DATENTREUHÄNDERSCHAFT
STATUS QUO UND ENTWICKLUNGSPERSPEKTIVEN

Kurzstudie im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz von der Begleitforschung zum Technologieprogramm „Smarte Datenwirtschaft"

Smarte Datenwirtschaft

IMPRESSUM

Die Kurzstudie wurde im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz im Rahmen der Begleitforschung zum Technologieprogramm „Smarte Datenwirtschaft“ erstellt.

AUTOREN

Maximilian Lindner,
Sebastian Straub

HERAUSGEBER

Peter Gabriel
Begleitforschung Smarte Datenwirtschaft
Institut für Innovation und Technik (iit)
in der VDI / VDE Innovation + Technik GmbH
Steinplatz 1
10623 Berlin
gabriel@iit-berlin.de

VERÖFFENTLICHUNG

Februar 2023

GESTALTUNG

LHLK Agentur für Kommunikation GmbH
Hauptstraße 28
10827 Berlin

BILDER

vit_mar, Inna – stock.adobe.com (Titel)

EXECUTIVE SUMMARY

Das Konzept des Datentreuhänders hat in den letzten Jahren deutlich an Gewicht gewonnen. Sein Versprechen ist es, die Bedingungen für das Data-Sharing in der Datenwirtschaft deutlich zu vereinfachen. Datentreuhänder sollen als Vertrauensinstanz zwischen den Akteuren vermitteln, für einen fairen Ausgleich der widerstreitenden Interessen sorgen und damit Impulse für die Datenwirtschaft insgesamt geben. Allerdings ist oft noch unklar, wie derartige Datentreuhandmodelle organisatorisch, rechtlich und technisch ausgestaltet sein sollten. Die vorliegende Studie widmet sich daher den grundlegenden Rahmenbedingungen von Datentreuhändermodellen und beleuchtet die bestehenden und aktuell diskutierten Ansätze, auch unter Darstellung von Praxisbeispielen. Hierdurch soll dem Leser oder der Leserin ein Überblick zum Status quo der Datentreuhänderschaft und den damit verbundenen Potenzialen, Herausforderungen und Perspektiven verdeutlicht werden. Die Studie beruht auf einer Literaturanalyse und Interviews mit ausgewählten Expertinnen und Experten aus Politik, Wissenschaft und Wirtschaft. Sie wurde im Rahmen der Begleitforschung zum Technologieprogramm „Smarte Datenwirtschaft“ (SDW) des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) erstellt.

Der Begriff „Datentreuhänder“. Der Begriff des Datentreuhänders ist noch unscharf und wird heute auf zwei Arten und Weisen verstanden: In einem engeren Verständnis sind damit tatsächlich, angelehnt an den angelsächsischen Rechtsbegriff des Trustees, die treuhänderische Verwaltung und die neutrale Mittlung von Daten gemeint. In einer weiteren Definition ist mit dem Treuhänder eher eine Instanz gemeint, die Vertrauen für Datengebende und Datennehmende schafft und bei Konfliktfällen schlichtet. In der noch überschaubaren Praxis der Datentreuhand-Plattformen sind beide Konzepte anzutreffen.

Nutzen und Hemmnisse. Gleich wie man den Datentreuhänder versteht, liegen seine ökonomischen Vorteile vor allem darin, dass Vertrauen in den Umgang mit sensiblen Unternehmens- oder Personendaten geschaffen, qualitativ hochwertige Datenangebote bereitgestellt und damit insgesamt die Transaktionskosten des Data-Sharing gesenkt werden. Gesellschaftlicher Nutzen sind eine gesteigerte Datensouveränität der bzw. des Einzelnen, etwa im Umgang mit ihren bzw. seinen Gesundheitsdaten, der bessere Zugang zu Daten für kleine und mittlere Unternehmen sowie eine bessere Datengrundlage für Forschung und staatliches Handeln. Die Hindernisse sind zum Teil deckungsgleich mit denen des Data-Sharing: geringe Bereitschaft zum Datenteilen und fehlendes Know-how bei den Unternehmen und die Angst vor Überteilung in den Plattformen. Dazu kommen die noch oft unklaren Vorstellungen zu Geschäfts- und Betriebsmodellen der Datentreuhänder.

