Juli 2021 · Aline Blankertz & Louisa Specht

Wie eine Regulierung für Datentreuhänder aussehen sollte

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Executive Summary

Datentreuhänder sind ein vielversprechendes Konzept, um Datennutzung zu ermöglichen und dabei Datenschutz beizubehalten. Datentreuhänder können viele Ziele verfolgen, wie die stärkere Teilhabe von Verbraucher:innen oder anderen Datensubjekten, die effektivere Umsetzung von Datenschutz oder die Stärkung von Datenaustausch entlang der Wertschöpfungskette. Sie haben das Potenzial, ein Alternativmodell zu werden zu den großen Plattformen, denen vorgeworfen wird, Datenmacht anzusammeln und diese primär für die eigenen Zwecke zu nutzen statt im Interesse ihrer Nutzer:innen. Um diese Hoffnungen zu erfüllen, müssen Datentreuhänder vertrauenswürdig sein, damit ihre Nutzer:innen verstehen und vertrauen, dass Daten in ihrem Interesse verwendet werden.

Dass die Politik das Potenzial von Datentreuhändern erkannt hat, ist ein wichtiger Schritt. Darauf sollten Maßnahmen folgen, die spezifische Risiken in den Blick nehmen und so Vertrauen in die Dienste fördern. Derzeit besteht die politische Strategie darin, durch eine „one size fits all"-Regulierung alle Formen von Datentreuhändern den gleichen Regeln zu unterwerfen. Das zeigt sich beispielsweise durch den Data Governance Act (DGA), der Datentreuhändern wenig Spielraum lässt, um sich am Markt durchzusetzen.

Um die Entwicklung von Datentreuhandmodellen zu fördern, ist es sinnvoller, Datentreuhandmodelle breit zu fassen als alle Organisationen, die Daten im Interesse anderer verwalten und sich dabei an den rechtlichen Rahmen (unter anderem Wettbewerb, Geschäftsgeheimnisse und Datenschutz) halten. Welche zusätzlichen vertrauensbildenden Regeln nötig sind, sollte je nach Anwendungsfall entschieden werden. Dabei sollten sowohl das Risiko verschiedener Anwendungsfälle Berücksichtigung finden als auch die Notwendigkeit von Anreizen, um als Datentreuhand tätig zu werden.

Risikofaktoren können sektorübergreifend identifiziert werden; insbesondere die zentrale oder dezentrale Datenspeicherung und die freiwillige oder verpflichtende Nutzung der Datentreuhand gehören dazu. Nicht dazu gehört das Geschäftsmodell: Auch wenn viele Regulierungsvorhaben eine umfassende Neutralität fordern, gibt es verschiedene Datentreuhandansätze, die ohne strikte Neutralität in Bezug auf Monetarisierung oder vertikale Integration vertrauenswürdig erscheinen. Zugleich ist unklar, welche Anreize für die Entwicklung strikt neutraler Datentreuhandmodelle bestehen. Neutralitätsanforderungen, die über das nötige Maß hinausgehen, machen es somit weniger wahrscheinlich, dass sich die gewünschten alternativen Modelle entwickeln und durchsetzen.

Wie eine risiko- und anreizbasierte Regulierung aussehen kann, lässt sich anhand von vier Anwendungsfällen zeigen (medizinische Daten, PIMS, Produktpässe und Agrardaten). Sie unterscheiden sich darin, welche Ziele sie verfolgen, ob Daten personenbezogen sind, wie risikobehaftet das Datenteilen ist und in welchem Umfang Daten bereits geteilt werden.

Der erste Anwendungsfall sind **medizinische Daten**, die ein enormes Potenzial für die medizinische Forschung bergen, um neue und stärker personalisierte Formen der Diagnose und Therapie zu entwickeln. Gleichzeitig sind die Daten sehr sensibel und umfassen neben aktuellen Behandlungsdaten auch mögliche zukünftige Risikofaktoren. Somit bestehen Risiken unter anderem in Form von selbstzensierendem Verhalten, Diskriminierung und auch der Fehlbehandlung, wenn Daten nicht mit der nötigen Sorgfalt interpretiert werden.

Um medizinische Daten umfassender zu nutzen, sollte ein Erlaubnistatbestand für die Datenverarbeitung für medizinische Forschung durch wissenschaftliche und kommerzielle Organisationen geschaffen werden, wenn die Daten von einer Datentreuhand bereitgestellt werden. Damit die Risiken beherrschbar bleiben, ist es notwendig, dass die IT-Sicherheit durch eine staatliche beaufsichtigte Stelle zertifiziert wird. Weiterhin sollte der Datenzugang so gestaltet sein, dass nur die für die Forschung notwendigen Daten zugänglich sind und der Personenbezug zum Beispiel mit Pseudonymisierung möglichst entfernt wird. Auch sollten Organisationen ausgeschlossen werden, die in Bereichen tätig sind, von denen leicht Diskriminierung ausgehen kann, wie etwa Versicherungen und Werbung.

Der zweite Anwendungsfall sind Personal Information Management Systems (**PIMS**), die Verbraucher:innen dabei helfen sollen, effektiver ihre Rechte und Interessen in Bezug auf Daten über sie durchzusetzen. Doch bisher nutzen Verbraucher:innen die Dienste nur zögerlich und Unternehmen wie große Plattformen haben es leicht, PIMS zu umgehen. Zugleich besteht im direkten Umgang mit Verbraucher:innen das Risiko von Missbrauch (z.B. durch irreführende Informationen und Menüführung).

Um die Risiken zu kontrollieren und gleichzeitig PIMS stärker zu ermöglichen, schlagen wir vor, Muster-Allgemeinen Geschäftsbedingungen (AGBs) für PIMS als Grundlage für eine Zertifizierung zu machen, die sie als vertrauenswürdig kennzeichnet. Diese AGBs sollten unter anderem Mindeststandards für IT-Sicherheit enthalten und eine explizite Einwilligung für die Monetarisierung personenbezogener Daten vorsehen. Weiterhin sollte es Transparenzvorgaben geben, die die monetäre und nicht-monetäre Übermittlung von Daten sichtbar machen. Auch Restriktionen für die Datennutzung der verbundenen Dienste sollten Teil der AGB sein, sodass sie unter gleichen Bedingungen stattfindet wie zu externen Diensten. Insgesamt sollte hier das Augenmerk darauf liegen, die PIMS an die Interessen der Nutzer:innen zu

binden. Auf dieser Grundlage können dann Unternehmen wie Social-Media-Plattformen dazu verpflichtet werden, mit zertifizierten PIMS zusammenzuarbeiten. Unter diesen Voraussetzungen ist es sinnvoll, dass PIMS Verbraucher:innen umfassender vertreten, also zum Beispiel die Erklärung und den Widerruf von Einwilligungen im Namen ihrer Nutzer:innen managen, wie es etwa für „authorized agents“ unter dem Californian Consumer Protection Act (CCPA) der Fall ist.

Der dritte Anwendungsfall sind **Produktpässe**, die es ermöglichen, Produkte und Produkteigenschaften über die Wertschöpfungskette hinweg nachzuverfolgen. Sie haben enormes Potenzial für die Förderung einer Kreislaufwirtschaft. Verschiedene Initiativen fördern die datenbasierte Wieder- und Weiterverwendung von Ressourcen, jedoch scheitern sie oft noch an hohem administrativem und finanziellem Aufwand und begrenzter Managementrelevanz.

Es ist nicht offensichtlich, dass es einer restriktiven Regulierung für Datentreuhänder bedürfte, die Produktpässe anbieten wollen. Stattdessen ist es eher vielversprechend, rechtliche Klarheit über das Datenteilen zwischen Unternehmen zu schaffen und staatliche Nachfrage strategisch zu nutzen, um bei der staatlichen Beschaffung die Nutzung von Produktpässen zu fördern.

Der vierte Anwendungsfall sind **Agrardaten**, die dabei helfen können, nicht nur landwirtschaftliche Erträge zu erhöhen, sondern auch Ressourcen gezielter einzusetzen. Sie werden zunehmend erhoben und genutzt, wobei ein wesentliches Hemmnis aktuell noch im teils zurückhaltenden Interesse an einer Digitalisierung von landwirtschaftlichen Betrieben besteht.

Eine regulatorische Einschränkung von Agrardatentreuhändern erscheint nicht geboten. Stattdessen können mehr Anreize gesetzt werden, zum Beispiel durch die verstärkte Bereitstellung staatlicher Daten für die Nutzung im Agrarbereich.

Sektorübergreifende Handlungsempfehlungen

Eine Regulierung von Datentreuhändern sollte bestehende Rechtsunsicherheit und Komplexität auf keinen Fall erhöhen, sondern senken. Dies ist nötig, um einen Anreiz für die Entwicklung neuer Modelle zu schaffen. Vertrauensstiftende Maßnahmen, die Risiken verringern, begründen auch das Absenken von Hürden. Übermäßig restriktive Neutralitätsanforderungen führen zwangsläufig dazu, dass Datentreuhänder nur vom Staat selbst bereitgestellt werden können, was andere potenzielle Probleme mit sich bringt. Stattdessen ist es zielführender, in den gesetzlichen Bestimmungen konkreten Interessenskonflikten vorzubeugen.

Zertifizierung kann sichtbar zu machen, ob konkret definierte Anforderungen erfüllt werden, insbesondere dann, wenn das Risiko einer zu restriktiven Regulierung hoch ist und etwa Informationsasymmetrien eine Intervention erforderlich machen. Eine weitere pragmatische Möglichkeit, Datentreuhandmodelle zu fördern, ist die Nutzung von Pilotprojekten und der strategische Einsatz staatlicher Nachfrage. Allerdings ersetzt dies nicht die Entwicklung neuer Modelle, insbesondere Geschäftsmodelle.

Ob Datentreuhänder die großen Hoffnungen erfüllen können, die auf sie gesetzt werden, hängt maßgeblich davon ab, wie der für sie geltende Rechtsrahmen gestaltet ist. Insgesamt sollten Regulierungsvorhaben für Datentreuhänder darauf abzielen, Datennutzung und Datenschutz besser vereinbar zu machen. Dafür ist es hilfreich, auf konkrete Risiken zu fokussieren, die durch den bestehenden Rechtsrahmen nicht abgedeckt sind; gleichzeitig aber auch Hürden abzubauen, die diesem Ziel im Wege stehen.

Inhalt

1. Einleitung

Datentreuhänder sind ein vielversprechendes Konzept, um Datennutzung zu ermöglichen und dabei Datenschutz beizubehalten – zu dieser Einschätzung kommen sowohl Politik, Wirtschaft als auch die Zivilgesellschaft.[1] Datentreuhänder haben das Potenzial, ein Alternativmodell zu werden zu den großen Plattformen, denen vorgeworfen wird, Datenmacht anzusammeln und diese primär für die eigenen Zwecke zu nutzen statt im Interesse ihrer Nutzer:innen.

Damit Datentreuhänder dieses Potential entfalten können, müssen sie als vertrauenswürdig wahrgenommen werden. Die aktuelle politische Strategie besteht darin, dieses Vertrauen durch eine neue, über den bestehenden Rechtsrahmen hinausgehende Regulierung zu erreichen: Allen Datendiensten werden etwa durch den Data Governance Act (DGA) dieselben Anforderungen auferlegt.

Solche „one size fits all"-Regulierungsansätze riskieren allerdings, dass Datentreuhänder sich gar nicht erst etablieren können, weil sie sich an Regeln halten **müssen**, die das Potenzial und die Risiken ihres konkreten Anwendungsfalls nicht berücksichtigen. Dabei sind die Einsatzgebiete, in denen Datenintermediären Vorteile bieten können, schon heute divers: von Personal Information Management Systems (PIMS)/Einwilligungsassistenten,[2] dem Gesundheitskontext,[3] Forschungsdatenzentren[4] hin zu Datenhubs für vernetzte Autos.[5]

Statt all diese Szenarien gleich zu behandeln, bedarf es einer risikobasierten Regulierung, die Sicherheit und Vertrauenswürdigkeit gewährleistet und auch Innovationen zulässt und Anreize schafft. Eine starre Regulierung sorgt nicht unbedingt für besonders sichere Datentreuhänder, sondern möglicherweise dafür, dass sie gar nicht erst entstehen. Deshalb ist es nötig, bei der Ausgestaltung der Regulierung die je nach Anwendungsfall unterschiedlichen Funktionen von und Herausforderungen für verschiedene Formen von Datentreuhändern zu berücksichtigen.

Zu diesem Zweck entwickeln wir in diesem Papier einen Ansatz, der das Risiko, das von verschiedenen Formen von Datentreuhändern ausgeht, sektorübergreifend

1 Datenethikkommission (2019), „Gutachten der Datenethikkommission"; Bundesregierung (2021), „Datenstrategie der Bundesregierung", Abschnitt 2.3, Januar; Rat für Informationsinfrastrukturen (2021), „Workshop-Bericht der AG Datentreuhänderschaft – Datentreuhänder: Potenziale, Erwartungen, Umsetzung"

2 PIMS sind Dienste, mit denen personenbezogene Daten verwaltet und über die Zugang gewährt werden kann, siehe Abschnitt 4.2. und zum Beispiel Schwartmann, Hanloser, Weiß (2021), „PIMS im TTDSG – Vorschlag zur Regelung von Diensten zur Einwilligungsverwaltung im Telekommunikation-Telemedien-Datenschutzgesetz", März

3 Siehe u.a. Bundesdruckerei, iRights (2019), „Zukunft Gesundheitsdaten", abrufbar unter: https://www.bundesdruckerei.de/system/files/dokumente/pdf/Studie_Zukunft-Gesundheitsdaten.pdf.

4 Siehe u.a. Bundesregierung (2021), op. cit.

5 Siehe u.a. Kerber (2018), „Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data", JIPITEC 9 (3), S. 310-331 und Gesamtverband der deutschen Versicherungswirtschaft (2018), „Datenkranz beim automatisierten Fahren gemäß § 63a StVG – externe Speicherung bei einem Datentreuhänder", Positionspapier, August

systematisiert. In vier Anwendungsfällen konkretisieren wir Regulierungsansätze, die einerseits Risiken eindämmen und andererseits Innovation ermöglichen sowie bestehende Eintrittshürden senken. Um solche Modelle und entsprechende Regulierung einzugrenzen, formulieren wir in Abschnitt 2 Mindestanforderungen an eine Datentreuhand, die als Definition dient. In Abschnitt 3 zeigen wir auf, inwiefern aktuellen Regulierungsvorhaben den Spielraum von Datentreuhandmodellen zu sehr einschränken, und welche Faktoren die Regulierungsstrenge bestimmen sollten. In Abschnitt 4 untersuchen wir den möglichen Einsatzbereich und Regulierungsbedarf von vier Anwendungsfällen von Datentreuhändern, nämlich für medizinische Daten, PIMS, Produktpässe und Agrardaten. Abschnitt 5 fasst die Ergebnisse zusammen.

