt auch in diesem Punkt eine Präzisierung, welche erstens Datenaltruismus als ökonomisches Kriterium konkret beschreibt *(non-profit* bzw. Absehen von Gewinninteresse, gegebenenfalls auch aufgrund einer hierzu vorgesehenen Gesellschaftsform) und zweitens die klare Unterscheidbarkeit von kommerziellen und „altruistischen“ DSP/DSS sicherstellt. Sofern Datenaltruismus durch den DGA gezielt gefördert werden soll, sollte der gesamtgesellschaftliche Vorteil dieser Form der Daten(weiter)gabe konkreter beschrieben werden (Gemeinwohlorientierung, Förderung zivilgesellschaftlicher Innovationen etc.).

Darüber hinaus sollte Artikel 22 des Entwurfs des DGA um Präzisierungen für die (Mindest-) Anforderungen an ein Einwilligungsformular angereichert werden. Ein die oben geforderte Forschungsklausel sinnvoll ergänzendes Ziel ist es, ein transparentes Einwilligungsmodell zur Ermöglichung bestimmter datenintensiver und datenverknüpfender Forschungsverfahren zu etablieren. Hier bieten sich technikgestützte Verfahren an, die standardisiert werden sollten.

D. Qualität von Daten und Datenintermediären: Über FAIR hinausdenken

Der RfII ist sich der Herausforderungen bewusst, die damit verbunden sind, einen europaweiten Rechtsrahmen für die Weiterverwendung geschützter Daten des öffentlichen Sektors zu formulieren und Grundlagen für einen vertrauensvollen Aufbau von DSP/DSS zu schaffen. Er möchte daher grundsätzlich anregen, Fragen der Qualität von Daten und datenbezogenen Services umfassender im Data Governance Act zu berücksichtigen. Angelehnt an die oben formulierten Empfehlungen sollten weitere Mechanismen der Qualitätssicherung vorgesehen werden – insbesondere Leitlinien für die Kontrolle und Klassifizierung der Qualität von Daten, die der DSP aufnimmt, gegebenenfalls aufbereitet und durch seine DSS bereitstellt. Hierbei wären die Datengeber/-produzenten angemessen zu beteiligen. Sofern es sich beispielsweise um Forschungsdaten handelt, ist primär die datengebende wissenschaftliche Einrichtung für die Datenqualität verantwortlich. Sie muss in Fragen der Eingangskontrolle, Klassifizierung und Aufbereitung der Daten durch den DSP einbezogen werden.

In Bezug auf die Qualität der Daten betrachtet der RfII einen bloßen Verweis auf die FAIR-Prinzipien als nicht hinreichend. Nicht nur aus Sicht der Wissenschaft und nicht nur mit Blick auf die wissenschaftliche Nutzbarkeit von Daten wäre es sinnvoll, wenn die DSP/DSS zumindest auch Angaben zur Qualität der bereitgestellten Daten mitliefern. Auch Daten, die nicht für Forschungszwecke Verwendung finden, haben nur dann einen Mehrwert für Innovationsketten in Wirtschaft und Gesellschaft, wenn sie mindestens im Rahmen ihrer Metadaten Auskunft zu ihrer Provenienz und anderen Kontexten ihrer Entstehung bzw. „Herstellung“ und ihres bisherigen Transfers bieten. Eine transparent gestaltete Kommunikation zwischen dem DSP und den Datengebern/-produzenten ist auch an dieser Schnittstelle nötig.

Die Forschung kann bezüglich einer verantwortlichen und transparenten Data Governance im Allgemeinen sowie eines vertrauensvollen Umgangs mit personenbezogenen Daten im Besonderen Best Practices als Orientierungspunkte für einen gesamtgesellschaftlich wirksamen DGA beisteuern. Dies zeigen unter anderem die im Bereich der medizinischen Forschung angewandten und etablierten Datenschutzkonzepte. Im vorliegenden Entwurf des DGA vermisst der RfII bislang Ausführungen, die beispielsweise dazu beitragen, dass das Risiko der Re-Identifikation bei der Bereitstellung personenbezogener Daten durch die künftigen DSP/DSS hinreichend berücksichtigt und minimiert wird. Erst solche Vorkehrungen schaffen das Vertrauen, auf dem ein florierender gemeinwohl- und innovationsfördernder Markt für Daten aufbauen kann. Mit Blick auf Anonymisierungstechniken unterstützt der RfII Vorhaben, auf europaweit gültige Standards hinzuwirken.