Data Governance Act. Große Bedeutung für das neue Konzept hat der ab September 2023 geltende Data Governance Act der EU, der einen harmonisierten Rahmen für den Datenaustausch in den Mitgliedsstaaten schaffen soll. Mit seinen Vorgaben an Neutralität und Zweckbindung der Plattform behindert der Data Governance Act unter Umständen ergänzende Service-Angebote der Treuhänder, die deren Geschäftsmodell erst tragfähig machen. Hier muss die Entwicklung der Rechtspraxis abgewartet werden.

Konzeption. Für die organisatorische, betriebswirtschaftliche und technische Umsetzung eines Datentreuhandangebots gibt es bereits umfangreiche konzeptionelle Vorarbeiten. Zu Beginn steht eine genaue Analyse der Anforderungen aller zukünftigen Akteure und ihrer potenziellen Nutzerinnen und Nutzer. Über eine Governance-Struktur muss dann das notwendige Vertrauen zwischen den Beteiligten hergestellt werden. Ein tatsächlicher Anreiz, sich an der Plattform zu beteiligen, wird dann über mit allen Beteiligten abgestimmte Nutzungsszenarien erreicht, in denen der konkrete Mehrwert für Datengebende und Datennehmende deutlich wird. Hier sollte eher Wert auf ein organisches Wachstum gelegt werden, um genügend Zeit für den Vertrauensaufbau zu lassen. Bei der betriebswirtschaftlichen Konzeption des Angebots gibt es eine breite Palette an Preismodellen – von Transaktionsgebühren über Pay-per-Use-Modelle bis hin zu Mitgliederbeiträgen. Während private Treuhänder mehr Agilität versprechen, schaffen öffentliche Betreiber leichter einen Vertrauensvorschuss. Auch genossenschaftliche Modelle sind denkbar. Noch die geringste Herausforderung ist die technische Umsetzung. Für die Wahrung von Datensouveränität, die Herstellung von Interoperabilität und die Umsetzung der eigentlichen Datenwertschöpfung stehen Technologien, Standards und Normen in breitem Umfang bereit. Eine Vorreiterrolle nehmen hier die Architektur und die technischen Standards der International Data Spaces Association ein.

Praxis. Die praktische Umsetzung steht aber noch hinter der Theorie zurück. Derzeit sind acht Datentreuhänder tatsächlich schon in Deutschland operativ tätig, darunter sowohl Plattformen mit einem engen Verständnis der Datentreuhänderschaft als auch solche mit einer weiteren Interpretation. Deutlich ist der starke Branchenbezug der meisten Plattformen. Weitere Plattformen und Projekte befinden sich noch in der Konzeption oder im Aufbau. Abgedeckt werden von den heutigen und den noch kommenden Plattformen die Branchen Gesundheit, Luftfahrt, produzierendes Gewerbe, Logistik, Automobilindustrie und Mobilität.

INHALT

Executive Summary 3

1 Einleitung 7

2 Grundlegende Merkmale eines Datentreuhänders 11
2.1 Enge versus weite Definition 12
2.1.1 Enges Verständnis: Treuhänderische Verwaltung und neutrale Mittlung von Daten 12
2.1.2 Weites Verständnis: Vertrauens- und Schlichtungsinstanz 12
2.2 Vertrauensfördernde Funktionen von Datentreuhändern 14

3 Potenziale und Herausforderungen 19
3.1 Potenziale des Datenteilens 19
3.2 Ökonomische Potenziale der Datentreuhand 20
3.3 Gesellschaftliche Potenziale der Datentreuhand 22
3.4 Herausforderungen für die Etablierung von Datentreuhändern 23

4 Rechtliche Rahmenbedingungen 27
4.1 Herleitung des Treuhandbegriffs und dessen Übertragbarkeit auf Datentreuhänder 27
4.2 Der Data Governance Act 28
4.3 Die möglichen Auswirkungen des Data Governance Act auf die Entwicklung von Datentreuhandmodellen 30
4.4 Weitere Regelungsbereiche 31
4.4.1 Datenschutzrecht 31
4.4.2 Urheberrecht 32
4.4.3 Geschäftsgeheimnisschutz 33
4.5 Aktuelle Diskussionen zur Weiterentwicklung des regulatorischen Rahmens 33