2. Definition

Bisher gibt es keine allgemein akzeptierte Definition davon, was genau eine Datentreuhand ausmacht und was sie erfüllen muss, um als Datentreuhand zu gelten. Aktuell wird der Begriff Datentreuhand für ein breites Spektrum an Ansätzen verwendet. Diese breite Verwendung erschließt sich insbesondere dann als sinnvoll, wenn das Ziel ist, neue beziehungsweise alternative Modelle zu erschaffen. Daher entwickeln wir Im Folgenden eine diese Verwendungen erfassende Grunddefinition für Datentreuhänder.[6]

Die Ziele von Datentreuhändern sind ein sinnvoller Ausgangspunkt für eine Bestimmung dessen, was Datentreuhänder ausmacht. Ein interdisziplinärer Austausch hat folgende Ziele von Datentreuhändern identifiziert, die miteinander kombiniert werden können, doch nicht müssen:[7]

- *„Stärkung, Gewährleistung oder Wiederherstellung individueller oder kollektiver Kontrolle über Daten durch Stärkung der Position von Datensubjekten, Verbraucher:innen, beziehungsweise Betroffenen im Sinne des Datenschutzrechts (z.B. durch Verringerung von Informationsasymmetrien/ Verhandlungsungleichgewichten)*
- *Förderung der Teilhabe der Datensubjekte (wie Verbraucher:innen) an der wirtschaftlichen Verwertung von Daten*
- *Förderung des Datenaustauschs und der weitreichenden oder gezielten Verfügbarmachung von Daten zur Förderung von Innovation und Wettbewerb durch eine weiterreichende Datennutzung*
- *Möglichkeit zur proaktiven Definition der Bedingungen des Datenteilens*
- *Erfüllung von Datenschutzbestimmungen, z.B. durch Pseudonymisierung oder Verschlüsselung von personenbezogenen Daten*
- *Aufbereitung und Bereitstellung hochqualitativer, pseudonymisierter Daten für Wissenschaft und Forschung*
- *Datenverwaltung mit Unparteilichkeit, Transparenz und ungeteilter Loyalität*
- *Ausschluss von unbefugtem Datenzugriff*
- *Einschränkung der marktbeherrschenden Stellung großer Plattformbetreiber*
- *Förderung vertrauenswürdiger europäischer Plattformangebote*
- *Stellung als Vertrauensanker beziehungsweise Intermediär zwischen Datengeber:innen und Datennutzer:innen“*

6 Diese Definition ist breiter als die „optimale“ Version einer Datentreuhand für Verbraucher:innendaten als kollektive Verhandlungsinstanz entwickelt in Blankertz (2020), „Designing Data Trusts“

7 Blankertz, von Braunmühl, Kuzev, Richter, Richter, Schallbruch (2020), „Datentreuhandmodelle“, abrufbar unter: https://www.ip.mpg.de/de/publikationen/details/datentreuhandmodelle-themenpapier.html

Aus diesen Zielen lassen sich folgende drei Grundmerkmale einer Datentreuhand ableiten:

- **(auch) Datenintermediär:** Eine Datentreuhand übernimmt eine Funktion der Datenverwaltung, -durchleitung und/oder -aufbereitung zum Nutzen einer anderen Partei (oder mehrerer).
- **Erfüllung rechtlicher Anforderungen:** Eine Datentreuhand ist mindestens an den bestehenden Rechtsrahmen gebunden. Das heißt, ihre Aktivitäten erfüllen sowohl allgemeine rechtliche Anforderungen (zum Beispiel Datenschutz, Kartellrecht) als auch spezifisch ausgestaltete Vereinbarungen zwischen beteiligten Parteien in Form eines Vertrags.
- **anwendungsabhängige Vertrauensanforderungen:** Je nach Einsatzbereich einer Datentreuhand können unterschiedliche Mechanismen sinnvoll und geboten sein, um Vertrauen und eine wünschenswerte Verteilung des aus Daten gewonnenen Wertes zu erzielen. Aufgrund der Vielfalt möglicher Ziele sind diese Anforderungen nicht allgemein, sondern in Abhängigkeit von Anwendungsfällen zu bestimmen.

Im weiteren Verlauf dieses Papiers widmen wir uns insbesondere dem dritten Punkt: Spezielle Anforderungen, möglicherweise in Regulierung verankert, die an Datentreuhänder zu stellen sind, sollten sich nicht an einem allgemeinen Idealbild möglicher Datenintermediäre orientieren. Anforderungen sollten so gewählt sein, dass sie möglichst konkrete Ziele erreichen und konkrete Risiken ausschließen.[8]

8 Aus rechtlicher Perspektive hat die Datentreuhand wenig mit dem zu tun, was zivilrechtlich unter dem Treuhandbegriff verstanden wird. Da an Daten bestehen im Regelfall keine absoluten Rechte bestehen (siehe Specht, Kerber (2017), „Datenrechte – eine rechts- und sozialwissenschaftliche Analyse im Vergleich Deutschland – USA“, Abida-Gutachten, abrufbar unter: https://www.abida.de/sites/default/files/ABIDA_Gutachten_Datenrechte.pdf), können diese nicht umfänglich übertragen werden. Anders verstanden als unechte Vollmachtstreuhand ist kein absolutes Recht an Daten erforderlich, um einen Datentreuhänder zum Beispiel zu bevollmächtigen, für den Datentreugeber (wie Verbraucher:innen oder Unternehmen) eine Zugangsentscheidung zu treffen. Werden mit der jüngeren Literatur sämtliche Rechtsverhältnisse, die im Innenverhältnis die Interessenwahrnehmung einer Vertragspartei gegenüber der anderen zum Gegenstand haben, als Treuhand erfasst, lässt sich auch die Datentreuhand unter diesen Begriff der Treuhand im weiteren Sinne fassen. Dieses weite Treuhandverständnis wiederum ist nicht notwendigerweise identisch mit dem Treuhandverständnis anderer Rechtsordnungen, zum Beispiel dem englischen Trust. Zu den Gemeinsamkeiten und Unterschieden der Treuhand und des Trusts vgl. Graf von Bernstorff (2011), „Einführung in das englische Recht“, 4. Aufl., S. 144 f.

3. Sektorübergreifende Regulierung

Verschiedene Vorhaben stehen im Raum, um Datendienste allgemein und Datentreuhänder im Speziellen stärker zu regulieren. Zunächst fassen wir bestehende Regulierungsbestrebungen zusammen und bewerten sie (Abschnitt 3.1.). Die Vorhaben sind primär darauf ausgerichtet, zusätzliche Anforderungen an Datendienste zu stellen. Dann entwickeln wir einen Vorschlag für eine risikobasierte Regulierung (Abschnitt 3.B). Darin spielen die (De-)Zentralität der Datenhaltung und die Freiwilligkeit der Nutzung von Datentreuhandmodellen eine wichtige Rolle dafür, wie streng Regulierung auszugestalten ist. Zugleich beleuchten wir kritisch, inwiefern ein neutrales Geschäftsmodell vorgeschrieben werden sollte.

3.1. Schwachstellen aktueller Regulierungsvorhaben

Inhalt der Vorhaben

Verschiedene Vorhaben streben eine Regulierung von Datentreuhändern an. Neben dem DGA als dem umfassendsten gibt es verschiedene weitere Bestrebungen, Vorgaben für Datenintermediäre festzuschreiben.

Die **Datenethikkommission** fordert, dass die Bundesregierung Qualitätsstandards sowie ein Zertifizierungs- und Überwachungssystem für Datentreuhänder und insbesondere PIMS erarbeiten solle.[9] Als mögliche Akteure nennt sie gemeinwohlorientierte Stiftungen oder Unternehmen, „wenn dabei der Betreiber an der Verwaltung, und nicht an der Nutzung der Daten verdient."[10] Wie in Abschnitt 3.2. ausgeführt, ist diese Unterscheidung in der Praxis weniger klar, als sie zunächst erscheint.

Der **Verbraucherzentrale Bundesverband** (vzbv) fordert ebenfalls, dass PIMS rechtlich gesichert „unabhängig, neutral und ohne ein wirtschaftliches Eigeninteresse an der Verwertung der im Auftrag der Verbraucher verwalteten Daten agieren".[11] Darüber hinaus solle es ein hohes Maß an Transparenz und angemessene Geschäftsbedingungen geben. vzbv bevorzugt eine Organisationsform wie Stiftungen und sieht eine mögliche Vergütung von Nutzenden kritisch.[12]

Das Wahlprogramm der **SPD** verspricht die Einrichtung öffentlicher Datentreuhänder neben einer „vertrauenswürdige[n] Daten-Teilen-Infrastruktur" und einer Pflicht

9 Datenethikkommission (2020), op. cit.
10 Ebd., S. 134
11 vzbv (2020), „Personal Information Management Systems (PIMS): Chancen, Risiken und Anforderungen", Februar, S. 11
12 Ebd.

für große Konzerne, „ihre Daten für gemeinwohlorientierte Ziele teilen“ zu müssen.[13] Dabei erfolgt keine genauere Spezifizierung dessen, wozu öffentliche Datentreuhänder dienen sollen. Die anderen politischen Parteien haben noch keine Programme veröffentlicht oder schweigen zur Regulierung von Datentreuhändern.

Im **TTDSG** (Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien) wird insbesondere für Einwilligungsdienste festgelegt, dass diese kein Interesse an Einwilligung haben oder mit einem daran interessierten Unternehmen verbunden sein dürfen.[14] Darüber schreibt das TTDSG keine konkrete Organisationsform vor, doch führt als Beispiel „etwa von Unternehmen als unabhängige Stiftung organisierte Einrichtungen [an], die sogenannte Single-Sign-On-Lösungen für die in der Stiftung zusammengeschlossenen Unternehmen anbieten, über die Nutzer ihre Einwilligung organisieren können.“[15] Solche Organisationen existieren im Moment nicht[16] und es ist nicht klar, welchen Anreiz es gibt, sie zu erschaffen.

Auch der DGA, der Ende 2020 im Entwurf vorgestellt wurde, stellt eine Reihe von Anforderungen an Datentreuhänder:

- **Anmeldung** (Art. 10): Sämtliche sogenannte „Dienste für die gemeinsame Datennutzung“, worunter Datentreuhänder fallen, müssen angemeldet werden und werden von einer Behörde im Hinblick auf die Einhaltung der in Art. 9 – 13 (Kapitel 3) enthaltenen Vorgaben überwacht.
- **Neutralitätspflicht** (Art. 11 Nr. 1-3): Die Bereitstellung, die Vermittlung und die Nutzung von Daten müssen institutionell voneinander getrennt werden. Anbieter von Vermittlungsleistungen dürfen die Daten nur vermitteln, und nicht für eigene Zwecke verwenden. Dies gilt auch für die Metadaten, die nur für die Entwicklung des Dienstes verwendet werden dürfen. Erforderlich ist eine gesonderte Rechtsperson zur Erbringung der Vermittlungsdienste sowie ein Leistungsangebot in einer nichtdiskriminierenden, fairen und transparenten Weise.[17] Mit der Trennung sollen eine (Über-)Nutzung der Daten für eigene Zwecke und Bevorzugung integrierter Dienste verhindert werden. Dies reflektiert möglicherweise die negative

13 SPD (2021): „Das Zukunftsprogramm der SPD“, abrufbar unter: https://www.spd.de/fileadmin/Dokumente/Beschluesse/Programm/SPD-Zukunftsprogramm.pdf, S. 15

14 Deutscher Bundestag (2021), „Beschlussempfehlung und Bericht des Ausschusses für Wirtschaft und Energie zu dem Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien“, Drucksache 19/29839, abrufbar unter: https://dip21.bundestag.de/dip21/btd/19/298/1929839.pdf

15 Ebd., S. 78

16 Eine Ausnahme ist netID Foundation, die von Mediengruppe RTL Deutschland, ProSiebenSat.1 und United Internet gegründet wurde und viele weitere Medien- und andere Unternehmen assoziiert. Es ist unklar, inwiefern sie die Anforderung erfüllt, kein Interesse an einer Einwilligung zu haben, denn die assoziierten Unternehmen verfolgen verschiedene Formen der Datenverarbeitung. Mehr Informationen unter: https://enid.foundation/

17 Kerber (2021), „DGA – einige Bemerkungen aus ökonomischer Sicht“, abrufbar unter: https://www.uni-marburg.de/de/fb02/professuren/vwl/wipol/pdf-dateien/kerber_dga_einige-bemerkungen_21012021.pdf

Erfahrung mit den Datenpraktiken großen Plattformen, zum Beispiel von Amazon gegenüber Marketplace-Anbietern.[18]

- **Bestes Interesse** (Art. 11 Nr. 10): Werden Dienste für die gemeinsame Datennutzung für die betroffene Person angeboten, hat der Dienst im besten Interesse der betroffenen Person zu handeln und ihr die Rechtsausübung zu erleichtern, indem sie sie zu den Zwecken der Datenverarbeitung und den damit verbundenen Bedingungen berät.

Zudem hebt der DGA hervor, dass Dienste für die gemeinsame Datennutzung Prozesse haben sollten, um betrügerisches oder missbräuchliches Verhalten in Bezug auf Datenzugang zu verhindern (Art. 11 Nr. 5), illegalen Zugang oder Übertragung nicht-personenbezogener Daten zu unterbinden (Art. 11 Nr. 7), ein hohes Sicherheitsniveau für nicht-personenbezogene Daten sicherzustellen (Art. 11 Nr. 8) und das Wettbewerbsrecht einzuhalten (Art. 11 Nr. 9). Sofern dies bedeutet, dass die Dienste sich an den etablierten Rechtsrahmen halten müssen, ist dies durch bestehende Gesetze bereits vorgegeben. Falls dies bedeutet, dass die Dienste darüber hinaus auch die Rechtmäßigkeit des Verhaltens ihrer Vertragspartner sicherstellen müssten, ergibt sich daraus eine Reihe neuer Pflichten für Datendienste.

Diese Anforderungen gelten nicht für Einrichtungen ohne Erwerbszweck, deren Tätigkeit ausschließlich darin besteht, für Ziele von allgemeinem Interesse Daten zu sammeln, die von natürlichen oder juristischen Personen auf der Grundlage des Datenaltruismus zur Verfügung gestellt werden.

Bewertung der Vorhaben

Die Regulierungsvorhaben sehen für Datentreuhänder zusätzliche Auflagen und Hürden vor, um ihre Vertrauenswürdigkeit sicherzustellen. Diese Auflagen geben implizit ein „optimales“ Zielbild für Datenmodelle vor, das Risiken möglichst weitgehend ausschließen soll. Dadurch werden andere Modelle ausgeschlossen, die zwar nicht komplett risikolos sein mögen, doch immer noch wünschenswert sein können, da ihr Potenzial ihre Risiken überwiegt.

Die Idealisierung einer völlig neutralen und gemeinnützigen Datentreuhand verkennt, dass durch die Regulierung keine Anreize bestehen oder geschaffen werden dafür, solche Organisationen bereitzustellen. Wenn eine Datentreuhand prinzipiell keine eigenen Interessen verfolgen darf, ist unklar, welches Interesse daran besteht, sie zu erschaffen. Es ist sinnvoll, mögliche Interessenkonflikte einer Datentreuhand zu gering zu halten, doch es gibt dafür weniger einschneidende Maßnahmen als der komplette Ausschluss eigener Interessen (diese entwickeln wir anwendungsspezifisch in Abschnitt 4).

18 Siehe Europäische Kommission (2020d), Case AT.40462 Amazon Marketplace

Außerdem kollidieren die in den aktuellen Vorhaben geforderten Anforderungen oft mit der Realität bestehender „neuer“ Modelle: Die Anforderung einer Neutralität, wie zum Beispiel im DGA beschrieben, verhindert Modelle, bei denen die Öffnung von selbst genutzten Daten für Externe erfolgt und eine Weiterentwicklung in eine Plattform für Datenflüsse auch dritter Parteien stattfindet. Eine Verknüpfung von Datendiensten mit Produktionsaktivitäten im gleichen Unternehmen ist eine Form von vertikaler Integration.

Solche vertikale Integration durch Öffnung bestehender Plattformen für die Verarbeitung und/oder Weitergabe externer Daten gibt es in verschiedenen Fällen. Eine solche Entwicklung fand zum Beispiel bei Tony's Chocolonely statt, einem niederländischen Schokoladenhersteller, der seine Plattform Open Chain zum Nachvollzug von fair hergestelltem Kakao für andere Schokoladenhersteller geöffnet hat.[19] Auch beim Zusammenschluss der Carsharing-Plattformen von DriveNow und Car2Go entstand eine (aus wettbewerblichen Gründen angeordnete) offene Plattform für Mobilitätsdienste, die trotz vertikaler Integration für andere Anbieter nutzbar ist.[20] Auch Internet of Things-Plattformen gehören oft zunächst einem Hersteller (zum Beispiel MindSphere zu Siemens,[21] Home Connect Plus zu Bosch[22]), bevor sie für andere Anbieter geöffnet werden.

Gerade im Kontext personenbezogener Daten gibt das Datenschutzrecht umfassend vor, für welche Zwecke und nach welchen (strengen) Maßgaben Daten verarbeitet werden dürfen. Weshalb Datentreuhändern zusätzliche und strengere Anforderungen auferlegt werden sollten, ist jedenfalls dann nicht unmittelbar nachvollziehbar, wenn man Anreize für die Entwicklung bestimmter Datentreuhandmodelle setzen möchte. Jede zusätzliche regulatorische Anforderung macht die Datentreuhandmodelle weniger umsetzbar und weniger wettbewerbsfähig im Vergleich zu unmittelbaren Datenaustauschmodellen, mit denen sie am Markt konkurrieren. Es besteht die Gefahr, dass der Markt für Vermittlungsdienstleistungen durch eine Überregulierung zurückgeht oder sogar gänzlich verschwindet.[23] Zusammenfassend riskieren die aktuellen Regulierungsvorhaben, mit einer zu engen Vorstellung wünschenswerter Datendienste die Entwicklung von Datentreuhändern zu erschweren, weil sie neben bestehenden gesetzlichen Vorgaben nicht unerhebliche weitere Anforderungen erfüllen sollen. Damit verhindern die Vorhaben Missbrauch zwar effektiv, doch als unerwünschten Nebeneffekt auch mögliche sinnvolle Formen des Datenaustauschs.