Der Rat für Informationsinfrastrukturen (RfII) wurde von der Gemeinsamen Wissenschaftskonferenz (GWK) eingerichtet, um Bund, Länder und Wissenschaftseinrichtungen bei der Weiterentwicklung wissenschaftlicher Informationsinfrastrukturen und zu verwandten Themen des digitalen Wandels in der Wissenschaft zu beraten. Bei seinen Überlegungen zu diesen Themen legt der RfII großen Wert auf eine ausgewogene Berücksichtigung der sich teilweise überschneidenden Bedürfnisse von Wissenschaft, öffentlicher Verwaltung und Wirtschaft sowie der damit verbundenen Aspekte der internationalen Zusammenarbeit.

April 2020

Datentreuhandstellen gestalten – Zu Erfahrungen der Wissenschaft

Die Bundesregierung befasst sich in der Ausarbeitung ihrer Datenstrategie mit dem Thema Datentreuhänderschaft. Sie verweist in einem Eckpunktepapier darauf, dass Anstrengungen unternommen werden, um die „verantwortungsvolle Bereitstellung und Nutzung von Daten durch Personen und Institutionen (…) signifikant zu steigern."[1] Dabei sollen neue Datenmonopole verhindert und eine „gerechte Teilhabe" gesichert werden. Ebenso hat die Europäische Kommission in ihrer Datenstrategie befürwortet, Datenpools „in strategischen Sektoren und Bereichen von öffentlichem Interesse" einzurichten, die – auch unter dem Gemeinwohlaspekt – den Datenzugang für verschiedene Akteure erleichtern sollen.[2]

Der Diskurs über Datentreuhänder will also auf das Problem, wie Daten auf eine dem Wettbewerb ein Stück weit entzogene Form von neutraler Seite bereitgehalten werden können, eine Antwort finden. Die Debatte hierzu ist eine primär außerwissenschaftliche, sie weist allerdings einige Analogien zu Aushandlungsprozessen in der Wissenschaft auf. So geht es um Austausch und um eine faire Nutzbarkeit der Daten, was beispielsweise bedeuten kann, dass unter mehreren Akteuren ein gleichberechtigter Zugriff auf Daten gewährleistet ist. Datentreuhänder können dazu motivieren, dass mehr als bislang Datenbestände zusammengeführt werden. Dies kann innovationspolitischen Interessen dienen, birgt aber auch erhebliches Potenzial zur Lösung großer gesellschaftlicher Herausforderungen in Bereichen wie Gesundheit, Klima, Mobilität oder Bekämpfung von Armutsursachen. Datentreuhänder können auch zum Einsatz kommen, wo ein Datenaustausch unter Akteuren in Konstellationen starker Machtasymmetrie oder Konkurrenz organisiert werden soll – zum Beispiel zwischen global agierenden Anbietern von Internetplattformen, Start-ups, Forschenden oder individuellen Verbraucherinnen und Verbrauchern.

Derzeit wird über das Konzept der Datentreuhänderschaft ergebnisoffen, aber auch vage diskutiert. Es besteht noch kein öffentliches oder politisches Einverständnis darüber, wie Datentreuhänder beziehungsweise Datentreuhandstellen aufgebaut sein sollen.[3]

Der RfII nimmt diese Überlegungen mit Aufmerksamkeit zur Kenntnis. Für die Erschließung neuer Datensätze und für deren Weiternutzung ist die Grundidee der nachhaltigen Bereitstellung von datenbasierten Dienstleistungen seitens neutraler Stellen, die Nutzerinnen und Nut-

1 Die Bundesregierung (2019): Eckpunkte einer Datenstrategie, S. 1.
2 Europäische Kommission (2020): Eine europäische Datenstrategie. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Brüssel, S. 25.
3 Auch die vom Bundesministerium für Wirtschaft und Energie eingesetzte Kommission „Wettbewerbsrecht 4.0" hat in ihrem Bericht 2019 zunächst lediglich befürwortet, die Einrichtung von Datentreuhändern und die verschiedenen Modelle zu prüfen. Siehe BMWi- Bundesministerium für Wirtschaft und Energie (2019): Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft. Bericht der Kommission Wettbewerbsrecht 4.0.

zern faire Bedingungen anbieten, von hoher Relevanz. Datentreuhänder könnten Teil einer gesamtgesellschaftlichen Dateninfrastruktur werden.