5 Umsetzungskonzepte 35
5.1 Anspruchsgruppenanalyse 36
5.2 Governance 36
5.3 Anreizsysteme 38
5.4 Geschäfts- und Betriebsmodelle 39
5.4.1 Finanzierung und Preismodell 39
5.4.2 Private Trägerschaft 41
5.4.3 Staatliche Trägerschaft 41
5.4.4 Sonderform Datengenossenschaft 42
5.5 Technik und Standards 44
5.5.1 Datensouveränität 45
5.5.2 Dateninteroperabilität 49
5.5.3 Datenwertschöpfung 52

6 Erste Beispiele aus der Praxis 54
6.1 Caruso Dataplace 55
6.2 CSDR 56
6.3 Data Intelligence Hub 57
6.4 Hilo MRM – Maritime Risk Management 58
6.5 Otonomo 58
6.6 SPOCC 59
6.7 Vivli 60
6.8 VTH eData-Pool 61

7 Ein Zwischenfazit zum Status quo 63

8 Literaturverzeichnis 66

Anhang 73
In Deutschland tätige Datentreuhänder-Projekte 73

01

1 EINLEITUNG

Daten sind neben Know-how und Technik einer der zentralen Innovationstreiber innerhalb der digitalen Gesellschaft und stellen in vielen Wertschöpfungsketten eine wesentliche Ressource dar. Je nach Anwendungsbereich bilden digitale Informationen, die etwa beim Betrieb von Produktionsmaschinen oder im Online-Handel entstehen, die Grundlage für das Angebot neuer Produkte und Dienstleistungen. Häufig dienen sie auch der Entwicklung selbstlernender Systeme und künstlicher Intelligenz. In vielen Wirtschaftszweigen kann die Sammlung und Auswertung von Daten zu Produktivitätssteigerungen, zu einem effizienteren Ressourceneinsatz oder zu einer stärker evidenzbasierten Entscheidungsfindung innerhalb der Unternehmensorganisation beitragen. Dementsprechend ist es nicht verwunderlich, dass die Zahl der datennutzenden Unternehmen gemäß den Ergebnissen des European Data Market Monitoring Tool zuletzt erkennbar gestiegen ist (Cattaneo et al. 2020). Die Erzeugung eines ökonomischen Mehrwerts kommt regelmäßig insbesondere dann zustande, wenn Daten aus unterschiedlichen Quellen ausgetauscht, aggregiert und ausgewertet werden, da die unternehmensintern verfügbare Datenmenge nicht ausreicht oder qualitativ unzureichend ist. Dies gilt insbesondere bei der Lösung domänenübergreifender Problemstellungen, die die Nutzbarkeit verschiedenster Datensätze erfordern (Element AI und nesta 2019). So erweist sich der unternehmensübergreifende Austausch von Daten als Schlüsselfaktor für die Entwicklung innovativer Geschäftsmodelle (Otto und Österle 2016).

Die Mehrwerte der – im Idealfall organisationsübergreifenden – Datennutzung werden auch in der wirtschaftlichen Praxis immer häufiger erkannt (ZVEI 2022). Dennoch zeigen unterschiedliche aktuelle Erhebungen und Analysen, dass Unternehmen entweder technische Voraussetzungen für die Bereitstellung und Nutzung von Datenbeständen außerhalb der eigenen Organisation fehlen oder es an der Bereitschaft für das Teilen eigener Datenbestände mangelt. Hier hemmen vor allem die Angst vor Abfluss von originärem Know-how aus der eigenen Organisation sowie die damit verbundene Gefahr der Übervorteilung durch den Wettbewerb und die Furcht vor dem unberechtigten Zugriff Dritter die organisationsübergreifende Verfügbarkeit von Daten (Azkan et al. 2022; Röhl und Bolwin 2021; Demary et al. 2019). Aber auch rechtliche Unsicherheiten im Umgang mit der Weitergabe personenbezogener Daten und den damit einhergehenden aber oftmals unklaren Anforderungen an Einwilligung oder deren Anonymisierung spielen eine zentrale Rolle als Hindernis auf dem Weg zu florierenden Datenökosystemen (Schneider 2022).