19 siehe „Tony's Open Chain“, abrufbar unter: https://www.tonysopenchain.com/
20 Europäische Kommission (2018), Case M.8744 -DAIMLER / BMW / CAR SHARING JV, 7. November
21 https://siemens.mindsphere.io
22 https://www.home-connect-plus.com/de/app/
23 Kerber (2021), op. cit.

3.2. Vorzüge eines risikobasierten Ansatzes

Wie streng reguliert wird, sollte auf die Risiken abgestimmt werden, die mit einer Datentreuhand einhergehen: Je mehr Risiko einer Datentreuhand innewohnt, umso strengeren Regeln sollte sie unterworfen sein. Demselben Ansatz folgt auch der Vorschlag einer KI-Verordnung der Europäischen Kommission.[24] Dabei sollte eine regulatorische Intervention immer auf einen Regulierungsbedarf zurückgeführt werden, der sich zum Beispiel aus Schutzpflichten des Staates ergeben kann. Wo ein hohes Risiko für die betroffenen Rechte und Interessen der beteiligten Personen besteht, ist prinzipiell ein höherer Regulierungsbedarf gegeben als dort, wo die Risiken von vornherein gering sind.[25]

Die Risiken einer Datentreuhand hängen vor allem mit den Rechten und Interessen der möglichen Beteiligten zusammen und sind insbesondere folgende:

- das informationelle Selbstbestimmungsrecht,
- der Geschäftsgeheimnisschutz,
- der Schutz von geistigem Eigentum und Urheberrechten,
- die Berufsfreiheit, die Forschungsfreiheit und
- die ebenfalls grundrechtlich verbürgte Privatautonomie.

	Freiwillige Nutzung	**Verpflichtende Nutzung**
Dezentrale Datenhaltung	Freiwillig & dezentral z.B. manche PIMS	Verpflichtend & dezentral z.B. Gateway (AUS)
Zentrale Datenhaltung	Freiwillig & zentral z.B. manche PIMS	Verpflichtend & zentral evtl. Auto-Daten

Abbildung 1: Risikobasierte Unterscheidung von Datentreuhandmodellen

Quelle: Stiftung Neue Verantwortung auf Grundlage von Specht-Riemenschneider et al. (2021)

Diese Rechte und Interessen sind abseits von der konkreten Funktionsgestaltung der Datentreuhand insbesondere durch zwei übergeordnete Parameter beeinflusst: Erstens, die Frage, ob die Datentreuhand obligatorisch verwendet wird und Betroffene daher zum Beispiel zwingt, Datenbestände durch eine Datentreuhand verwalten zu lassen. Zweitens, ob die Daten zentral oder dezentral gespeichert werden, also

24 Europäische Kommission (2021), „Proposal for a Regulation laying down harmonised rules on artificial intelligence", abrufbar unter: https://ec.europa.eu/newsroom/dae/redirection/document/75788

25 Specht-Riemenschneider, Blankertz, Sierek, Schneider, Henne (2021), „Datentreuhand: Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierungserfordernisse für Datentreuhandmodelle", Beilage in MMR, Juni

zum Beispiel in einer zentralen Datenbank oder bei den einzelnen Beteiligten. Diese Parameter erlauben eine Unterscheidung der vier Modelle in Abbildung 1.

Es gibt Beispiele für alle Modelle. PIMS (siehe Abschnitt 4.2.) verfolgen sowohl zentrale als auch dezentrale Ansätze und bisher sind sie für alle Seiten freiwillig in ihrer Nutzung. Das Gateway für den australischen Energiesektor ist eine Datenzugangsstelle, die Unternehmen nutzen müssen, um zu den weiter dezentral vorliegenden Daten Zugang zu gewähren (siehe weiter unten in diesem Abschnitt). Bei den Auto-Daten ist es möglich, dass sich ein zentraler und verpflichtender Ansatz durchsetzt.[26]

Darüber hinaus ist die Verarbeitung personenbezogener Daten durch die Datentreuhand ein wichtiger Risikofaktor. Dieser wird durch das Datenschutzrecht umfassend regulatorisch erfasst, insb. die Datenschutzgrundverordnung (DSGVO), das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze sowie Spezialregelungen wie beispielsweise im Zehnten Sozialgesetzbuch. Daher wird erst in der Diskussion spezifischer Anwendungsfälle (siehe Abschnitt 4) zwischen solchen mit und ohne Personenbezug unterschieden.

Risikofaktor: zentrale Speicherung der Daten bei Datentreuhand oder dezentrale Speicherung bei Datenverarbeiter/Betroffenen

Ein wesentliches Unterscheidungsmerkmal von Datentreuhandmodellen ist, wo das Datentreugut gespeichert ist. Die Daten können zentral beim Datentreuhänder oder dezentral beim Datenverarbeiter oder beim Betroffenen liegen.[27] Wie in Tabelle 1 dargestellt, ist eine zentrale Datenhaltung mit höheren Risiken verbunden. Dabei ermöglicht sie allerdings zusätzliche Formen der Datennutzung und stellt zugleich höhere Anforderungen an die zugrundeliegende Infrastruktur.

26 Siehe Gesamtverband der deutschen Versicherungswirtschaft (2018), op. cit.

27 Vgl. mit ähnlicher Überlegung zum Data Trustee Wendehorst, Schwamberger, Grinzinger (2020), „Datentreuhand –wie hilfreich sind sachenrechtliche Konzepte?“, in Pertot (Hrsg), Rechte an Daten, [S. 103–121] S. 107; Specht-Riemenschneider et al. (2021)

Tabelle 1: Merkmale von zentralen und dezentralen Datentreuhandmodellen

	Zentral	Dezentral
Möglichkeiten		
Mögliche Befugnisse für DTH	Umfassend, von Zugangsmanagement bis Analyse im Auftrag Dritter	Begrenzt auf Zugangsmanagement
Mögliche Datennutzung	Umfassend, inkl. explorativer Datenanalyse	Begrenzt auf zum Beispiel Algorithmentraining
Infrastrukturerfordernisse	Potenziell niedriger (zum Beispiel wenn keine Echtzeit-datenübertragung nötig)	Volle Integration über DTH nötig
Risiken		
Kontrolle bei Datengebenden	Niedriger	Potenziell höher, je nach Implementation
Datenschutzrisiko	Höher	Niedriger
Missbrauchsrisiko durch DTH	Höher	Niedriger
Sicherheitsrisiko	Höher	Niedriger

Quelle: Stiftung Neue Verantwortung

Die zentrale Speicherung beim Datentreuhänder verspricht eine einfachere Verwaltung der Daten durch den Datentreuhänder. Weitergehende Befugnisse sind möglich, wie zum Beispiel auch, den Datenverarbeiter vom Zugang auszuschließen (siehe Microsoft Cloud[28]). Die Datentreuhand kann im Falle einer zentralen Speicherung die Daten umfassend nutzen (zum Beispiel analysieren) oder verändern (zum Beispiel löschen). Derzeit entscheidet das Datenschutzrecht darüber, inwieweit dies zulässig ist. Wenn eine Datentreuhand Daten anonymisiert oder pseudonymisiert, können Daten dezentral gehalten und eine Datentreuhand kann zentral Zugang zu den entsprechend anonymisierten oder pseudonymisierten Daten an (vertraglich definierte) Dritte gewähren.

Bei einer zentralen Datenspeicherung durch eine Datentreuhand sind die Risiken tendenziell höher. Die Kontrolle über die Daten ist zumindest teilweise bei der Da-

28 Dies war das Konzept einer Kollaboration zwischen Microsoft und Deutsche Telekom, bei der Deutsche Telekom als Datentreuhand für Microsoft-Clouddienste fungieren sollte. Das Projekt wurde allerdings 2019 eingestellt, siehe Nitschke (2018), „Microsoft stellt seine Cloud-Dienste ab 2019 aus neuen Rechenzentren in Deutschland bereit und reagiert damit auf veränderte Kundenanforderungen“, abrufbar unter: https://news.microsoft.com/de-de/microsoft-cloud-2019-rechenzentren-deutschland/

tentreuhand, was mehr Absicherung gegenüber den Datengebenden erforderlich macht. Auch der Datenschutz ist, sofern personenbezogene Daten vorliegen, schwieriger zu gewährleisten, wenn Daten explizit und unverschlüsselt mit einer Datentreuhand geteilt werden. Außerdem kann die Datentreuhand über die Zusammenführung großer Datenmengen eine „Datenmacht" erlangen, die das Risiko des Missbrauchs birgt (z. B. dass so erlangte Erkenntnisse nicht zum Vorteil der Datengebenden verwandt werden). Auch das Sicherheitsrisiko ist bei zentralen vorgehaltenen Daten größer, denn bei Angriffen gegen den Intermediär ist der potenzielle Schaden höher.

Beispiele von Datenintermediären, die verschiedene Formen von (de-)zentraler Datenhaltung nutzen, werden im Weiteren dargestellt. Gelegentlich werden dabei auch zentrale mit dezentralen Elementen kombiniert.

Das Forschungsdaten- und Servicezentrum (FDSZ) der Bundesbank verwaltet den Zugang zu umfassenden Datenbeständen, die auch sensible Mikrodaten beinhalten. Die Daten liegen zentral bei der Bundesbank vor und können teilweise abgefragt werden. Wenn Forscher:innen oder Analytiker:innen Zugang zu granularen und datenschutzrechtlich relevanten Daten benötigen, können sie diese nach Prüfung vor Ort erhalten, hierbei „[trägt d]as FDSZ Sorge dafür, dass nur anonymisierte Ergebnisse das sichere Umfeld des Gastforscherarbeitsplatzes im FDSZ verlassen."[29] Die Sicherheit und der Datenschutz werden somit über eine starke Zugangsbeschränkung sichergestellt.

In Australien entwickelt die australische Verbraucher- und Wettbewerbsbehörde (ACCC) das Verbraucherdatenrecht (Consumer Data Right) zunächst im Energiesektor. Während Verbraucher:innen besseren Zugriff auf Daten und einfachere Wechselmöglichkeiten zwischen Anbietern erhalten sollen, lehnte die ACCC Bestrebungen in Australien für eine zentrale Speicherung von Datensätzen im Energiesektor ab.[30] Stattdessen greift man auf ein Modell dezentraler Speicherung in Kombination mit einer koordinierenden Datendurch- und -weiterleitungsstelle, das Gateway, zurück.[31] Abbildung 2 zeigt, wie das Gateway eine koordinierende Funktion einnimmt, ohne Daten zusammenzuführen.

29 Deutsche Bundesbank, „Forschungsdaten- und Servicezentrum (FDSZ)", abrufbar unter: https://www.bundesbank.de/de/bundesbank/forschung/fdsz/forschungsdaten-und-servicezentrum-fdsz--604430

30 Vor- und Nachteile von Ausgestaltungsoptionen eines Datenzugangs im australischen Energiesektor wurden im Rahmen einer öffentlichen Konsultation gesammelt und durch die ACCC in folgendem Dokument tabellarisch zusammengefasst, siehe ACCC (2019), „Consumer Data Right in Energy – Position Paper: data access model for energy data", abrufbar unter: https://www.accc.gov.au/system/files/ACCC%20-%20CDR%20-%20energy%20-%20data%20access%20models%20position%20paper%20-%20August%202019.pdf

31 Für eine Diskussion des Gateway im Energiesektor siehe ACCC (2020), „Energy Rules Framework – Consultation Paper", S.36 f., abrufbar unter: https://www.accc.gov.au/system/files/CDR%20-%20Energy%20rules%20framework%20consultation%20paper%20-%20July%202020_0.pdf

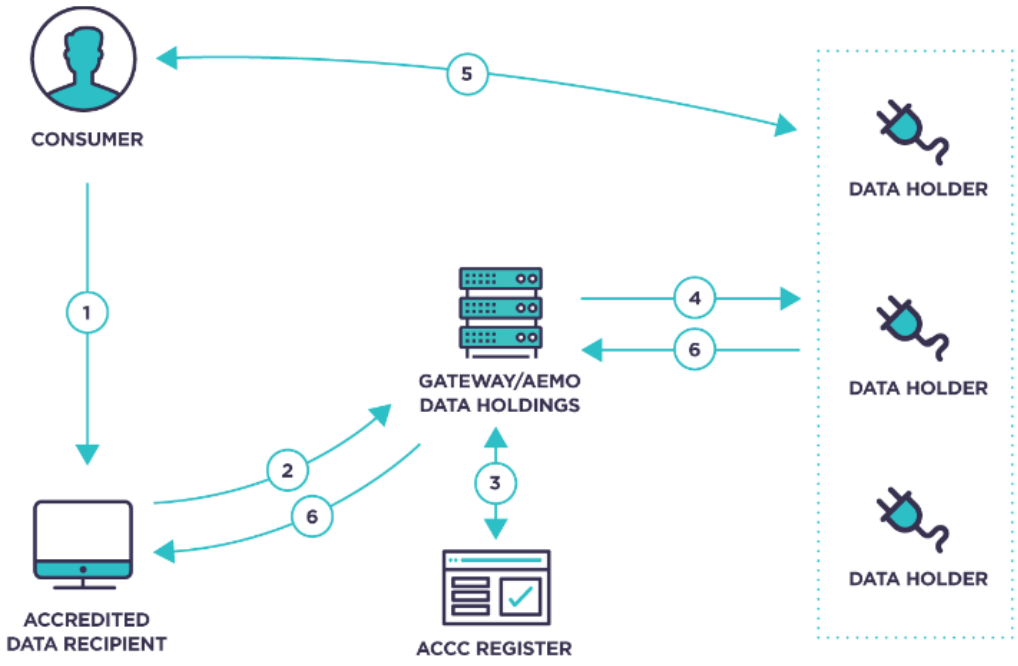

Abbildung 2: Übersicht der Datenflüsse über das Gateway im australischen Energiesektor

Quelle: ACCC (2019), „Consumer Data Right in Energy – Position Paper: data access model for energy data", S. 14a

1. The consumer consents to an ADR obtaining their data.
2. The ADR contacts the gateway, seeking to access the consumer's data.
3. The gateway authenticates the ADR using data previously obtained from the ACCC's Register.
4. The gateway identifies which data holder(s) hold the consumer's data and provides transaction details to them.
5. The process of authentication and authorisation occurs in accordance with any requirements in the CDR energy rules. The gateway's role in this process is to be determined.
6. The consumer's data is shared with the ADR via the gateway.

Kommerzielle Dienste in Europa und anderswo erproben die verschiedene Modelle zur vertrauenswürdigen Nutzbarmachung von Daten. Hierzu gehören die Kollaborationsplattform apheris und der PIMS-ähnliche Dienst polypoly. Bei apheris[32] werden zum Beispiel pharmazeutische Daten von verschiedenen Beteiligten in verschlüsselter Form bereitgestellt, um auf ihnen dezentral Analysen durchzuführen. Die Rolle von apheris besteht in der Bereitstellung der technischen Plattform und anwendungsspezifischer Verschlüsselung. Bei polypoly[33] befindet sich eine solche Infrastruktur noch im Aufbau, die Verbraucher:innen ermöglichen soll, Daten umfassend auf Endgeräten zu speichern und zu verwalten. Auch hier ist die Absicht, dass Algorithmen dezentral, d.h. über Federated Learning, lernen.

32 https://www.apheris.com
33 https://polypoly.org/en-gb/

Risikofaktor: freiwillige oder verpflichtende Nutzung der Datentreuhand

Ein weiteres Unterscheidungsmerkmal von Datentreuhandmodellen ist, ob sie freiwillig oder verpflichtend in ihrer Nutzung sind. Als Ausgangspunkt wird allgemein angenommen, dass Beteiligte frei sind in ihrer Entscheidung, ob sie eine Datentreuhand nutzen wollen, sofern nicht besondere Gründe vorliegen, die eine Verpflichtung begründen. Bei freiwilliger Nutzung lässt sich die Datentreuhand über einen Datentreuhandvertrag regeln, der die rechtliche Grundlage des Datenaustauschs darstellt.[34] Je nach Sektor und Anwendung kann es geboten sein, der Vertragsgestaltung bestimmte Grenzen zu setzen.

Eine Pflicht zur Nutzung einer Datentreuhand kann dadurch begründet werden, dass das Ziel durch freiwillige Maßnahmen nicht zu erreichen ist. Zudem muss das Ziel eine regulatorische Intervention rechtfertigen. Dazu können verschiedene Faktoren beitragen, darunter:

- ausgeprägtes öffentliches Interesse an dem mit der Datentreuhand verfolgten Ziel, beispielsweise aufgrund von Nähe zur staatlichen Daseinsfürsorge (wie in den Bereichen Gesundheit, Bildung oder Mobilität),
- hohe Konzentration auf einem der an der Datentreuhand beteiligten Märkte beziehungsweise ein deutliches Ungleichgewicht zwischen den Beteiligten, sodass Verhandlungsmacht überwiegend bei einer Partei liegt.