Aus dieser Grundidee ergeben sich allerdings erhebliche Anforderungen an die konkrete Ausgestaltung einer solchen Treuhänderrolle, an den zu garantierenden vertrauensvollen Umgang mit personenbezogenen und anderweitig sensiblen Daten sowie an die Voraussetzungen ihrer sicheren, langfristigen Aufbewahrung. Der RfII regt, um hier von existierenden Vorbildern zu lernen, einen Erfahrungsaustausch mit der Wissenschaft an: Wissenschaftliche Fachgemeinschaften/Communities verfügen bereits über eine längere Tradition des fairen Teilens qualitätsgesicherter Daten und haben Regularien entwickelt, um die Rechte von Datengebern zu sichern. Zugleich hat die Wissenschaft auch eigene Erwartungen an Datentreuhandstellen, die außerhalb der Wissenschaft entstehen.[4]

Der RfII ist ein Beratungsgremium, das sich mit dem Aufbau und der Weiterentwicklung von Informationsinfrastrukturen in der Wissenschaft befasst. Vor diesem Hintergrund ordnet er das Konzept der Datentreuhänderschaft begrifflich ein und formuliert Empfehlungen hinsichtlich der Ausgestaltung von Datentreuhandstellen in der Zivilgesellschaft und in der Wirtschaft, vor allem – aber nicht nur – mit einem besonderen Blick auf deren Nutzen für Forschung und Entwicklung.

BEGRIFFSKLÄRUNG

Allgemeines zum Treuhandbegriff

Die Vorstellung einer treuhänderischen Übernahme von Verantwortung oder Pflichten hat eine vielfältige Tradition. Sie wird hier nur kurz umrissen – auch um deutlich zu machen, dass Gestaltungsspielräume bestehen.

Im **juristischen Verständnis** ist die **Treuhänderschaft** ein Rechtsverhältnis zwischen einem Treuhänder *(fiduciary/trustee)* und einem **Treugeber**: Dem Treuhänder werden seitens des Treugebers bestimmte Rechte im Hinblick auf das Treugut übertragen oder eingeräumt, die der Treuhänder im Außenverhältnis im eigenen oder auch fremden Namen wahrnehmen darf. Im Verhältnis zum Treugeber bleibt er dennoch an vereinbarte Vorgaben, Bedingungen und Grenzen gebunden, wobei der Treuhandvertrag gesetzlich nicht im Detail geregelt ist. Je nach Treuhandverhältnis sind daher verschiedene rechtliche Regelungen anwendbar. Ein Treuhandverhältnis kann zur Sicherung der Interessen des Treuhänders („eigennützige Treuhand“) oder der Interessen des Treugebers („fremdnützige Treuhand“) begründet werden. Ein Treuhänder kann aber insbesondere auch im Falle widerstreitender Interessen verschiedener Personen tätig werden („doppelseitige Treuhand“). Im letzteren Fall dient das Treuhandverhältnis dazu,

4 Vgl. hierzu RatSWD- Rat für Sozial- und Wirtschaftsdaten (2019): Big Data in den Sozial-, Verhaltens- und Wirtschaftswissenschaften: Datenzugang und Forschungsdatenmanagement, Berlin, S. 21ff. Der RatSWD formuliert hier auch bereits einen Aufgaben- und Kriterienkatalog für die Ausgestaltung einer Datentreuhandstelle in den Wirtschafts- und Sozialwissenschaften.

den Interessen der Beteiligten durch die Einschaltung eines in der Sache uneigennützig handelnden und vertrauenswürdigen Dritten gerecht zu werden.