Trotz erkennbarer guter Ansätze zum Aufbau von plattformbasierten Datenökosystemen in Wirtschaft und Forschung (ZVEI 2022) (Lindner et al. 2021) fehlt oftmals noch das Vertrauen der relevanten Teilnehmenden des Ökosystems und so wird die organisationsübergreifende Bereitstellung von Daten als zentrale Ressource für Wirtschaft und Forschung verhindert. Ein Grund dafür ist laut Alex Pentland, Direktor des Connection Science Lab des MIT, dass es zwar Banken zur Abwicklung von Zahlungsströmen gebe, aber keine vergleichbare Transaktionsinfrastruktur für Daten vorhanden sei. Aus seiner Perspektive könnten und sollten Datentreuhänder (data trustees) oder Datengenossenschaften (data cooperatives) diese Lücke füllen und die ihnen zur Verfügung gestellten Daten als Dienstleistung verwalten (Weirens et al. 2021).

Das Konzept der Datentreuhänderschaft hat, insbesondere im Kontext der Bereitstellung personenbezogener Daten für Forschungszwecke, einen regelrechten Hype erfahren: Ausgehend von rechtswissenschaftlichen Fachdiskussionen und der Verankerung der zugrunde liegenden Idee in verschiedenen Datenschutzkonzepten der Verbundforschung, attestiert etwa die Datenethikkommission der Bundesregierung Datentreuhändern in ihrem Gutachten aus dem Jahr 2019

eine hohe praktische Relevanz für die Etablierung funktionierender Datenökosysteme (Buchner et al. 2021). Aufbauend auf den Ratschlägen der Datenethikkommission wurde die stärkere Förderung von Datentreuhandmodellen in die Datenstrategie der vorhergehenden Bundesregierung aufgenommen und dies ist auch ein erklärtes Ziel im Koalitionsvertrag der im Jahr 2021 neu gewählten Bundesregierung aus SPD, FDP und Bündnis 90/Die Grünen (Mehr Fortschritt wagen 2021). Zugleich wurde auf europäischer Ebene mit dem Data Governance Act ein Rechtsrahmen für Datenvermittlungsdienste geschaffen. Die EU will damit den vertrauenswürdigen Austausch von Daten fördern und neue Impulse für die Datenwirtschaft setzen. Trotz des deutlich erkennbaren politischen Willens, Datentreuhänder zu etablieren, wird das zugrunde liegende Konzept in der aktuellen Diskussion bei genauerer Betrachtung oft noch sehr unkonkret behandelt und der Begriff des Datentreuhänders wird zwar inflationär, aber oft ohne klaren inhaltlichen Fokus verwendet.

An dieser Stelle setzt die vorliegende Studie an und analysiert das noch „unbekannte Wesen" Datentreuhänder (Hottelet 2021; Richter 2021a). Der Analyse liegen folgende Fragestellungen zugrunde:

- Welches Verständnis des Datentreuhänderbegriffs kristallisiert sich in der aktuellen Debatte heraus und welche Funktionen können Datentreuhänder wahrnehmen?
- Welche rechtlichen Rahmenbedingungen bestehen national und auf europäischer Ebene und welche organisatorischen Konzepte und technischen Lösungsansätze sind erkennbar?
- Gibt es in Deutschland bereits operativ tätige Datentreuhänder im unternehmerischen Kontext?
- Gibt es schon erste Erkenntnisse aus der laufenden Diskussion und den ersten Pilotbetrieben zu Aufbau und Betrieb von Datentreuhändern?