Die Verpflichtung zur Nutzung einer Datentreuhand kann auf unterschiedliche Weise erfolgen: Es kann alle Beteiligten eine Pflicht auferlegt werden, bestimmte Daten in eine Datentreuhand zu geben oder von einer Datentreuhand zu empfangen. Allerdings ist dies meist nur für die Seite(n) sinnvoll, die sich sonst wahrscheinlich der Nutzung entziehen würde. Dies kann je nach Konstellation die datengebende Seite sein (zum Beispiel Autohersteller im Automobilkontext) oder auch die datennutzende Seite (zum Beispiel digitale Plattformen).

Bei einer verpflichtenden Datentreuhand ergibt sich ein höheres Risiko, weil die Datentreuhand nicht umgangen werden kann und recht stark in die Beziehung zwischen den Beteiligten eingegriffen wird. Dadurch kann eine problematische Ausgestaltung größeren Schaden anrichten als bei einem freiwilligen Modell. Somit ergibt sich eine Sorgfaltspflicht für eine angemessene Wahl der weiteren Merkmale der Datentreuhand wie, welche Voraussetzungen und Bedingungen des Datenzugangs und IT-Sicherheitsstandards der Gesetzgeber festlegen will oder dem Markt überlässt. Wird die Datentreuhand zum Beispiel nicht als vertrauenswürdig wahrgenommen oder werden überhöhte Sicherheitsstandards festgesetzt, die ihre Nutzung erschweren,

34 Specht-Riemenschneider et al. (2021), op. cit.

kann dies sogar zu weniger Datenaustausch führen als ohne Datentreuhand erreicht würde. Zu niedrige Standards wiederum können Missbrauch durch eine verhandlungsstarke Seite und Sicherheitsrisiken mit sich bringen.

Eine Pflicht zur Nutzung einer Datentreuhand zieht weitere Fragen nach sich wie zum Beispiel, ob gesetzliche Anforderungen für die Voraussetzungen der Zugangsgewährung bestimmt werden und ob eine Vergütung für die Zugangsgewährung anfällt.[35] Diese im Detail zu untersuchen übersteigt den Rahmen dieses Papiers.

Nur gezielt einschränken: das Geschäftsmodell

Ein oftmals hervorgehobener Gestaltungsaspekt von Datentreuhändern ist das Geschäftsmodell. Jedoch ist dieses nicht allgemein ein wesentlicher Risikofaktor und sollte nicht vorschnell regulatorisch eingeschränkt werden. Forderungen nach einem „neutralen“ Geschäftsmodell, wie in vielen der in Abschnitt 3.1. diskutierten Vorhaben artikuliert, sind oft unspezifisch. Wird Neutralität verstanden als ein Ausschluss eines Gewinnmotivs und einer vertikalen Integration, bleibt kein Spielraum für Ansätze, die stärker zur Datenauswertung beitragen und/oder sich aus den Daten bestehender Geschäftsbereiche erschließen lassen. Stattdessen ist es zielführender, anwendungsabhängig zu bestimmen, welche Form der Neutralität nötig ist.

Monetarisierung
Vielerorts äußert sich eine Vorliebe für Datentreuhänder, die ohne Monetarisierung auskommen, da damit Interessenskonflikte ausgeschlossen würden. Dies wird deutlich durch das Konzept von „datenaltruistischen“ Organisationen im DGA,[36] die anders als andere Datendienste nicht der allgemeinen Aufsicht für Datendienste unterstehen sollen. Das Wahlprogramm der SPD sieht staatliche Datentreuhänder vor und auch der vzbv befürwortet gemeinnützige Stiftungen und staatliche Förderung (siehe Abschnitt 3.1.).

Jedoch sind die Vermittlung, Verwaltung und gegebenenfalls Aufbereitung von Daten mit Aufwand verbunden, der wiederum mit Kosten einhergeht. Diese können auf verschiedene Weisen gedeckt werden: Es besteht die Möglichkeit staatlicher Finanzierung oder mindestens Subventionierung, wodurch eine Umlegung auf steuerzahlende Personen und Organisationen erfolgt. Alternativ können private Organisationen Dienste gegen einen Preis anbieten, und mit den Umsätzen einen Gewinn

35 Der Vorschlag für den Digital Markets Act (DMA) beinhaltet eine FRAND(fair, reasonable and non-discriminatory)-Vergütung für u.a. Klickdaten von Suchmaschinen, siehe Europäische Kommission (2020e), „Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)“, Artikel 6j.
36 Europäische Kommission (2020b), op. cit. Rn. 36

(oder Verlust) erzielen oder auch eine Gewinnerzielung ausschließen (zum Beispiel über die Organisationsform einer gemeinnützigen GmbH oder eines gemeinnützigen Vereins).

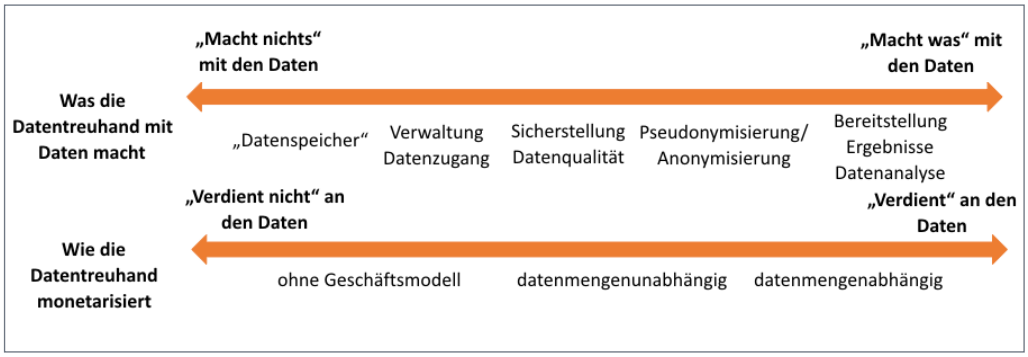

Abbildung 3:
Spektrum der Aktivitäten und Monetarisierung von Datentreuhandmodellen

Quelle:
Stiftung Neue Verantwortung

Es ist fragwürdig, ob ein Ausschluss des Gewinnmotivs notwendig oder hinreichend ist, um die Vertrauenswürdigkeit der Datentreuhand sicherzustellen. Implizit scheint die Sorge, dass die Datentreuhand Daten nicht für die vorgesehenen Zwecke, sondern für eigene Interessen nutzen könne. Allerdings ist unklar, was genau damit gemeint ist beziehungsweise inwiefern dies gerade durch ein Gewinnmotiv verursacht wird.

Abbildung 3 zeigt, dass es ein Spektrum an Funktionen beziehungsweise Aktivitäten gibt, die eine Datentreuhand mit Daten ausüben kann, sowie ein Spektrum an Monetarisierungsansätzen. Je weiter links diese liegen, umso eher werden diese üblicherweise als unkritisch gesehen. Allerdings schränken die links angesiedelten Aktivitäten und Geschäftsmodelle tendenziell stärker ein, in welchem Umfang Mehrwert aus Daten generiert werden kann. Es besteht also das Risiko, dass eher solche Modelle befürwortet werden, die sich darauf beschränken, Daten zu speichern, und nur in geringem Umfang zum Gewinn neuer Erkenntnisse beitragen.

Im Kontext der Monetarisierung wird insbesondere eine vom Datenvolumen abhängige Bezahlung als problematisch angesehen, da sie tendenziell den Anreiz schafft, mehr Daten(zugang) an mehr Datennutzende zu „verkaufen“.[37] Gleichzeitig besteht aber auch das Risiko einer Unternutzung, das Unternutzung kann sich ergeben, wenn die Datentreuhand zu passiv ist und das mit ihr verfolgte Ziel nur unvollständig erreicht. Dies kann der Fall sein, wenn gerade der Zugang zu oder Austausch größerer Datenmengen sinnvoll ist, um bspw. die Hürden für neue Anbieter von Trainingsalgorithmen zu senken. Außerdem bedeutet der prinzipielle Ausschluss von Monetarisierung, dass Kosten in möglicherweise unnötigem Umfang auf das Kollektiv umgelegt werden (wenn staatliche Finanzierung genutzt wird).

37 Siehe zum Beispiel vzbv (2020), op. cit.

Vertikale Integration

Auch eine Neutralitätsforderung in Bezug auf eine vertikale Integration oft weder klar noch sinnvoll. Der Data Governance Act fordert eine Abspaltung von Datendiensten von anderen Geschäftsfeldern (siehe Abschnitt 3.1.). Allerdings ist vertikale Integration nicht immer problematisch, das heißt, sie führt nicht immer zu einer Schlechterbehandlung anderer Dienste oder Selbstbevorzugung, und selbst dann, wenn sie es tut, ist Selbstbevorzugung nicht immer problematisch. Wie die Expert Group for the Observatory on the Online Platform Economy feststellte, ist Ungleichbehandlung von Plattformen dann problematisch, wenn Anbieter marktmächtig sind und/oder Nutzende nur einen Dienst verwenden und Wechselkosten hoch sind.[38] In anderen Konstellationen kann ein gewisses Maß an vertikaler Integration nötig sein, um bestimmte Aktivitäten wirtschaftlich sinnvoll beziehungsweise skalierbar zu machen.

Auch bei einer Datentreuhand ist eine Angliederung an andere Aktivitäten nicht immer problematisch. Wie bereits in Abschnitt 3.1. erwähnt, kann sich vertikale Integration von Datendiensten dann ergeben, wenn eine Organisation sich dazu entscheidet, ihre Daten für Dritte nutzbar zu machen, gegebenenfalls in Kombination mit Daten anderer. Ein Verbot vertikaler Integration beziehungsweise ein Gebot vertikaler Entflechtung kann verhindern, dass solche Formen von Datentreuhandmodellen entstehen. Damit wird ein möglicher Missbrauch mit Sicherheit in Fällen unterbunden, in denen sich ein problematisches Ausmaß an Selbstbevorzugung ergeben könnte. Doch insgesamt verringert ein Verbot den Spielraum für mögliche Entwicklungspfade und Geschäftsmodelle von Datentreuhändern.

Spezifische Regeln statt allgemeiner Neutralität

Statt einer allgemeinen Forderung nach Neutralität sind passgenauere Regeln sinnvoll, um den Risiken von bestimmten Datentreuhandanwendungen entgegenzuwirken. So kann Transparenz über Einnahmequellen sinnvoll sein oder eine separate Einwilligung für Monetarisierung von Daten. Diese anwendungsspezifischen Regeln beleuchtet Abschnitt 4 im Detail.

Eine gezielte Einschränkung des Geschäftsmodells kann die Organisationsform einer Datentreuhand prinzipiell offenlassen. Wie bei den Geschäftsmodellen kann auch hier von einem Spektrum von Optionen ausgegangen werden, das gegebenenfalls anwendungsspezifisch einzuschränken sein kann. Es reicht von gemeinnützigen Organisationen über Genossenschaften hin zu anderen juristischen Personen und Personengesellschaften.

38 Siehe Graef, Jeon, Rieder, van Hoboken, Husovec (2021), „Work stream on Differentiated treatment", Final report

4. Anwendungsfälle und anwendungsspezifische Regulierung

Wenn die Regulierung von Datentreuhändern risikobasiert erfolgen soll, ist es wichtig, anwendungsspezifische Risiken zu verstehen und regulatorische Antworten zu entwickeln. Im Weiteren betrachten wir vier Bereiche, in denen verstärktes Datenteilen vielfach als wünschenswert erachtet wird. Datentreuhandmodelle in unterschiedlicher Ausgestaltung können hierbei zum Einsatz kommen. Durch die Betrachtung der spezifischen Herausforderungen und Risiken können konkrete Maßnahmen zu einer regulatorischen oder anderweitigen politischen Intervention formuliert werden.

Die vier möglichen Anwendungsfälle für Datentreuhänder sind medizinische Daten, PIMS, Agrardaten und Daten für Produktpässe. Sie bilden ein Spektrum ab, das sich unterscheidet in Hinsicht darauf, wie relevant der Personenbezug ist, inwiefern Datenteilen und -nutzung schon stattfindet und ob, entsprechend der in Abschnitt 3.1. vorgestellten Risikounterscheidung, Daten zentral oder dezentral vorgehalten werden beziehungsweise verpflichtend oder freiwillig geteilt werden.

Für jeden Anwendungsfall beleuchten wir die Ausgangslage, wie und in welchem Umfang bereits Datenteilen stattfindet. Dem folgt eine Bewertung des Nutzens und der Risiken, die mit einem verstärkten Datenteilen einhergehen. Im letzten Schritt wird abgeleitet, welcher Bedarf an Regulierung oder anderweitiger politischer Intervention nötig ist, um den Nutzen und die Risiken in Einklang zu bringen.

4.1. Medizinische Daten

Status Quo

Medizinische Daten bergen ein enormes Potenzial für die medizinische Forschung, beispielsweise für die Entwicklung neuer Formen von Diagnose und Therapie. Dies zeigt sich unter anderem in den Fortschritten der KI-gestützten Analyse von Bilddaten aus der Radiologie zum Beispiel durch das deutschen Unternehmen Smart Reporting[39] oder Mediaire[40]. Jedoch werden vorhandene Daten bisher wenig genutzt. Eine wesentliche Ursache liegt in der unklaren rechtlichen Auslegung dessen, wel-

39 Smart Reporting wurde 2014 in München gegründet und bietet KI-gestützte Bildanalyse für Radiologiedaten. Das Cloud-basierte Softwaretool wird von „mehr als 10.000 Ärzten in über 90 Ländern“ genutzt. Mehr Informationen unter: https://www.smart-reporting.com/en/company/about

40 Das 2018 in Berlin gegründete Unternehmen Mediaire baut auf KI-Technik zur Bilddatenanalyse von Gehirn und Rückenmark mit dem Ziel Diagnose und Behandlungsqualität zu verbessern, sowie effektivere Arbeitsabläufe in der Radiologie zu ermöglichen. Mehr Informationen unter: https://mediaire.de/

che Formen des Datenaustauschs erlaubt sind, und (bei einer strengen Auslegung) auch in einer Unterbindung von gesellschaftlich wünschenswertem Datenaustausch. Konkret sind datenschutzrechtliche Bedenken und Unklarheiten besonders prominent. Mindestens für bestehende Datenbestände ist eine Nutzung für nicht ausdrücklich in der Einwilligung aufgeführte Zwecke untersagt. Dies verhindert den Einsatz dieser Daten für neue Forschungszwecke, die zum Zeitpunkt der Datenerhebung nicht absehbar waren.

Zugleich gibt es vielfache Bestrebungen, um Gesundheitsdaten besser systematisch nutzbar zu machen. Die Medizininformatik-Initiative soll Daten aus Krankenversorgung und bestehender Forschung besser zugänglich machen. Dabei sollen Daten zum Beispiel aus Kliniken standardisiert werden, um einen produktiven institutionsübergreifenden Austausch überhaupt zu ermöglichen, und der Einwilligungsprozess soll über ein standardisiertes Formular[41] so Patient:innen sinnvolle Wahlmöglichkeiten geben, die den Forschungsspielraum nicht unnötig einschränken. Die Einführung der elektronischen Patientenakte (ePA) soll Datenflüsse zwischen Krankenkassen, behandelnden Ärzt:innen und Forschenden ermöglichen. Seit Januar 2021 können Patient:innen die ePa von ihrer Krankenkasse anfordern und mit ihren Gesundheitsdaten befüllen. Die Freigabe dieser Daten für Forschungszwecke soll ab Juni 2022 folgen. Zur zentralen Aufbereitung der Daten soll das „Forschungsdatenzentrum für Sozialdaten“ weiter ausgebaut werden.