Der **wirtschaftliche Treuhandbegriff** ist demgegenüber weiter gefasst, indem hier bereits die Wahrnehmung fremder Interessen als Treuhandschaft verstanden werden kann. Auch im **englischsprachigen Kontext** kann *trustee* ganz allgemein einen vertrauenswürdigen Verwalter meinen. An solche offenen, eher pragmatischen Vorstellungen von der Treuhänderrolle schließt auch die Diskussion über Datentreuhandstellen an.[5]

Datentreuhänder

Der Begriff des „Datentreuhänders" hat sich im Digitalisierungsdiskurs als Metapher oder Analogie für Stellen herausgebildet, die in besonderer Weise als Intermediäre zwischen einem oder mehreren Datengebern und einer Nachfrageseite agieren. Es gibt bereits eine Reihe von Beschreibungen und Anwendungsfeldern. Für Anwendungsfälle im Medizinbereich wird ein Datentreuhänder beispielsweise definiert als eine „rechtlich, räumlich und personell selbstständige und unabhängige Stelle, die idealerweise einer besonderen Geheimhaltungspflicht unterliegt".[6] Der Begriff wird zum Teil auch weiter gefasst. So definiert die Bundesdruckerei einen Datentreuhänder als „eine unabhängige Vertrauensinstanz, die Daten zwischen Datengeber und Datennutzer sicher und gesetzeskonform vermittelt.[7] Dies kann insbesondere bedeuten, dass der Datentreuhänder im Falle personenbezogener Daten Aufgaben der Pseudonymisierung oder der Anonymisierung wahrnimmt und die Daten nur pseudonymisiert, anonymisiert oder aggregiert zur Verfügung gestellt werden.

Innerhalb der Wissenschaft bestehen keine Treuhandverhältnisse im engeren juristischen Sinn. Dennoch nehmen wissenschaftliche Institutionen die Rolle neutraler, das heißt nicht-kommerzieller und inhaltlich unabhängiger Datenarchive wahr. Ein Beispiel sind hier Biobanken oder auch Forschungsdatenzentren in den Sozial- und Wirtschaftswissenschaften.

Rechts- und digitalpolitische Forderungen nach der Schaffung sowie gegebenenfalls auch Kodifizierung der Rolle eines oder mehrerer Datentreuhänder sind vergleichsweise neu. Sie werden beispielsweise im Zusammenhang mit besonders umfangreichen (und häufig zugleich in ihrer Integrität schutzbedürftigen) Datensätzen artikuliert, die durch den Einsatz neuer IT-gestützter Datenverarbeitung anfallen. So besteht ein erhebliches Interesse daran, **Medizin-, Mobilitäts- oder Nutzungsdaten,** die im wirtschaftlichen Kontext oder in Alltagsanwendungen des Internets der Dinge produziert werden, besser für die Weiterverwendung zu erschließen, das heißt für Dritte, die Gesellschaft oder die Forschung nutzbar zu machen. Im zivilgesellschaftlichen Bereich werden Datentreuhandsysteme auch als Option für einen faireren und stärker **selbst-**

---

5 Insbesondere wird so auf die Idee von Dateneigentum verzichtet. Vgl. hierzu die Empfehlung der Datenethikkommission; Datenethikkommission der Bundesregierung (2019): Gutachten der Datenethikkommission, Berlin, S. 18.

6 Pommerening, Klaus et al. (2014): Leitfaden zum Datenschutz in medizinischen Forschungsprojekten. Generische Lösungen der TMF 2.0 (Schriftenreihe der TMF, 11), Berlin, S. 209.

7 https://www.bundesdruckerei.de/system/files/dokumente/pdf/BDR.de_Datentreuhaender.pdf (zuletzt geprüft am: 03.04.2020). Vgl. zur Definition des Datentreuhänders u.a. auch RatSWD- Rat für Sozial- und Wirtschaftsdaten (2017): Handreichung Datenschutz (RatSWD Output, 5 (5)), Berlin, S. 16.

bestimmten Umgang mit Verbraucherdaten diskutiert *(Personal Data Trusts, Personal Information Management Systems)*. Hier steht die individuelle Datensouveränität im Vordergrund. Die Datenethikkommission der Bundesregierung hat in diesem Kontext allerdings ausdrücklich darauf aufmerksam gemacht, dass der Einzelne vor „vermeintlichen Interessenverwaltern", die vor allem wirtschaftliche Eigeninteressen vertreten, zu schützen sei.[8]