In einem ersten Schritt nähert sich die Studie entsprechend analytisch dem Begriff Datentreuhänder, stellt in der Praxis erkennbare Unterschiede in der Verwendung des Begriffs heraus und beschreibt die daraus resultierenden Folgen für den möglichen Funktionsumfang operativ tätiger Datentreuhänder. Anschließend erfolgt eine Analyse der Potenziale, die mit dem Konzept der Datentreuhänderschaft im Hinblick auf die Wirtschaft, die Gesellschaft und den Staat verbunden werden. Darüber hinaus werden aktuell erkennbare Herausforderungen näher beleuchtet, die der nachhaltigen Etablierung von Datentreuhändern derzeit noch entgegenstehen. Anschließend werden die rechtlichen Rahmenbedingungen beschrieben, die bei der Entwicklung und dem Betrieb von Datentreuhändern in der Praxis zu beachten sind. Auf Basis der ersten Praxisbeispiele und der Interviews werden zudem die organisatorischen, betriebswirtschaftlichen und technischen Konzepte zur Ausgestaltung von Datentreuhändern im Realbetrieb diskutiert. Zuletzt werden ausgewählte Praxisbeispiele von in Deutschland operativ tätigen Datentreuhändern dargestellt, ehe die Studie mit einem Zwischenfazit zum Status quo des Datentreuhandkonzepts abschließt. Im Anhang findet sich eine Übersicht zu Datentreuhand-Projekten und -Plattformen, darunter auch solche, die sich noch in der Konzeption, der Entwicklung, der Pilotierung oder im frühen Regelbetrieb befinden.[1]

1 Personal Information Management Systems (PIMS) werden von dieser Studie nicht adressiert, da es bei ihnen nicht um das gleichbe-rechtigte Teilen von Daten zwischen Akteuren geht, sondern um die Ausübung von Datenschutzrechten für Privatpersonen. Datentreu-händer können aber auch einen erheblichen Beitrag für funktionierende und faire Datenökosysteme leisten (Blankertz 2022).

Die Basis für die vorliegende Studie bildet die Sammlung und Auswertung einschlägiger Veröffentlichungen mit den Schwerpunkten wissenschaftlicher Studien, ohne dabei graue Literatur aus dem politisch-gesellschaftlichen Diskurs auszuschließen. Darüber hinaus wurden die öffentlich verfügbaren Informationen von zumindest bereits operativ tätigen Datentreuhändern ausgewertet. Um die Ergebnisse der Dokumentenanalyse zu validieren und weiteren Input für die Studie zu generieren, wurden darüber hinaus mit 14 Expertinnen und Experten leitfadengestützte Interviews zum Thema Datentreuhänderschaft geführt und die Antworten mittels Methoden der qualitativen Inhaltsanalyse ausgewertet. Knapp die Hälfte der befragten Expertinnen und Experten sind dabei aufgrund ihrer Verortung in Wissenschaft, Verbänden oder der Europäischen Kommission eher auf der Makroebene des Diskurses zu verorten, während die andere Hälfte einen stärkeren Praxisbezug auf der operativen Ebene repräsentiert.

Die Autoren bedanken sich herzlich bei den Expertinnen und Experten für die Teilnahme an den Interviews:

- **Dr. Can Azkan**, Wissenschaftlicher Mitarbeiter, Fraunhofer-Institut für Software- und Systemtechnik ISST
- **Dr. Malte Beyer-Katzenberger**, Teamleiter Datenpolitik und Dateninnovation, Europäische Kommission – DG CNECT
- **Aline Blankertz**, Referentin Politik, Wikimedia Deutschland e. V.
- **Dr. Sicco Lehmann-Brauns**, Senior Director Innovation Policy, Siemens AG
- **Denis Feth**, Expert Security and Privacy Technologies, Fraunhofer-Institut für Experimentelles Software Engineering – IESE
- **Prof. Dr. Mathias Fischer**, Professor für Rechennetze, Universität Hamburg
- **Prof. Dr. Andreas Harth**, Lehrstuhl für Wirtschaftsinformatik, insb. Technische Informationssysteme, Friedrich-Alexander-Universität Erlangen-Nürnberg
- **Rosemarie Hinsch**, Senior Sales Manager Trusted Data Solutions, Bundesdruckerei GmbH
- **Dipl.-Ing. Frank Heinze**, Projektleiter „S3I-X – Trusted Data Exchange and Analytics", RIF Institut für Forschung und Transfer e. V.
- **Prof. Dr. Wolfgang Kerber**, Universität Marburg, Fachbereich Wirtschaftswissenschaften
- **Jonathan Mencke**, Projekt „EuroDat – The European Data Trustee", Hessisches Ministerium für Wirtschaft, Energie, Verkehr und Wohnen
- **Dr. Judith Puttkammer**, Senior Strategic Project Manager – Mobility Data Space, acatech – Deutsche Akademie der Technikwissenschaften
- **Bernd Rauch**, Department Head Architecture-Centric Engineering (ACE), Fraunhofer-Institut für Experimentelles Software Engineering - IESE
- **Juliane Schneider**, Wissenschaftliche Mitarbeiterin, Fraunhofer-Institut für Windenergiesysteme IWES
- **Julia Walgern**, Gruppenleiterin Technische Zuverlässigkeit, Fraunhofer-Institut für Windenergiesysteme IWES
- **Prof. Dr. Beatrix Weber**, MLE, Leiterin Forschungsgruppe Recht in Nachhaltigkeit, Compliance und IT, Institut für Informationssysteme, Hochschule Hof