Aktuell fehlt es insbesondere an einer kumulierten Auswertung von Daten aus verschiedenen medizinischen Domänen. Das Krebsregister und das Transplantationsregister stellen erste Ansätze dafür da, Daten zentral zugänglich zu machen und für datengetriebene Forschung zugänglich zu machen. Beim Krebsregister liegt der Fokus auf Krebsforschung, die über das Zentrum für Krebsregisterdaten (ZfKD) in Form einer Scientific Use File angefragt werden können. Dies ist im Bundeskrebsregisterdatengesetz (BKRD) geregelt, das voraussetzt, dass „ein berechtigtes, insbesondere wissenschaftliches Interesse glaubhaft gemacht wird.[42] Das Transplantationsregister ermöglicht seit dem ersten Quartal 2021 Zugang zu Daten für Dritte zu Forschungszwecken auf Antrag.[43]

Nutzen und Risiken

Mehr Austausch und Nutzung von medizinischen Daten für die Forschung können verschiedene Vorteile bringen. Zunächst ermöglichen sie einen gesellschaftlichen Erkenntnisgewinn darüber, welche Krankheiten und Faktoren wie zusammenhän-

41 Medizininformatik-Initiative (2020), „Arbeitsgruppe Consent Mustertext Patienteneinwilligung, abrufbar unter: „https://www.medizininformatik-initiative.de/sites/default/files/2020-04/MII_AG-Consent_Einheitlicher-Mustertext_v1.6d.pdf
42 BKRD Para. 5 Abs. 3
43 https://transplantations-register.de/forschung

gen und welche Behandlungsmöglichkeiten für welche Gruppen besonders gut (oder auch nicht) funktionieren. Dies wiederum ist eine Grundlage für eine verbesserte und stärker personalisierte Behandlung von Patient:innen, die individuelle Risikofaktoren berücksichtigt. Im Kontext der Corona-Pandemie ist belegt, dass viele Menschen die Weitergabe von Daten über sich befürworten, wenn dadurch ein Nutzen für sie selbst und/oder andere entsteht.[44]

Anwendungsbeispiele sind zahlreich, zum Beispiel eine bessere Erkennung seltener Krankheiten durch die Zusammenführung von Datenbeständen, um Muster zu erkennen, die bei der Betrachtung einzelner Fälle nicht ersichtlich sind. Die Analyse von Mustern ist wichtig auch im Kontext von Langzeitfolgen von Covid-19-Erkrankungen, für deren Erforschung erhebliche Ressourcen aufgewandt werden, unter anderem für die Datenbeschaffung.[45] Auch bei weit verbreiteten gesundheitlichen Problemen, die zum Beispiel Wirbelsäulen betreffen, können Daten helfen, sowohl die individuelle Behandlung anhand von Bilddaten genauer und sicherer zu gestalten als auch patient:innenübergreifend Behandlungsergebnisse vorherzusagen und dies für die Auswahl der geeigneten Behandlung zu nutzen.

Risiken von stärkerem Austausch bestehen in darin, dass einzelne Patient:innen und/oder bestimmte Patient:innengruppen (mit gemeinsamen Merkmalen wie zum Beispiel Vorerkrankungen) in Datensätzen identifiziert werden können. Dadurch ist die Privatsphäre negativ beeinträchtigt, was in sich problematisch ist und zu selbstzensierendem Verhalten führen kann, wie zum Beispiel dem Unterbleiben von medizinisch gebotener Suche nach Informationen oder sogar Behandlung.[46] Zudem kann Identifizierung auch zu Diskriminierung führen: Private Kranken- oder Berufsunfähigkeitsversicherungen nehmen dann Personen mit höherem Risiko nur zu schlechteren Bedingungen oder gar nicht auf. Auch Werbung kann auf bestimmte Gesundheitsmerkmale zugeschnitten werden, ohne dass dies im Interesse der Empfänger:innen wäre.[47]

Bei einer unsauberen Verwendung von Daten können große Datenmengen Forschende dazu verleiten, Fehldiagnosen zu stellen oder Fehlbehandlungen zu empfehlen. Dies ist insbesondere dann der Fall, wenn Korrelation von Krankheitsbildern mit einem kausalen Zusammenhang verwechselt wird, oder wenn die Limitationen von Daten (zum Beispiel nicht-repräsentative Stichproben) nicht ausreichend berücksichtigt werden.

44 Dohmen, Schmelz (2021), „Datenschutz in der (Corona-)Krise: Selbstbestimmung und Vertrauen im Fokus – Policy Paper“, abrufbar unter: https://www.progressives-zentrum.org/wp-content/uploads/2021/05/Datenschutz-in-der-Corona-Krise_Policy-Paper-05_Dohmen-Schmelz.pdf

45 National Institutes of Health (2021), „NIH launches new initiative to study ‚Long COVID‘“, 23. Februar, https://www.nih.gov/about-nih/who-we-are/nih-director/statements/nih-launches-new-initiative-study-long-covid

46 Marthews, Tucker (2017), „Government Surveillance and Internet Search Behavior“, abrufbar unter https://ssrn.com/abstract=2412564

47 Lecher (2021), „ How Big Pharma Finds Sick Users on Facebook“, abrufbar unter: https://themarkup.org/citizen-browser/2021/05/06/how-big-pharma-finds-sick-users-on-facebook

Auch bestehen Sorgen darüber, dass mehr Datenaustausch vor allem diejenigen begünstigt, die wegen möglicherweise problematischer Datenpraktiken unter Beobachtung sind. So sind auch Google und Amazon in medizinischen Geschäftsbereichen aktiv.[48] Je nach Ausgestaltung von stärkerem Datenaustausch könnte dieser Konzentrationstendenzen in diesen Märkten verstärken.

Politik & Regulierung

Das Problem der Rechtsunsicherheit über den Austausch von medizinischen Daten lässt sich über die Schaffung eines klaren Rechtsrahmens für Datentreuhänder lösen. Dieser sollte medizinische Forschung so ermöglichen, dass dabei die Risiken beherrschbar bleiben. Unser Vorschlag ist:

→ **Einen Erlaubnistatbestand für die Datenverarbeitung von medizinischen, über eine Datentreuhand vermittelte Daten für medizinische Forschung schaffen**

Datentreuhänder sind geeignet, um stärkeres Datenteilen zu fördern und gleichzeitig die Risiken systematisch zu verringern. Im Idealfall können sie Zugang zu aktuell dezentral gespeicherten Daten geben, bei dem die Forschenden nicht die Daten erhalten, sondern Algorithmen mit Hilfe der Daten trainieren. Jedoch kann es auch ein gewisses Maß an Zentralisierung im Vergleich zum Status Quo geben, je nach Herkunft der Daten. Um die Datennutzung vertrauenswürdig zu gestalten, sind folgende Elemente geeignet:

- eine **Zertifizierung der IT-Sicherheit** durch eine staatlich beaufsichtigte Stelle: Dies ist wichtig, um den Zugang zu den Daten (beziehungsweise der Datenverwaltung) vor unbefugten Zugriffen zu schützen. Hierzu gibt es bereits etablierte Prozesse zum Beispiel beim Bundesamt für Sicherheit in der Informationstechnik. Prinzipiell ist auch die Zertifizierung weiterer Aspekte von Datentreuhändern möglich.[49]
- forschungsprojektspezifische **Ausgestaltung des Datenzugangs in Form von Federated Learning, Aggregierung oder Pseudonymisierung:** Dies ist wichtig, damit der Zugriff auf die Daten nur in dem Umfang erfolgt, der nötig ist, um den gewünschten beziehungsweise erhofften Erkenntnisgewinn zu realisieren. Das heißt, ein Algorithmus kann deutlich präziser werden, wenn dieser (mit Hilfe von Federated Learning) zu großen zusätzlichen Datenmengen geschickt wird, ohne

48 Hurtz (2019), „50 Millionen Patientendaten landen auf Googles Servern", abrufbar unter: https://www.sueddeutsche.de/digital/google-project-nightingale-gesundheitsdaten-ascension-1.4681463; Cellan-Jones (2018), „Amazon joins up with US firms to enter healthcare sector", abrufbar unter: https://www.bbc.com/news/business-42877287; Vengattil, Humer (2020), „Alphabet's Verily targets employer health insurance with Swiss Re partnership", abrufbar unter: https://www.reuters.com/article/us-alphabet-verily-idUKKBN25L1Q9

49 Martin, Pasquarelli (2019), „Exploring Data Trust Certifications", Oxford Insights, abrufbar unter: https://theodi.org/wp-content/uploads/2019/04/Report_-Exploring-Data-Trust-Certification.pdf

dass sensible Daten geteilt werden. Andere Formen der Forschung erfordern aggregierte Daten, zum Beispiel um Hypothesen bzgl. der Risikofaktoren von weit verbreiteten Krankheiten zu testen. Mögliche Treiber zum Beispiel von seltenen Krankheiten explorativ zu erforschen, ist jedoch ohne Zugang zu (pseudonymisierten) individuellen Daten kaum möglich.

- eine **Begrenzung des Datentreuhand-Status und des Datenzugangs** auf (wissenschaftliche oder kommerzielle) Institutionen, die medizinische Forschung betreiben und nicht in einem der für Diskriminierung anfälligen Bereiche (Versicherungen und Werbung) tätig sind:[50] Dies ist wichtig, um bestimmte Risiken kategorisch auszuschließen, wie zum Beispiel das der Diskriminierung. Es ist zwar nicht grundsätzlich ausgeschlossen, dass es Unternehmen gibt, die auch im Versicherungs- oder Werbesektor aktiv sind und gesellschaftlich wünschenswerte Forschungszwecke verfolgen. Jedoch ist es wahrscheinlich, dass der Vertrauensgewinn auf Seiten der Patient:innen durch einen klaren Ausschluss den potenziellen Nutzen des Datenteilens mit solchen Unternehmen überwiegt.

Derzeit basiert die Verarbeitung medizinischer Daten (Routinedaten und Forschungsdaten) überwiegend auf Einwilligungslösungen. Damit Routine- und Forschungsdaten auch für über die in der Einwilligung genannten Zwecke verarbeitet werden dürfen, wird ein Erlaubnistatbestand benötigt. Dieser Erlaubnistatbestand kann die Verarbeitung personenbezogener Daten zum Zwecke der wissenschaftlichen Forschung über eine Datentreuhand gestatten. Er tritt damit an die Stelle alternativer Broad-Consent-Lösungen. Um die berechtigten Interessen der Patient:innen zu wahren, bedarf es auch bei dieser Lösung einer Widerspruchsmöglichkeit. Weitere bestehende Prozesse zur Sicherstellung des Patient:innenschutzes, wie die Prüfung durch eine Ethikkommission, sollten erhalten bleiben.

Während die Nutzung der Datentreuhand somit auf Seite der Patient:innen prinzipiell freiwillig bleibt, kann es sinnvoll sein, mindestens manche Datenbereitstellenden dazu zu verpflichten. Dies gilt für Daten, die im Rahmen öffentlich geförderter Forschung gesammelt werden, und könnte auf andere Gruppen wie Kliniken ausgeweitet werden. Auch ist denkbar, Anreize zur Teilnahme für datenerhebende Organisationen (Kliniken, Medizinunternehmen und andere) zu schaffen, indem Reziprozität als Prinzip etabliert wird: Wer Zugang zu Daten anderer möchte, muss selbst auch Daten bereitstellen (ohne dass dadurch die Widerspruchsmöglichkeit der Patient:innen eingeschränkt würde).

50 Siehe auch Hentschel (2021), „DLD-Konferenz: Interview mit Stefan Vilsmeier – Daten in der Medizin: „Krankheiten lassen sich viel früher erkennen“, abrufbar unter: https://www.focus.de/digital/dldaily/dld-konferenz-interview-mit-stefan-vilsmeier-daten-in-der-medizin-krankheiten-lassen-sich-viel-frueher-erkennen_id_13012769.html?__blob=publicationFile&v=1h

Explizit offengelassen ist, wer Datentreuhand sein kann. In Anbetracht der großen Schwierigkeiten bei der Digitalisierung öffentlicher Einrichtungen und insbesondere des Forschungsdatenzentrums[51] erscheint es wenig zielführend, eine staatliche Stelle mit der Erfüllung der Datentreuhand-Funktion zu beauftragen. Die Expertise von technologisch-medizinischen Unternehmen wie zum Beispiel Brainlab,[52] einem „Google Maps für den OP-Saal", erscheint unerlässlich, um eine effektive Datenmittelung zu ermöglichen. Denkbar sind auch Public-Private-Partnerships. Auch wenn im Gesundheitsbereich vieles für die Etablierung einer einzelnen Datentreuhand-Organisation spricht, ist eine zeitnahe Umsetzung deutlich realistischer, wenn eine Einigung auf Mindeststandards für Interoperabilität zwischen Datentreuhändern erfolgt.

Auch beim Geschäftsmodell sollte Gestaltungsspielraum nicht vorschnell verengt werden. Aufgrund der Nähe zur staatlichen Daseinsfürsorge liegt eine Begründung für eine (teilweise) öffentliche Finanzierung auf der Hand. Zugleich gibt es auch privatwirtschaftliches Interesse an einem stärkeren Datenzugang, der nicht unbedingt dem gesellschaftlichen Interesse entgegensteht. Dies hat sich unter anderem in der Entwicklung der Covid-19-Impfstoffe gezeigt. Auch Unternehmen können dementsprechend zur Finanzierung zumindest beitragen. Auch ist denkbar, dass es Vorgaben geben kann über die Veröffentlichung von Erkenntnissen, die mit über die Datentreuhand bereitgestellten Daten gewonnen werden. Gleiches gilt für Vorgaben für öffentliche Einrichtungen, Daten bereitzustellen. Solche Vorgaben betreffen allerdings auch den Datenzugang über Datentreuhänder hinaus und sollten kohärent ausgestaltet werden.

Umsetzung

Um zeitnah eine Umsetzung anzustreben und die Hürden für eine gesetzliche Regelung überschaubar zu halten, können zunächst Gestaltungsspielräume für einzelne Forschungsbereiche geschaffen werden. Dabei kann es sinnvoll sein, Bereiche mit hoher Dringlichkeit medizinischer Forschung und guter Datenverfügbarkeit zu priorisieren. Die Fokussierung zunächst auf einzelne Bereiche hat in Großbritannien bereits zu Erfolgen geführt. Dort wurden im Oktober 2019 Health Data Research Hubs eingesetzt, die sich klar definierten Bereichen widmen: mentale Gesundheit, Machbarkeit klinischer Studien, Krebsversorgung, Darmentzündungen, einwilligungsgestützter Diagnose, Augenerkrankungen, Lungen- sowie Herz- und Kreislauferkrankungen und klinische Versorgung.[53] Nach eineinhalb Jahren hat die Initiative 300

51 Bundesinstitut für Arzneimittel und Medizinprodukte, „Das Forschungsdatenzentrum", abrufbar unter: https://www.dimdi.de/dynamic/de/weitere-fachdienste/forschungsdatenzentrum/
52 https://www.brainlab.com
53 Health Data Research UK, „Our Hubs", abrufbar unter: https://www.hdruk.ac.uk/helping-with-health-data/our-hubs-across-the-ukz

Projekte umgesetzt, 20.000 Interaktionen mit Patient:innen und der Öffentlichkeit geführt und 157 Datensets verfügbar gemacht.[54]

Als Referenzpunkte im deutschen System können das Krebsregister und das Transplantationsdatengesetz dienen. Auch wenn diese bisher nur sehr eng Daten innerhalb ihrer jeweiligen Domäne nutzbar machen, bieten sie bestimmte Gestaltungselemente, die ausgeweitet werden können. Zugang zum Transplantationsregister kann nach Paragraf 15g des Transplantationsgesetzes auch ohne Einwilligung der Betroffenen gewährt werden, wenn die Einholung einer solchen nur mit unverhältnismäßigem Aufwand möglich ist, das öffentliche Interesse an der Forschung die Interessen der Person überwiegt und der Forschungszweck nur so zu erreichen ist. Zugleich stellt der Einsatz einer Vertrauensstelle ein Mindestmaß an Datenschutz sicher, indem sie die Daten standardmäßig pseudonymisiert. Beim Krebsregister werden zumindest teilweise auch weitere Daten einbezogen und stark aggregierte Ergebnisse lassen sich sogar in einer über die Webseite abrufbare Datenbank ohne zusätzliche Hürden einsehen.

Allerdings ist es wichtig, dass priorisierte Bereiche für die Entwicklung von Datentreuhandmodellen verbunden sein sollten, ähnlich wie die Health Data Research Hubs in Großbritannien zentral koordiniert sind. Ein Mindestmaß an Standardisierung und Interoperabilität, die möglichst früh in die Gestaltung der Modelle einbezogen werden sollte, ist wichtig, damit erfolgreiche Ansätze schnell skaliert werden können.