EMPFEHLUNGEN

Aus Sicht des RfII können etablierte Praktiken des Datenzugangs und der Datennutzung in der Wissenschaft auch als Rollenmodell für den Aufbau von Dateninfrastrukturen in anderen gesellschaftlichen Teilbereichen fungieren. An den Fernerkundungsdaten der großen Satellitenmissionen lässt sich beispielsweise zeigen, wie ein **faires Teilen von Daten** im Rahmen **größerer Fachgemeinschaften/Communities** gut funktionieren kann und für diese eine langfristige Nutzbarkeit sicherstellt. Erst dadurch wird die Erforschung komplexer Systemzusammenhänge überhaupt ermöglicht. Die Großforschung, etwa am Large Hadron Collider des CERN, ist mit ihrer **hochkomplexen, arbeitsteiligen Datenarchivierung** ein Beispiel dafür, wie Forschenden weltweit eine Nutzung großer Datenmengen unter Gewährleistung verbindlicher Standards für die Datenqualität ermöglicht werden kann. Das räumlich dezentrale, aber sachlich zentral koordinierte deutsche Bibliothekssystem verfügt über seit Jahrhunderten sich evolutionär entwickelnde Formen der Metadatenvergabe. Die **Forschungsdatenzentren in den Sozial- und Wirtschaftswissenschaften** liefern Modelle für den rechtskonformen Zugang zu und die Nachnutzung von Daten, die aus Gründen des unternehmerischen Eigentums oder des Datenschutzes sensibel sind. Diese Beispiele aus der Wissenschaft zeigen, wie ein mit einheitlichen Standards qualitätsgesicherter und gleichzeitig unter mehreren Akteuren fair organisierter Datenaustausch aufgebaut werden kann.

Ausgehend von diesen Erfahrungen versteht der RfII Datentreuhandstellen nachfolgend in einem institutionellen Sinn, nämlich als eine Dateninfrastruktur besonderen Typs.

Dateninfrastrukturen für Wissenschaft, Wirtschaft und Gesellschaft gut ausbalanciert gestalten

Die aktuellen Diskussionen zur Intensivierung der Nutzung von Daten und zur Etablierung von Modellen der Datentreuhänderschaft zeigen der Politik Wege auf, in welche Richtung die zahlreichen Projekte und Initiativen im Bereich der Dateninfrastrukturen strategisch weiterentwickelt werden sollten. In der International *Data Spaces Association* entsteht ein Referenzmodell für Plattformen, die Unternehmen den Zugang, die Nutzung und den sicheren Austausch von Daten erleichtern wollen. Mit dem Projekt GAIA-X wird für Unternehmen und Organisationen ein europaweit offenes „Ökosystem" vertrauenswürdiger Werkzeuge, Dienstleistungen sowie Speicher- und Rechenkapazitäten angestrebt. Mit Blick auf Gemeinwohl und innovationspoliti-

8 Datenethikkommission (2019): Gutachten der Datenethikkommission, S. 21.

sche Ziele will die EU-Kommission sogenannte „Datenpools“ für spezifische Sektoren einrichten, darunter Industrie, Umwelt und Gesundheit.[9] Weltweit erschließen Behörden ihre Datenbestände und stellen sie über Portale wie Transparenzregister, GovData oder das *European Data Portal* zur Verfügung. Ganz ähnliche Anstrengungen werden unter den besonderen Vorzeichen von Wissenschaft seit einigen Jahren mit der Einrichtung von wissenschaftlichen Datenzentren für die Forschung unternommen.

Der Charakter von Unternehmens- und Verbraucherdaten kann sich von denen der wissenschaftlichen Datenbestände unterscheiden. Beiden gemeinsam ist allerdings, dass sie bestimmte Qualitätsmerkmale erfüllen müssen. Auch Kriterien wie Vertrauenswürdigkeit, Rechtskonformität sowie Transparenz des Zugangs haben in beiden Welten den gleichen Wert. In diesen Punkten können sich die Interessen der Marktteilnehmer wie auch von Wissenschaft, Politik und Gesellschaft treffen.