4.2. PIMS

Status Quo

PIMS sind bisher keine klar abgegrenzte Gruppe von Diensten. Der Europäische Datenschutzbeauftragte charakterisiert sie als „Systeme, die natürlichen Personen mehr Kontrolle über ihre personenbezogenen Daten geben sollen“.[55] Sie werden oft als Datenportale bezeichnet, über die Verbraucher:innen Daten aus unterschiedlichen Quellen zusammenführen und gegebenenfalls neuen Zwecken zuführen, wie

54 Health Data Research UK (2021), „Improving UK Health Data: Impact from Health Data Research Hubs“, abrufbar unter: https://www.hdruk.ac.uk/wp-content/uploads/2021/04/Improving-UK-Health-Data-Impacts-from-Health-Data-Research-Hubs_compressed.pdf

55 Weiter schreibt der Europäische Datenschutzbeauftragte: „Mittels PIMS haben Menschen die Möglichkeit, ihre personenbezogenen Daten in sicheren, lokalen oder Online-Speichersystemen zu verwalten und sie zu teilen, wann und mit wem sie es wünschen. Anbieter von Onlinediensten und Werbetreibende werden mit den PIMS interagieren müssen, wenn sie beabsichtigen, die Daten natürlicher Personen zu verarbeiten. Dadurch können ein am Menschen orientierter Ansatz in Bezug auf personenbezogene Informationen und auch neue Geschäftsmodelle entstehen.“, abrufbar unter: https://edps.europa.eu/data-protection/our-work/subjects/systeme-de-gestion-des-informations-personnelles_de

die Dienste beziehungsweise Unternehmen digi.me, bitsabout.me, itsmydata oder (in der Entwicklungsphase) polypoly.[56] Eingeschlossen sind auch Einwilligungsmanagementsysteme, mit denen Verbraucher:innen an einer Stelle ihre Präferenzen bezüglich der Sammlung und Verwendung von Daten über sie festlegen können. Diese befinden sich zwar noch in der Entwicklung, werden jedoch schon im Rahmen des TTDSG und auch des DGA (siehe Abschnitt 3.1.) regulatorisch betrachtet. Tabelle 2 fasst die wesentlichen Funktionalitäten und Geschäftsmodelle ausgewählter aktiver PIMS zusammen.

Tabelle 2: Ausgewählte aktive PIMS

Name	Funktionalitäten	(De-)Zentral	Geschäftsmodell	Fokusbereich(e)
Digi.me	Nutzer:innen tragen persönliche Daten von diversen Plattformen und Diensten in App/Website zusammen, erlangen eine Übersicht und verfügen über mögliche Nutzung durch Dritte	Dezentrale Speicherung in Cloud der Nutzer:innen	Transaktionsgebühr (7,5%)	App ist Basis eines Daten-Ökosystems aus Apps, die von Dritten entwickelt werden, zum Beispiel Gesundheits- oder Travel-Apps
Bitsabout.me		Zentrale Speicherung auf EU-Servern	Transaktionsgebühr (7,5%)	Monetarisierung persönlicher Daten durch Nutzer:in
Itsmydata		Zentrale Speicherung auf deutschen Servern	Verkauf von Bonitätsbescheinigung an Nutzerinnen; geplant: Transaktionsgebühr	Günstiges Bonitätszertifikat basierend auf Daten von Schufa, Boniversum, etc.
polypoly		Dezentrale Speicherung auf Gerät der Nutzer:innen	Geplant: Software-Lizenzen, Transaktionsgebühren	Genossenschaftliche Verwaltung der Technologie

Quellen: Webseiten der Diensteanbieter

Allerdings ist die Nutzung von PIMS begrenzt, was auch auf ihre eingeschränkten Funktionalitäten zurückgeführt werden kann. Ein Grund dafür wiederum liegt in der individualistischen Lesart der Datenrechte in der DSGVO, die eine Delegierung des Einwilligens oder der Wahrnehmung von Rechten wie des Rechts auf Portabilität untersagt. Damit obliegt es Individuen weiterhin, jede (Nicht-)Einwilligung in Datensammlung und -nutzung vermeintlich informiert selbst durchzusetzen.[57]

56 https://www.itsmydata.de; https://www.digi.me; https://www.polypoly.eu; https://www.bitsabout.me
57 Zu den Problemen einer individuellen Einwilligung siehe u.a. Blankertz (2020), „Designing Data Trusts“

Eine Form der Delegation von Rechten von PIMS ist erlaubt unter dem California Consumer Privacy Act (CCPA). Dieser erlaubt Verbraucher:innen die Benennung von „authorized agents", die Unternehmen den Verkauf persönlicher Daten verbieten oder ihre Löschung anfordern können. Consumer Reports, eine US-amerikanische Verbraucher:innenorganisation, hat in einem Pilotprojekt[58] festgestellt, dass eine deutliche Nachfrage nach einem solchen Dienst besteht, um die Durchsetzung von Datenrechten effektiver und einfacher zu gestalten.[59] Aktuell bietet eine Bandbreite an Organisationen sich als authorized agent an. Der CCPA schränkt prinzipiell nicht ein, wer diese Rolle übernehmen kann und zu welchen Konditionen. Das heißt, es obliegt Verbraucher:innen, für ihre Zwecke geeignete und vertrauenswürdige Organisationen auszuwählen. Bisher scheint dieser Ansatz funktional, denn es sind keine Fälle von Missbrauch öffentlich bekannt.

Ein weiterer Grund für die geringe Marktdurchdringung von PIMS ist ihre Freiwilligkeit: Momentan sind sie für alle Beteiligten freiwillig in der Nutzung und damit leicht zu umgehen. Verbraucher:innen können zwar Daten über sich zu PIMS „lenken", doch sie können nicht Unternehmen dazu verpflichten, zum Beispiel den Einwilligungsprozess über den PIMS abzuwickeln. Das heißt, dass PIMS für Verbraucher:innen bisher ein zusätzlicher Dienst sind, den sie neben der manuellen Steuerung von Datenflüssen nutzen, statt die manuelle Steuerung über den PIMS zumindest teilweise ersetzen zu können.

Nutzen und Risiken

Dienste, die die Interessen von Verbraucher:innen in Bezug auf Daten durchsetzen, werden vielfach propagiert, unter anderem durch die Organisation MyData. Das Potenzial liegt in einem Datenökosystem, in dem sich Datenflüsse stärker an den Interessen von Verbraucher:innen orientieren. Das bedeutet einerseits eine effektivere Begrenzung von Datenflüssen und Herstellung eines gewünschten, einheitlichen Datenschutzniveaus[60] und andererseits eine (einfache) Ermöglichung von Datenflüssen, wo diese Verbraucher:innen begünstigen.[61]

58 Consumer Reports (2021), „Consumer Reports study finds authorized agents can empower people to exercise their digital privacy rights in California", abrufbar unter: https://advocacy.consumerreports.org/press_release/consumer-reports-study-finds-authorized-agents-can-empower-people-to-exercise-their-digital-privacy-rights-in-california/

59 Es wurden weiterhin umfassende Schwierigkeiten in der Kommunikation mit Diensteanbietern berichtet, damit diese auf die Anfragen reagierten. Dabei erscheint es plausibel, dass interessierte Individuen bei solchen Schwierigkeiten keinen weiteren Aufwand auf sich genommen hätten, im Gegensatz zu Consumer Reports.

60 Stiftung Datenschutz (2017), „Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen", abrufbar unter: https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/PIMS-Abschluss-Studie-30032017/stiftungdatenschutz_PolicyPaper_Neue_Wege_zur_Einwilligung_DE_EN_final.pdf

61 Blankertz (2020), op. cit.

Gleichzeitig bestehen große Bedenken, ob beziehungsweise welche Organisationen als PIMS beziehungsweise Datentreuhand im Verbraucher:inneninteresse in Betracht kommen dürfen. Für PIMS für Einwilligungsmanagement legt das TTDSG eine Unternehmensstiftung als Organisationsform nahe und sieht kommerzielle Ansätze skeptisch (siehe Abschnitt 3.1.). Diese Skepsis dürfte darauf beruhen, dass viele Dienste, die für problematische Datenpraktiken bekannt sind, ebendiese Praktiken gegenüber ihren Nutzer:innen verschleiern.[62] Somit steht bei Google, Facebook und anderen in Frage, ob die Verbraucher:innenentscheidung, diesen Unternehmen eine Einwilligung zur Erhebung umfassender personenbezogener Daten zu geben, gesellschaftlich wünschenswert ist. Bei neuen Diensten besteht dementsprechend eine starke politische Absicht, ähnliche Dynamiken zu vermeiden. Allerdings deutet das Beispiel des authorized agent im CCPA darauf hin, dass auch ein wenig restriktiver Ansatz fruchtbar sein kann.

Es liegt nahe, möglichen Machtmissbrauch durch PIMS weitestgehend im Vorfeld ausschließen zu wollen. Jedoch deutet der Umstand, dass sich bisher noch kein PIMS wirklich am Markt durchgesetzt hat, darauf hin, dass die bestehenden Gegebenheiten bereits herausfordernd sind, um einen für viele Verbraucher:innen attraktiven Dienst zu entwickeln. Weitere Beschränkung durch Regulierung würde die Chancen eines möglichen Erfolgs von PIMS erst recht verringern. Stattdessen könnte stärker ermöglichende Regulierung dabei helfen, eine kritische Masse an PIMS-Diensten und -Nutzer:innen anzureizen.

Politik und Regulierung

PIMS erhalten vielfach politische Aufmerksamkeit, zuletzt mit der Verabschiedung des TTDSG. Bisher mangelt es jedoch an konkreten Vorschlägen, die die bekannten Hürden – insbesondere mangelnde Delegierbarkeit und einfache Umgehbarkeit – zusammen löst. Unser Vorschlag ist:

→ **Muster-AGB für PIMS zur Grundlage für eine Zertifizierung machen und eine verpflichtende Zusammenarbeit mit zertifizierten PIMS unternehmensseitig vorsehen**

Die Zertifizierung von Allgemeinen Geschäftsbedingungen (AGB) kann einen hohen, vertrauenswürdigen Mindeststandards von PIMS sicherstellen. Die Zertifizierung, durchzuführen durch eine staatliche Stelle (zum Beispiel den BfDI oder die Bundesdruckerei), dient dazu, die PIMS umfassend an die Interessen der Nutzer:innen zu binden. Hierzu geeignete Elemente sind:

62 Forbrukerrådet (2018), „Deceived by Design“, abrufbar unter: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

1. **Mindeststandards für IT-Sicherheit** (analog zu denen für Gesundheitsdaten).
2. **Restriktionen in Bezug auf die Monetarisierung** personenbezogener Daten durch die Datentreuhand, sodass diese nur mit expliziter Einwilligung erfolgen darf: Sofern die Weitergabe personenbezogener Daten gegen Bezahlung erfolgt, sollte hierzu eine explizite Einwilligung der Verbraucher:innen vorliegen. Um das Missbrauchspotenzial auch nicht-personenbezogener Daten möglichst gering zu halten, kann dies Daten in aggregierter oder anonymisierter Form betreffen, selbst wenn deren Weitergabe datenschutzrechtlich möglicherweise zulässig ist. Demgegenüber kann die bei nicht-monetärem Datenzugang erforderliche Einwilligung entsprechend breiter (zum Beispiel für allgemeinere Zwecke) gefasst werden.
3. **Restriktionen des Datenzugangs für verbundene Dienste:** Datenzugang an verbundene Dienste sollte zu gleichen Bedingungen stattfinden wie zu externen Diensten. Damit wird sichergestellt, dass auch intern eine explizite Einwilligung eingeholt wird für Daten, die nach außen monetarisiert werden.
4. **Transparenzvorgaben** in Bezug auf die monetäre und nicht-monetäre Übermittlung von Daten: Beispielsweise ist denkbar, dass eine leicht zugängliche, ständig aktualisiert Übersicht bereitgestellt wird darüber, welchen Organisationen Datenzugang mit beziehungsweise ohne Bezahlung gewährt wird, mit mehr Detail zum Datenzugang bei monetärem Austausch.

Wenn diese Standards erfüllt sind, ist das Risiko von für Nutzer:innen nachteilhaften Datenpraktiken deutlich verringert. Dies wiederum ist die Voraussetzung, um den PIMS stärkere Befugnisse einzuräumen, wie zum Beispiel authorized agents unter dem CCPA sie erhalten. Für Nutzer:innen wiederum ist der Nutzen eines PIMS größer, wenn sie die Durchsetzung ihrer Datenrechte stärker delegieren können. Eine Möglichkeit zur Umsetzung besteht darin, dass ein PIMS eine „breite" Einwilligung von Nutzer:innen einholen darf und diese wiederum spezifisch gegenüber weiteren Parteien durchsetzt, ohne dass der:die Nutzer:in in jeder Interaktion aktiv werden muss.

Damit Datentreuhändern nicht so einfach zu umgehen sind, insbesondere wenn die Datentreuhänder die Durchsetzung von Datenrechten fördern, ist es zielführend, mindestens bestimmten datenverarbeitenden Diensten eine Pflicht zur Kooperation aufzuerlegen. Dabei kann mindestens zu Beginn eine Beschränkung auf einzelne Sektoren sinnvoll sein, um hohen administrativen Aufwand für Unternehmen zu vermeiden. Mögliche Kandidaten sind Browser-Anbieter und/oder Zielgruppen von Wettbewerbsregulierung wie Adressaten des Digital Markets Act oder des Artikel 19a des Gesetzes gegen Wettbewerbsbeschränkungen.[63]

63 Diese beiden Regulierungen beziehungsweise -entwürfe beziehen sich auf nach verschiedenen Kriterien definierte marktübergreifend besonders wichtige Dienste, an die höhere Anforderungen gestellt werden. Siehe Referentenentwurf zur 10. GWB-Novelle des Bundesministeriums für Wirtschaft und Energie (2021), „Zehntes Gesetz zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 (GWB-Digitalisierungsgesetz)" und Europäische Kommission (2020e), op. cit.

Gleichzeitig weisen die Geschäftsmodelle aktiver PIMS-Anbieter darauf hin, dass zu allgemein gefasste Anforderungen an Neutralität riskieren, dass die bestehenden Ansätze unzulässig würden. Alle in Tabelle 2 aufgeführten Anbieter erheben oder planen die Erhebung von Transaktionsgebühren, die als ein Interesse an einem Datenaustausch gewertet werden können. Durch prozentuale Transaktionsgebühren entsteht nämlich prinzipiell ein Interesse an einem größeren Datenvolumen, das über den PIMS vermittelt wird. Allerdings gibt es im Konkreten bisher keine Kritikpunkte an den Praktiken dieser PIMS und sie werden teilweise sogar als förderns-wert erachtet.[64]

4.3. Produktpässe

Status Quo

Die Nachverfolgbarkeit von Produkten und Produkteigenschaften über die Wertschöpfungskette ist ein zunehmend wichtiger Erfolgsfaktor für die Wirtschaft. Viele Verbraucher:innen legen Wert zum Beispiel auf die Produktionsbedingungen von Unternehmen; die Politik fördert und fordert nachhaltigeres Wirtschaften. Ein Beispiel ist die geplante Entstehung eines Datenraums für eine Kreislaufwirtschaft, der sogenannte Produktpässe beinhalten soll.[65] Priorisiert werden hierbei Sektoren mit hohem Ressourcenverbrauch und großem Potenzial für stärkere Wiederverwertung wie elektronische Geräte, Batterien und Autos, Verpackung, Textilien, Gebäude, Nahrungsmittel und Wasser.[66] Die Vielfalt der Prioritäten zeigt bereits auf, dass sehr unterschiedliche Produktbestandteile und -eigenschaften über eine Datentreuhand erfassbar sind.

Verschiedene Anbieter stellen Lösungen bereit, um Produkte über Lieferketten hinweg nachverfolgbar zu machen. Wichtig ist dabei, dass es ein gewisses Maß an Standardisierung gibt, um produkt- beziehungsweise herstellerübergreifende Lösungen zu ermöglichen. Eine Plattform für das Setzen solcher Standards ist GS1, ein Zusammenschluss zahlreicher internationaler Unternehmen, der standardisierte Barcodes bereitstellt,67 vor allem in den Bereichen Nahrungsmittel, Gesundheit und Transport.

64 So fördert die Europäische Union Projekte zur Nutzung und Monetarisierung personenbezogener Daten u.a. mit dem Projekt DataVaults, https://www.datavaults.eu/

65 Europäische Kommission (2020a), „Appendix to the Communication ‚A European strategy for data'", abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

66 Europäische Kommission (2020c), „Circular economy action plan", abrufbar unter: https://ec.europa.eu/environment/strategy/circular-economy-action-plan_en

67 https://www.gs1.org/about

Nutzen und Risiken

Aktuell ist die Nachfrage nach Produktdaten durch Endverbraucher:innen oder Investor:innen getrieben, die die Einhaltung bestimmter Standards wünschen. Eine bisher untergeordnete Rolle spielt die Entstehung von neuen Märkten, die auf Grundlage der Produktdaten bestehende Ressourcen effizienter zuordnen und eine Monetarisierung von aktuell ungenutzten Ressourcen ermöglichen. Die Vermittlung zwischen denjenigen, die recyclebare Ressourcen haben, und denen, die sie nutzen können, ist komplex – insbesondere im Falle von sektorübergreifender Kooperation. Gefordert sind Plattformen wie zum Beispiel Excess Materials Exchange,[68] die in vielen der von der EU priorisierten Bereiche Projekte zur Wiederverwertung etabliert haben. Perspektivisch ist eine Einbindung von Daten über die Wertschöpfungskette erforderlich, über die schon bei der Produktentwicklung die späteren Verwertungsmöglichkeiten in Erwägung gezogen werden.

Die steigende Transparenz durch Produktpässe ist für viele Beteiligte potenziell wertvoll. Sie ist eine Voraussetzung (wenn auch keine hinreichende Bedingung), um eine Einhaltung von Standards sicherzustellen. Risiken und Nachteile ergeben sich zunächst für diejenigen, die von Intransparenz profitieren, oder auch, wenn ineffiziente Standards gesetzt werden. Außerdem könnten Ungleichgewichte innerhalb der Wertschöpfungskette verstärkt werden, falls Transparenz nur einseitig gewährleistet wird oder der stärkere Verhandlungspartner sich die Effizienzen allein aneignet (zum Beispiel über das Verhandeln strengerer Lieferbedingungen). Auch in der Standardisierung könnten Ungleichgewichte zum Tragen kommen, wenn große Anbieter Anforderungen durchsetzen, die kleinere benachteiligen. Jedoch konzentrieren sich die Anstrengungen momentan darauf, überhaupt einen möglichst übergreifenden Standard zu schaffen, weil eine starke Zersplitterung den Erfolg von Produktpässen gefährden könnte. Die Risiken scheinen bisher limitiert, sondern die Herausforderung besteht darin, den Datenaustausch zunächst zu ermöglichen.

Für eine stärkere Nachvollziehbarkeit über Wertschöpfungsketten hinweg gibt es zwei wesentliche Hürden: Erstens ist der administrative und finanzielle Aufwand einer Digitalisierung von Liefer- und Produktionsprozessen oft erheblich. Zweitens wird es oft als primär administrative Aufgabe verstanden, die aus Management-Sicht eher niedrig priorisiert wird oder, gerade für kleine Unternehmen, die verfügbaren Ressourcen übersteigt. Dies trifft selbst dann zu, wenn der Nutzen über die Transparenz gegenüber Abnehmer:innen und Endkund:innen deutlich hinausgeht und durch die Daten ein positiver Wert generiert werden kann, der jedoch nicht geschäftskritisch ist. Beide Hürden sind voraussichtlich temporär, da eine Digitalisierung und Datenerfassung innerhalb von Unternehmen unausweichlich erscheint und die schlechte Datenverfügbarkeit einer der Hauptgründe für den hohen Management-Aufwand ist.

68 https://excessmaterialsexchange.com/en_us/

Politik & Regulierung

Es ist nicht offensichtlich, dass es einer restriktiven Regulierung für Datentreuhänder bedarf, die Produktpässe anbieten wollen. So ist es offen, inwiefern zentrale oder dezentrale Modelle zum Einsatz kommen sollen und es kann je nach Produkt und Funktion variieren. Fälle von Missbrauch oder anderen negativen Konsequenzen durch Produktdatenintermediäre sind nicht bekannt. Aus wettbewerbspolitischer Sicht kann sich ein Bedarf zur Abwägung verschiedener Ziele ergeben, wenn ein Unternehmen Marktmacht nutzt, um höhere Nachhaltigkeitsstandards in Lieferketten durchzusetzen.

Stattdessen stellt sich vielmehr die Frage, inwiefern sich die Entwicklung von Transparenz in Form von Produktpässen fördern lässt, da Unternehmen bisher eher zurückhaltend damit sind, ihre Produkte stärker nachvollziehbar zu machen. Ein ermöglichendes Element ist die kartellrechtliche Prüfung von Datenkooperationen, die seit der 10. GWB-Novelle innerhalb maximal eines halben Jahres durch das Bundeskartellamt geschehen soll.[69] Darüber hinaus kann der Staat die Weiterentwicklung des Datenaustausch in bestimmten Bereichen fördern, wie aktuell auf EU-Ebene über Pilotprojekte im Kontext des Kreislaufwirtschaft-Datenraums erfolgt. Ein weiteres Instrument ist die strategische Nachfrage des Staates in der Beschaffung zum Beispiel von Bauprojekten, in der die Bereitstellung von Produktpässen eine notwendige Voraussetzung werden kann. Damit würde die Nutzung einer solchen Datentreuhand unter gewissen Umständen nicht rein freiwillig, sondern teilweise verpflichtend. Ähnliches gilt für mögliche Nachhaltigkeitsreporting-Anforderungen, die der Staat und/oder Finanzmärkte an Unternehmen stellen. Diese können dazu führen, dass Nachhaltigkeit in Lieferketten und internen Prozessen an unternehmensinterner Relevanz gewinnen.

4.4. Agrardaten

Status Quo

Daten aus und für die Landwirtschaft stammen aus vielfältigen Quellen, von Sensoren im Boden und Maschinen, über Wetter- und Klimadaten, hin zu ökonomischen Entwicklungen auf dem Weltmarkt.[70] Dabei im Fokus stehen häufig die Maschinendaten, deren Kompatibilität, Zugang und Weiterverwendung vielerorts diskutiert

69 Gesetz gegen Wettbewerbsbeschränkungen, Paragraf 32c.4
70 Wolfert, Ge, Verdouw, Bogaardt (2017), „Big Data in Smart Farming – A review", Agricultural Systems, Volume 153, Seite 69-80, abrufbar unter: https://www.sciencedirect.com/science/article/pii/S0308521X16303754

werden, von Australien[71] über die USA[72] nach Europa.[73] Das Niveau der Digitalisierung der Maschinen ist recht hoch und viele Daten werden standardmäßig erfasst, ohne dass Landwirt:innen hierzu weitere Bemühungen anstellen müssten.

Nutzen und Risiken

Teilweise nutzen landwirtschaftliche Betriebe Maschinen- und andere Daten bereits, um die Bewirtschaftung zum Beispiel mit Düngemitteln oder Wasser stärker auf die Beschaffenheit von Teilflächen abzustimmen (auch Precision Farming genannt). Es besteht ein deutliches Potenzial, nicht nur Erträge zu erhöhen, sondern auch Ressourcen gezielter einzusetzen. So können Daten für einzelne Maschinen kalibriert werden, um verschiedene Flächen eines Ackers unterschiedlich zu bearbeiten.

Aktuell erfolgt die Datenerhebung und -nutzung in einzelnen Betrieben ohne einen Austausch über Betriebe hinweg. Das heißt, dass jeder Betrieb nur aus den eigenen Daten lernt und keine übergreifenden Analysen erfolgen.

Um betriebsübergreifende Analysen zu ermöglichen, bedarf es allerdings zwei Voraussetzungen: Erstens müssen Daten in einem austauschbaren Format vorliegen, um sinnvoll ausgewertet werden zu können. Der Prozess der Standardisierung läuft bereits und Organisationen wie zum Beispiel agrirouter arbeiten an Lösungen, die eine maschinenherstellerübergreifende Datenverarbeitung ermöglichen. Agrirouter fungiert als eine Plattform zwischen vielen Maschinenherstellern, die Softwareanbieter über standardisierte Schnittstellen mit Landwirt:innen verbindet.

Zweitens bedarf es einer Bereitschaft, Daten tatsächlich auszutauschen. Hierzu mangelt es teils an der Digitalisierung und Datennutzung in den Betrieben selbst (auch wenn die Maschinen die Daten erheben). Darüber hinaus werden die Risiken oft als konkreter wahrgenommen als der mögliche Nutzen einer besser trainierten Bewirtschaftungssoftware. Zu diesen Risiken zählt insbesondere die Aufgabe von Geschäftsgeheimnissen, wie zum Beispiel die spezifischen Erträge und Bewirtschaftungsweisen. Im deutschen Kontext nicht praktisch relevant erscheint das Macht- und Informationsgefälle zwischen Maschinenherstellern und Landwirt:innen, auch wenn dies in der Literatur gelegentlich Erwähnung findet.[74]

71 Wiseman, Sanderson (2017), "The legal dimensions of digital agriculture in Australia: An examination of the current and future state of data rules dealing with ownership, access, privacy and trust", abrufbar unter: https://www.crdc.com.au/sites/default/files/CRD18001-001%20CRDC%20P2D%20Report%20low%20res.pdf

72 American Farm Bureau Federation (2016), "Privacy and Security Principles for Farm Data", abrufbar unter: https://www.fb.org/issues/innovation/data-privacy/privacy-and-security-principles-for-farm-data

73 an der Burg, Wiseman, Krkeljas (2020), „Trust in farm data sharing: reflections on the EU code of conduct for agricultural data sharing", Ethics and Information Technology, abrufbar unter: https://link.springer.com/article/10.1007/s10676-020-09543-1

74 Zscheischler et al. (2021), „Kapitel 4 Landwirtschaft, Digitalisierung und digitale Daten" in DiDaT Weißbuch, abrufbar unter: https://www.researchgate.net/publication/349557077_Kapitel_4_Landwirtschaft_Digitalisierung_und_digitale_Daten

Politik & Regulierung

Auf deutscher Ebene, in Anlehnung an die geplanten EU-Datenräume, ist bereits „Agri-Gaia“ in Planung unter Planung des Bundesministeriums für Wirtschaft und Energie. Dieses soll unter anderem Datenteilen zwischen Akteuren befördern, wobei nicht absehbar ist, inwieweit dies betriebsübergreifende Analysen einschließt. Es ist davon auszugehen, dass es sich dabei um eine primär dezentrale Datentreuhand handeln wird, deren Nutzung überwiegend freiwillig sein wird. Das geht einher mit einer eher niedrigen Risikobewertung des Datenaustauschs, was wiederum für eine niedrige Regulierungsintensität spricht.

Es könnten allerdings Anreize zur Nutzung einer Datentreuhand in Erwägung gezogen werden: Landwirt:innen wünschen sich teilweise eine bessere Bereitstellung relevanter Daten durch den Staat, zum Beispiel von präzisen Kartendaten einschließlich umweltregulatorischer Anforderungen. Wie in Abbildung 4 ersichtlich, treten staatliche Stellen nicht als Bereitsteller von Daten von Agri-Gaia in Erscheinung. Dabei könnte ein staatlich generierter Mehrwert der Nutzung einer solchen Datentreuhand durchaus die Hürden für Landwirt:innen senken, selbst Daten zu erheben und bereitzustellen.

Darüber hinaus ist eine stärker monetäre Anreizsetzung denkbar. Beispielsweise ist es nicht unüblich, die Weiterzahlung mancher Subventionen an bestimmte Voraussetzungen zu knüpfen. Die Bereitstellung entsprechend zu anonymisierender Daten könnte eine solche Voraussetzung sein.

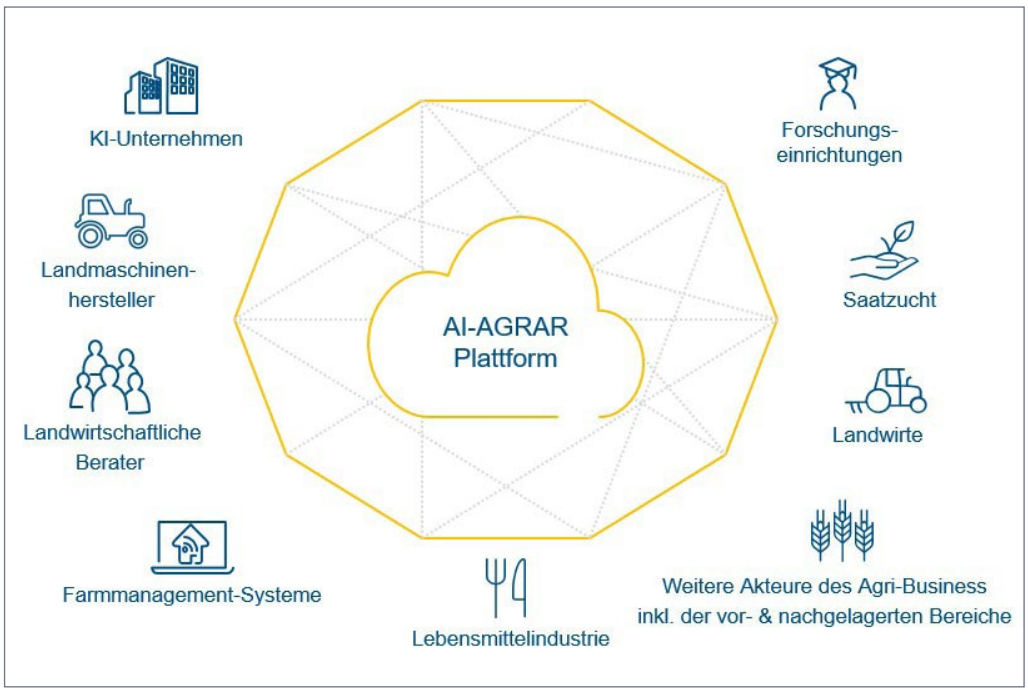

Abbildung 4: Akteure der AI-Agrar-Plattform

Quelle: Bundesministerium für Wirtschaft und Energie, „Agri-Gaia“, abrufbar unter: https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/GAIA-X-Use-Cases/agri-gaia.htm

5. Schlussfolgerungen für die Ausgestaltung von Datentreuhänderregulierung

Datentreuhandmodelle können viele verschiedene Formen annehmen, um Datennutzung und Datenschutz und gegebenenfalls weitere Schutzzwecke zusammenzuführen. Aktuelle Regulierungsvorhaben riskieren eine zu starke Verengung des Spielraums für Unternehmen und andere Organisationen, die als Datentreuhand aktiv sind oder werden können. Diese Vorhaben, insbesondere der DGA, formulieren allgemeine Anforderungen, die sich bei der Betrachtung spezifischer Anwendungsfälle oft als nicht notwendig herausstellen.

Wenn die Politik einen Beitrag dazu leisten will, dass sich Datentreuhandmodelle etablieren, sollte sie Vertrauenswürdigkeit gezielt durch eine Regulierung fördern, die die Risiken spezifischer Anwendungsfälle berücksichtigt. Risikofaktoren können sektorübergreifend identifiziert werden; insbesondere die zentrale oder dezentrale Datenspeicherung und die freiwillige oder verpflichtende Nutzung der Datentreuhand gehören dazu. Nicht dazu gehört das Geschäftsmodell: Während die Regulierungsvorhaben allgemein Neutralität fordern, gibt es verschiedene Datentreuhandansätze, die auch ohne strikte Neutralität in Bezug auf Monetarisierung oder vertikale Integration vertrauenswürdig erscheinen. Zugleich ist unklar, welche Anreize für die Entwicklung strikt neutraler Datentreuhandmodelle bestehen.

Zudem erschließen sich aus der Betrachtung der vier Anwendungsfälle Empfehlungen für die konkrete Ausgestaltung von Datentreuhandregulierung:

Die Anwendungsfälle zeigen ein breites Spektrum von Ansätzen auf, mit denen verschiedene Ziele verfolgt werden und die mit spezifischen Herausforderungen verbunden sind. Eine Regulierung sollte nicht dazu dienen, ein vermeintlich optimales Modell zu etablieren, insbesondere bei fehlenden Anreizen zur Umsetzung eines solchen Modells. Stattdessen sollte die Regulierung konkrete Risiken und Probleme lösen.

- Bei den beiden Anwendungsfällen ohne nennenswerten Personenbezug (Agrardaten und Produktpässe) ist fraglich, inwiefern Regulierung sinnvoll ist, da es vor allem an Anreizen mangelt, um stärkeres Datenteilen und/oder neue Modelle zu etablieren.
- Bei den beiden Anwendungsfällen mit Personenbezug (medizinische Daten und PIMS) bestehen teilweise unterschiedliche Ziele und Risiken, die gezielter Maßnahmen bedürfen.

Eine Regulierung sollte bestehende Rechtsunsicherheit und Komplexität auf keinen Fall erhöhen, sondern senken. Dies ist nötig, um einen Anreiz für die Entwicklung neuer Modelle zu schaffen.

- Vertrauensstiftende Maßnahmen, die Risiken absichern, begründen die Verringerung anderer Hürden. Dies ist der Fall zum Beispiel bei einem Erlaubnistatbestand für Gesundheitsdaten über eine Datentreuhand, der auch ohne eine Einwilligung die Nutzung der Daten für medizinische Forschung ermöglicht. In ähnlicher Form kann es PIMS erlaubt werden, Nutzer:innen umfassender zu vertreten, wenn weitere Absicherungsmechanismen vorliegen, die Missbrauch verhindern.
- Übermäßig restriktive Neutralitätsanforderungen führen zwangsläufig zu einer Bereitstellung von Datentreuhändern durch den Staat, was aus verschiedenen Gründen je nach Anwendungsfall problematisch sein kann. Neutralität in Bezug auf Monetarisierung und vertikale Integration entsprechen nicht der Realität von bestehenden PIMS und anderen Datentreuhandmodellen. Vorzuziehen sind Bestimmungen zur Vermeidung konkreter Interessenkonflikte, wie zum Beispiel der Ausschluss von Versicherungen und Werbeunternehmen im Zusammenhang mit einer medizinischen Datentreuhand.