Die **Idee eines Systems von „Treuhandstellen“,** die einem Grundkonzept der gleichermaßen effektiven wie rechtskonformen und im Sinne der Datensouveränität nachvollziehbaren Nutzung von qualitätsgesicherten Datenbeständen folgt, erscheint dem RfII daher überaus sinnvoll für die Entwicklung einer Datenstrategie. Ein Ausbau solcher Dateninfrastrukturen sollte **mit gesamtgesellschaftlichem Auftrag** vorangetrieben werden, gegebenenfalls mit öffentlicher Förderung. Allerdings sollte auch genau geprüft werden, in welchen Bereichen Treuhandmodelle funktionieren und ob sie – ihrer Zielsetzung entsprechend qualitätsgesicherte – Datenbestände zusammenführen oder einen Datenaustausch zwischen verteilten Ressourcen koordinieren sollen.

Zugang für Forschung und Entwicklung sichern

Der RfII sieht in Datentreuhandstellen ein großes Potenzial, sowohl einen vertrauensvollen Austausch von Daten nicht nur innerhalb eines Sektors (u. a. Kooperation unter Wettbewerbern in Innovationsprozessen der Industrie, Verfügbarmachung und Zusammenführung von gesundheitsrelevanten Daten, Verwaltungsdaten, etc.) zu organisieren, als auch im Sinne von Schnittstellen zwischen Wissenschaft, Wirtschaft und Gesellschaft zu fungieren. Hierdurch ließe sich das wirtschaftliche und gemeinwohlorientierte **Innovationspotenzial** ausschöpfen, das mit *data sharing* verbunden ist.

In Fällen, in denen die öffentliche Hand als Treuhandstelle fungiert, ist es aus Sicht des RfII wichtig, dass ein möglichst weitreichender Datenzugang für Forschung und Entwicklung gewährleistet wird. Wenn unter wettbewerbsrechtlichen Aspekten Regulierungsmaßnahmen ergriffen werden, um die Daten großer Plattformen auch für andere Marktteilnehmer zu öffnen,[10] dann sollte ein solcher **Zugang** auch und erst recht öffentlich geförderter Forschung **in sachgerechtem Umfang** eingeräumt werden.

---

9 Europäische Kommission (2020): Eine europäische Datenstrategie.

10 Dies sieht zurzeit beispielsweise ein Konzept der Projektgruppe „KI und Wirtschaft“ der Enquete Kommission „Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale“ vor: Projektgruppe „KI und Wirtschaft“ (2019): Zusammenfassung der vorläufigen Ergebnisse, Stand: 18. Dezember 2019.

Der RfII möchte die Bedarfe der Wissenschaft in diesem Prozess deutlich artikulieren: Sektorale Datenmonopole oder andere sachwidrige Beschränkungen des Zugangs für die Wissenschaft sind zu vermeiden. Demnach wäre in Regelungsvorhaben jeweils eine **Forschungsklausel** zu etablieren, in der die Belange der Forschung in sachgerechter Art und Weise berücksichtigt sind.

Darüber hinaus gibt es zahlreiche Anwendungsbeispiele für Datenplattformen, in denen sich ein Datenzugang durch Forschungsverträge, Kooperationsvereinbarungen oder das Bereitstellen von Forschungsdatensätzen erreichen lässt. Treuhandstellen können hier je nach Schutzstufe der Daten eine Vielzahl an Aufgaben wahrnehmen, bis hin zur Entwicklung von Datenprodukten für spezifische Nachnutzungsfälle und unterschiedliche Zielgruppen. Derartige Szenarien sind bereits in der Forschung erprobt und werden in zahlreichen Anwendungsbereichen schon mit Erfolg eingesetzt.

Qualitätssicherung für Treuhandstellen etablieren

Datentreuhänder sollen als Vertrauensinstanz transparent und fair eine Nutzung von Daten für möglicherweise auch miteinander konkurrierende Akteure organisieren. Eine weitergehende Festlegung der funktionalen Dimensionen, die solche Infrastrukturen zu erfüllen haben, steht allerdings noch aus. Um einer künftig inflationären Verwendung des Datentreuhänder-Begriffs vorzubeugen, schlägt der RfII vor, für solch neutrale, anerkannte Vertrauensinstanzen **die Bezeichnung „Datentreuhandstelle“** zu etablieren und diese Bezeichnung durch ein Siegel oder eine Zertifizierung zu **schützen**. Aus Sicht des RfII sollte mit dem Begriff ein Qualitätsanspruch verbunden sein, der durch entsprechende Qualitätssicherungsmaßnahmen untermauert wird und die gewünschte Neutralität sichert. Bei der Festlegung der hierfür erforderlichen Kriterien sollte auch die Datenqualität Berücksichtigung finden.[11] Auch wenn Datentreuhandstellen nicht explizit für die Qualitätssicherung der Daten zuständig sind beziehungsweise sein sollten, so müssten sie zumindest eine Beurteilung der bereitgestellten Daten ermöglichen und Informationen über die Qualität der Daten an die Nutzerinnen und Nutzer weitergeben.

Da sowohl die Daten in ihrer Sensibilität als auch die geplanten Nutzungen und die jeweils damit verbundenen Bedingungen große Unterschiede aufweisen können, bietet es sich an, verschiedene Stufen von Qualitätsgarantien für die Vertrauensinstanzen vorzusehen. So werden bei hoher Kritikalität und großem Risikopotenzial Überprüfungen durch Dritte, etwa unabhängige Zertifizierungsstellen oder staatliche Überwachungsstellen, notwendig sein. Bei geringerer Kritikalität können auch Selbstverpflichtungsmechanismen zum Beispiel über *Codes of Conduct* erwogen werden. Die Wissenschaft kennt solche Stufenmodelle beispielsweise in der Zer-

11 Vgl. hierzu RfII- Rat für Informationsinfrastrukturen (2019): Herausforderung Datenqualität – Empfehlungen zur Zukunftsfähigkeit von Forschung im digitalen Wandel, 2. Aufl., Göttingen.

tifizierung „vertrauenswürdiger Langzeitarchive“.[12] Der Erwerb von Siegeln oder Akkreditierungen beinhaltet zudem oftmals die Aufnahme in eine Community of Practice, in der die Datenzentren Erfahrungsaustausch und laufende Weiterentwicklung der Verfahren organisieren.

Ausgestaltung und Regulierung von Datentreuhandstellen sektorenübergreifend voranbringen

Der RfII regt an, zeitnah Gespräche zwischen den Akteuren in Politik, Wirtschaft, Verwaltung und Wissenschaft anzustoßen, um konkrete Ansätze für ein System zertifizierter Datentreuhandstellen zu entwickeln – letztlich auch mit Blick auf die europäische Ebene. In diesen Prozess sollte die Wissenschaft nicht nur ihre Erfahrungen mit der Regelung des Zugangs und der Nutzung von Daten einbringen, sondern auch ihre eigenen spezifischen Bedarfe artikulieren. Gestaltungsmerkmale und Regulierungen für Datentreuhandstellen werden insbesondere in Abhängigkeit von Kritikalität der jeweils bereitgestellten Daten und der Nutzungszwecke festzulegen sein. Eine **Förderung von Vorhaben,** die Anforderungen und Regelungsbedarfe detaillierter ausarbeiten, wäre ein hilfreicher Impuls, um den Aufbau solcher Dateninfrastrukturen kontrolliert voranzubringen.

12 Konformität kann hier in unterschiedlich detaillierter Form vom peer-review-gestützten Selbstevaluierungsverfahren des sogenannten Core Trust Seal bis hin zu einem formalen externen Audit nachgewiesen werden. Grundlage ist jeweils das OAIS-Referenzmodell (ISO-Standard 14721).

D. MITWIRKENDE

MITGLIEDER DES RATES (STAND: JUNI 2023)

Vertretung der wissenschaftlichen Nutzer

Prof. Dr. Marion Albers
Universität Hamburg – Juristische Fakultät

Prof. Dr. Stefan Decker
FIT – Fraunhofer-Institut für Angewandte Informationstechnik

Prof. Dr. Petra Gehring (Vorsitzende)
Technische Universität Darmstadt – Institut für Philosophie

Prof. Dr. Kurt Kremer
MPI – Max-Planck-Institut für Polymerforschung Mainz

Prof. Dr. Wolfgang Marquardt
Forschungszentrum Jülich GmbH

Prof. Dr. Stefanie Speidel
Nationales Centrum für Tumorerkrankungen Dresden (NCT/UCC)