Zertifizierung kann ein sinnvolles Instrument sein, um Transparenz bezüglich konkret definierter Anforderungen zu erhöhen. Sie kann dort zum Einsatz kommen, wo das Risiko einer zu restriktiven Regulierung zu hoch ist und gleichzeitig klarer Interventionsbedarf besteht, zum Beispiel aufgrund von Informationsasymmetrien.

- Im IT-Sicherheitsbereich ist Zertifizierung bereits etabliert und kann besonders dort sinnvoll sein, wo Verbraucher:innen die Dienste nutzen, da diese tendenziell weniger Expertise und Ressourcen haben, um einen Anbieter zu beurteilen. Dies ist vor allem bei medizinischen Daten und PIMS der Fall.
- Für PIMS ist die Zertifizierung von AGBs eine Möglichkeit, um die Vertrauenswürdigkeit von Diensten zu erhöhen, ohne Dienste zu verbieten, die bestimmte Kriterien nicht erfüllen. Das gilt zum Beispiel für die volle Transparenz von Datenmonetarisierung und Gleichbehandlung vertikal integrierter Dienste.

Eine pragmatische Möglichkeit, Datentreuhandmodelle zu fördern, ist die Nutzung von Pilotprojekten und der strategische Einsatz staatlicher Nachfrage. Allerdings ersetzt dies nicht die Entwicklung von neuen Modellen und insbesondere Geschäftsmodellen.

- Die Erfahrung mit authorized agents im CCPA zeigt, dass die Repräsentierung von Verbraucher:innen durch zum Beispiel PIMS ein sinnvolles Instrument zur Stärkung von Datenrechten sein kann.

- Die Erfahrung in Großbritannien mit Health Data Research Hubs zeigt, dass es möglich ist, für Gesundheitsdaten Prioritäten zu setzen, um Datenaustausch zunächst in bestimmten Bereichen zu verbessern, ohne eine allübergreifende Datenbank zu erschaffen.
- Im Bereich der Produktpässe für die Kreislaufwirtschaft kann staatliche Nachfrage ein starker Treiber für die Verbreitung von Produktpässen für bestimmte Produkte sein.

Zusammengefasst gibt es viele Wege, die Entwicklung von Datentreuhändern zu fördern, um Datennutzung und Datenschutz besser vereinbar zu machen. Die aktuellen Regulierungsvorhaben sind hierbei allerdings eher kontraproduktiv. Regulierung sollte sich auf konkrete Risiken fokussieren, die durch den bestehenden Rechtsrahmen nicht abgedeckt sind, und auch eine Absenkung mancher Hürden in Erwägung ziehen, wenn zusätzliche Regulierung die Risiken bereits ausreichend adressieren.

Literaturverzeichnis

ACCC (2019), „Consumer Data Right in Energy – Position Paper: data access model for energy data“, abrufbar unter: https://www.accc.gov.au/system/files/ACCC%20-%20CDR%20-%20energy%20-%20data%20access%20models%20position%20paper%20-%20August%202019.pdf

ACCC (2020), „Energy Rules Framework – Consultation Paper“, S.36 f., abrufbar unter: https://www.accc.gov.au/system/files/CDR%20-%20Energy%20rules%20framework%20consultation%20paper%20-%20July%202020_0.pdf.

American Farm Bureau Federation (2016), “Privacy and Security Principles for Farm Data“

an der Burg, Wiseman, Krkeljas (2020), „Trust in farm data sharing: reflections on the EU code of conduct for agricultural data sharing“, Ethics and Information Technology, abrufbar unter: https://link.springer.com/article/10.1007/s10676-020-09543-1

Blankertz (2020), „Designing Data Trusts“

Blankertz, von Braunmühl, Kuzev, Richter, Richter, Schallbruch (2020), „Datentreuhandmodelle“, abrufbar unter: https://www.ip.mpg.de/de/publikationen/details/datentreuhandmodelle-themenpapier.html

Bundesdruckerei, iRights (2019), „Zukunft Gesundheitsdaten“, abrufbar unter: https://www.bundesdruckerei.de/system/files/dokumente/pdf/Studie_Zukunft-Gesundheitsdaten.pdf.

Bundesinstitut für Arzneimittel und Medizinprodukte, „Das Forschungsdatenzentrum“, abrufbar unter: https://www.dimdi.de/dynamic/de/weitere-fachdienste/forschungsdatenzentrum/

Bundesministeriums für Wirtschaft und Energie (2021), „Zehntes Gesetz zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 (GWB-Digitalisierungsgesetz)“

Bundesregierung (2021), „Datenstrategie der Bundesregierung“, Januar

Cellan-Jones (2018), „Amazon joins up with US firms to enter healthcare sector“, abrufbar unter: https://www.bbc.com/news/business-42877287

Consumer Reports (2021), „Consumer Reports study finds authorized agents can empower people to exercise their digital privacy rights in California“, abrufbar unter: https://advocacy.consumerreports.org/press_release/consumer-reports-study-finds-authorized-agents-can-empower-people-to-exercise-their-digital-privacy-rights-in-california/

Datenethikkommission (2019), „Gutachten der Datenethikkommission“

Deutsche Bundesbank, „Forschungsdaten- und Servicezentrum (FDSZ)“, abrufbar unter: https://www.bundesbank.de/de/bundesbank/forschung/fdsz/forschungsdaten-und-servicezentrum-fdsz--604430

Deutscher Bundestag (2021), „Beschlussempfehlung und Bericht des Ausschusses für Wirtschaft und Energie zu dem Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien“, Drucksache 19/29839, abrufbar unter: https://dip21.bundestag.de/dip21/btd/19/298/1929839.pdf

Dohmen, Schmelz (2021), „Datenschutz in der (Corona-)Krise: Selbstbestimmung und Vertrauen im Fokus – Policy Paper“, abrufbar unter: https://www.progressives-zentrum.org/wp-content/uploads/2021/05/Datenschutz-in-der-Corona-Krise_Policy-Paper-05_Dohmen-Schmelz.pdf

Europäische Kommission (2018), Case M.8744 -DAIMLER / BMW / CAR SHARING JV, 7. November

Europäische Kommission (2020a), „Appendix to the Communication ‚A European strategy for data‘“, abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

Europäische Kommission (2020b), „Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance Gesetz)“

Europäische Kommission (2020c), „Circular economy action plan“, abrufbar unter: https://ec.europa.eu/environment/strategy/circular-economy-action-plan_en

Europäische Kommission (2020d), Case AT.40462 Amazon Marketplace

Europäische Kommission (2020e), „Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)“

Europäische Kommission (2021), „Proposal for a Regulation laying down harmonised rules on artificial intelligence“, abrufbar unter: https://ec.europa.eu/newsroom/dae/redirection/document/75788

Forbrukerrådet (2018), „Deceived by Design“, abrufbar unter: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

Gesamtverband der deutschen Versicherungswirtschaft (2018), „Datenkranz beim automatisierten Fahren gemäß § 63a StVG – externe Speicherung bei einem Datentreuhänder“, Positionspapier, August

Graef, Jeon, Rieder, van Hoboken, Husovec (2021), „Work stream on Differentiated treatment“, Final report.

Graf von Bernstorff (2011), „Einführung in das englische Recht“, 4. Aufl.

Health Data Research UK (2021), „Improving UK Health Data: Impact from Health Data Research Hubs“, abrufbar unter: https://www.hdruk.ac.uk/wp-content/uploads/2021/04/Improving-UK-Health-Data-Impacts-from-Health-Data-Research-Hubs_compressed.pdf

Health Data Research UK, „Our Hubs“, abrufbar unter: https://www.hdruk.ac.uk/helping-with-health-data/our-hubs-across-the-uk/

Hentschel (2021), „DLD-Konferenz: Interview mit Stefan Vilsmeier – Daten in der Medizin: „Krankheiten lassen sich viel früher erkennen“, abrufbar unter: https://www.focus.de/digital/dldaily/dld-konferenz-interview-mit-stefan-vilsmeier-daten-in-der-medizin-krankheiten-lassen-sich-viel-frueher-erkennen_id_13012769.html?__blob=publicationFile&v=1h

Hurtz (2019), „50 Millionen Patientendaten landen auf Googles Servern“, abrufbar unter: https://www.sueddeutsche.de/digital/google-project-nightingale-gesundheitsdaten-ascension-1.4681463

Kerber (2018), “Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data“, JIPITEC 9 (3)

Kerber (2021), „DGA – einige Bemerkungen aus ökonomischer Sicht“, abrufbar unter: https://www.uni-marburg.de/de/fb02/professuren/vwl/wipol/pdf-dateien/kerber_dga_einige-bemerkungen_21012021.pdf

Lecher (2021), „How Big Pharma Finds Sick Users on Facebook“, abrufbar unter: https://themarkup.org/citizen-browser/2021/05/06/how-big-pharma-finds-sick-users-on-facebook

Marthews, Tucker (2017), „Government Surveillance and Internet Search Behavior“, abrufbar unter https://ssrn.com/abstract=2412564

Martin, Pasquarelli (2019), „Exploring Data TrustCertifications“, Oxford Insights, abrufbar unter: https://theodi.org/wp-content/uploads/2019/04/Report_-Exploring-Data-Trust-Certification.pdf

Medizininformatik-Initiative (2020), „Arbeitsgruppe Consent Mustertext Patienteneinwilligung, abrufbar unter: https://www.medizininformatik-initiative.de/sites/default/files/2020-04/MII_AG-Consent_Einheitlicher-Mustertext_v1.6d.pdf

National Institutes of Health (2021), „NIH launches new initiative to study ‚Long COVID‘“, 23. Februar, https://www.nih.gov/about-nih/who-we-are/nih-director/statements/nih-launches-new-initiative-study-long-covid

Nitschke (2018), „Microsoft stellt seine Cloud-Dienste ab 2019 aus neuen Rechenzentren in Deutschland bereit und reagiert damit auf veränderte Kundenanforderungen“, abrufbar unter: https://news.microsoft.com/de-de/microsoft-cloud-2019-rechenzentren-deutschland/

Rat für Informationsinfrastrukturen (2021), „Workshop-Bericht der AG Datentreuhänderschaft – Datentreuhänder: Potenziale, Erwartungen, Umsetzung“

Schwartmann, Hanloser, Weiß (2021), „PIMS im TTDSG – Vorschlag zur Regelung von Diensten zur Einwilligungsverwaltung im Telekommunikation-Telemedien-Datenschutzgesetz“, März

SPD (2021): „Das Zukunftsprogramm der SPD“, abrufbar unter: https://www.spd.de/fileadmin/Dokumente/Beschluesse/Programm/SPD-Zukunftsprogramm.pdf, S. 15

Specht, Kerber (2017), „Datenrechte – eine rechts- und sozialwissenschaftliche Analyse im Vergleich Deutschland – USA“, Abida-Gutachten, abrufbar unter: https://www.abida.de/sites/default/files/ABIDA_Gutachten_Datenrechte.pdf.

Specht-Riemenschneider, Blankertz, Sierek, Schneider, Henne (2021), „Datentreuhand: Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierungserfordernisse für Datentreuhandmodelle“, Beilage in MMR, Juni

Stiftung Datenschutz (2017), „Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen“, abrufbar unter: https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/PIMS-Abschluss-Studie-30032017/stiftungdatenschutz_PolicyPaper_Neue_Wege_zur_Einwilligung_DE_EN_final.pdf

Vengattil, Humer (2020), „Alphabet's Verily targets employer health insurance with Swiss Re partnership“, abrufbar unter: https://www.reuters.com/article/us-alphabet-verily-idUKKBN25L1Q9

vzbv (2020), „Personal Information Management Systems (PIMS): Chancen, Risiken und Anforderungen“, Februar

Wendehorst, Schwamberger, Grinzinger (2020), „Datentreuhand –wie hilfreich sind sachenrechtliche Konzepte?“, in Pertot (Hrsg), Rechte an Daten

Wiseman, Sanderson (2017), „The legal dimensions of digital agriculture in Australia: An examination of the current and future state of data rules dealing with ownership, access, privacy and trust“, abrufbar unter: https://www.crdc.com.au/sites/default/files/CRD18001-001%20CRDC%20P2D%20Report%20low%20res.pdf

Wolfert, Ge, Verdouw, Bogaardt (2017), „Big Data in Smart Farming – A review“, Agricultural Systems, Volume 153, Seite 69-80, abrufbar unter: https://www.sciencedirect.com/science/article/pii/S0308521X16303754

Zscheischler et al. (2021), „Kapitel 4 Landwirtschaft, Digitalisierung und digitale Daten“ in DiDaT Weißbuch, abrufbar unter: https://www.researchgate.net/publication/349557077_Kapitel_4_Landwirtschaft_Digitalisierung_und_digitale_Daten

Internet-Links (alle zuletzt abgerufen am 01.06.2021)

https://edps.europa.eu/data-protection/our-work/subjects/systeme-de-gestion-des-informations-personnelles_de

https://excessmaterialsexchange.com/en_us/

https://polypoly.org/en-gb/

https://siemens.mindsphere.io

https://transplantations-register.de/forschung

https://www.apheris.com

https://www.bbc.com/news/business-42877287

https://www.bitsabout.me

https://www.brainlab.com

https://www.datavaults.eu/

https://www.digi.me

https://enid.foundation/

https://www.gs1.org/about

https://www.home-connect-plus.com/de/app/

https://www.itsmydata.de

https://mediaire.de/

https://www.polypoly.eu

https://www.smart-reporting.com/en/company/about

https://www.tonysopenchain.com/

Danksagung

Vielen Dank an die vielen Expert:innen aus Unternehmen, Universitäten und Forschungseinrichtungen, Regulierungsbehörden und Ministerien, die ihre Erkenntnisse mit uns geteilt haben. Dazu gehören insbesondere Luis Hopf, Brainlab, Wolfgang Kerber, Universität Marburg, Walter Pasquarelli, Open Data Institute, Alexander Radbruch, Universitätsklinikum Bonn, Stephan Ramesohl, Wuppertal-Institut, Ingrid Schneider, Universität Hamburg, sowie unsere Kolleg:innen, vor allem Theresa Henne und Julian Jaursch (SNV) wie auch Jakob Knapp, Ruben Schneider (Universität Bonn) und Pascal Sierek (Osborne Clarke). Die Ansichten in diesem Papier spiegeln nicht notwendigerweise die der Fachleute wider, und alle verbleibenden Fehler sind unsere eigenen.

Über die Stiftung Neue Verantwortung

Die Stiftung Neue Verantwortung (SNV) ist ein gemeinnütziger Think Tank, der an der Schnittstelle von Technologie und Gesellschaft arbeitet. Die Kernmethode der SNV ist die kollaborative Entwicklung von Politikvorschlägen und -analysen. Die Expert:innen der SNV arbeiten nicht allein, sondern entwickeln und testen Ideen gemeinsam mit Vertreter:innen aus Politik und Verwaltung, Technologieunternehmen, Zivilgesellschaft und Wissenschaft. Unsere Expert:innen arbeiten unabhängig von Interessengruppen und Parteien. Unsere Unabhängigkeit gewährleisten wir durch eine Mischfinanzierung, zu der viele verschiedene Stiftungen, öffentliche Mittel und Unternehmensspenden beitragen.

Über den Autorinnen

Aline Blankertz leitet das Projekt „Datenökonomie“, das ökonomische, technische und gesellschaftliche Fragestellungen untersucht, um innovative datenpolitische Handlungsempfehlungen zu entwickeln. Vor der Stiftung Neue Verantwortung leitete sie verschiedene wirtschaftswissenschaftliche Analysen zur Plattformökonomie, darunter zu Wettbewerb, Datenschutz und Algorithmen.

Prof. Dr. Louisa Specht ist Inhaberin des Lehrstuhls für Bürgerliches Recht, Informations- und Datenrecht an der Universität Bonn, Leiterin der Forschungsstelle für Rechtsfragen neuer Technologien sowie Datenrecht (ForTech) und stellvertretende Vorsitzende des Sachverständigenrates für Verbraucherfragen am Bundesministerium der Justiz und für Verbraucherschutz.

So erreichen Sie die Autorinnen:

Aline Blankertz
Projektleiterin Datenökonomie
ablankertz@stiftung-nv.de
+49 (0)30 40 36 76 98 1

Louisa Specht
sekretariat.specht@jura.uni-bonn.de
@louisa_specht
+49 (0)228 73 42 40

Impressum

Stiftung Neue Verantwortung e.V.
Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Jan Klöthe