Prof. Dr. Joachim Wambsganß
ZAH – Zentrum für Astronomie der Universität Heidelberg

Vertretung der Einrichtungen

Prof. Dr. Sören Auer
TIB – Technische Informationsbibliothek Hannover

Prof. Dr. Lars Bernard (stellv. Vorsitzender)
Technische Universität Dresden

Prof. Dr. Barbara Helwing (stellv. Vorsitzende)
Vorderasiatisches Museum Berlin – SMB SPK

Prof. Dr. Beatrice Rammstedt
Leibniz Institut für Sozialwissenschaften – GESIS Mannheim

Prof. Dr. Sandra Richter
DLA – Deutsches Literaturarchiv Marbach

Prof. Dr. Gerhard Sagerer
Universität Bielefeld

Katrin Stump
Sächsische Landesbibliothek – Staats- und Universitätsbibliothek Dresden

Prof. Dr. Ramin Yahyapour
GWDG – Gesellschaft für Wissenschaftliche Datenverarbeitung mbH Göttingen

Vertretung von Bund und Ländern

Rüdiger Eichel
Niedersächsisches Ministerium für Wissenschaft und Kultur

Dr. Christiane Fricke
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

Dr. Dietrich Nelle
Bundesministerium für Bildung und Forschung

Marion Steinberger
Bundesministerium für Bildung und Forschung

Vertretung des öffentlichen Lebens

Dr. Anke Beck
Frontiers

Dr. h.c. Marit Hansen
Landesbeauftragte für Datenschutz Schleswig-Holstein

Christine Regitz
SAP SE

Dr. Harald Schöning
Software AG

AG Datentreuhänderschaft

Dr. h.c. Marit Hansen (Leitung), Sabine Brünger-Weilandt, Prof. Dr. Petra Gehring, Dr. Nicola Jentzsch (Gast bis 04/2022), Dr. Dietrich Nelle, Prof. Dr. Stefanie Speidel, Prof. Dr. Doris Wedlich (†)

Gremienbetreuung

Die Arbeitsgruppe wurde seitens der RfII-Geschäftsstelle inhaltlich und organisatorisch begleitet von Dr. Kirsten Gerland und Dr. Stefan Lange.

Redaktion des Berichts

Dr. Kirsten Gerland, Dr. Stefan Lange, Dr. Beata Mache

DANK

Der RfII bedankt sich bei allen Expertinnen und Experten sowie Gästen, die sich an der Arbeit der Arbeitsgruppe Datentreuhänderschaft beteiligt haben.

Besonderer Dank gilt den Sachverständigen des Workshops 2020 sowie des Fachgesprächs 2022:

- Stefan Bender (Forschungsdaten- und Servicezentrum der Deutschen Bundesbank)
- Fred Blüthner (FSD Fahrzeugsystemdaten Zentrale Stelle nach StVG)
- Franziska Boehm (FIZ Karlsruhe/KIT Karlsruhe)
- Rainer Böhme (Universität Innsbruck)
- Lina Ehrig (Verbraucherzentrale Bundesverband)
- Thomas Ganslandt (Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V., TMF)
- Monika Jungbauer-Gans (Deutsches Zentrum für Hochschul- und Wissenschafts-forschung, DZHW und Vorsitzende des Rates für Sozial- und Wirtschaftsdaten, RatSWD)
- Christian Junger (MADANA)
- Tibor S. Pataki (Gesamtverband der Deutschen Versicherungswirtschaft, GDV)
- Jan Schallaböck (iRIGHTS)
- Egbert Schark (d-fine)
- Robert Schmitt (RWTH Aachen)
- Henning Schwabe (BASF)
- Rolf Schwartmann (TH Köln)
- Sebastian Semmler (Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V., TMF)
- Louisa Specht-Riemenschneider (Universität Bonn)
- Matthias Spielkamp (AlgorithmWatch)
- York Sure-Vetter (Direktor der NFDI)
- Ralf Wehrspohn (Vorstand der Fraunhofer-Gesellschaft)
- Christiane Wendehorst (Universität Wien)
- Thomas Zurek (SAP)