Die Verantwortung für den Inhalt dieser Studie liegt ausschließlich bei den Autoren.

Die Studie wurde im Rahmen der Begleitforschung zum Technologieprogramm „Smarte Datenwirtschaft" (SDW) des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) erstellt. Im Programm arbeiten 21 Projekte an der Erprobung innovativer Digitaltechnologien für die Datenwirtschaft (www.smarte-datenwirtschaft.de).

02

2 GRUNDLEGENDE MERKMALE EINES DATENTREUHÄNDERS

Trotz des häufigen Gebrauchs des Begriffs Datentreuhänder in der öffentlichen Debatte, aber auch im akademischen Diskurs gestaltet sich die Suche nach einer prägnanten und allgemein akzeptierten Definition noch schwierig (Schwartmann 2020; Hottelet 2021; Richter 2021a). Vielmehr handelt es sich bei Datentreuhändern um „schillernde Wesen", in die viele Hoffnungen zum Aufbau florierender und gleichzeitig fairer Datenökosysteme gesetzt werden – ohne dass oftmals eine Abgrenzung zu anderen Modellen des Datenaustauschs erfolgt (Kühling und Buchner 2021). Die Forderung nach der Etablierung von Datentreuhändern als wichtige Voraussetzung für florierende Datenökosysteme ist dabei nicht neu: Bereits in den Debatten um die Realisierung von populations- und krankheitsspezifischen Biodatenbanken zu Beginn der frühen 2000er-Jahre sind entsprechende Konzepte zum Schutz der hochsensiblen Gesundheitsdaten von Patientinnen und Patienten erkennbar (Schneider 2022). Aufbauend auf dieser Tradition ist das Konzept des Datentreuhänders vor allem in der Diskussion um personenbezogene Daten und deren Schutz sehr präsent. Jedoch wird der Einsatz von Datentreuhändern auch zunehmend im Kontext der Nutzbarmachung von Daten über Unternehmens- und Organisationsgrenzen hinweg diskutiert.

Unabhängig davon, ob es sich um Daten von Einzelpersonen oder von Unternehmen handelt, können Datentreuhänder als Intermediäre zwischen Datengebenden (in manchen Kontexten auch als Datenproduzenten oder Datensubjekte bezeichnet) und Datennutzenden charakterisiert werden. Damit kann ein Datentreuhänder im ökonomischen Sinn als Plattform verstanden werden, über die die Daten der beiden genannten Gruppen verfügbar gemacht werden. Entsprechend spielt die Realisierung von Netzwerk- und Skaleneffekten eine herausragende Bedeutung für die erfolgreiche Etablierung von florierenden Datenökosystemen mittels eines Datentreuhänders. Gleichzeitig bestehen damit aber auch Risiken einer ungewollten Machtkonzentration und eines Prinzipal-Agenten-Konflikts zwischen Datentreuhänder und Datengebenden (Blankertz et al. 2020).

Im Hinblick auf die weitere rechtliche Ausgestaltung von Datentreuhänderschaft sind hier grundsätzlich freiwillige (fakultative) und verpflichtende (obligatorische) Datentreuhandmodelle in unterschiedlichen Anwendungsfällen denkbar. Die Nutzung fakultativer Datentreuhänder beruht dabei auf der freiwilligen Entscheidung der beteiligten Akteure. Obligatorische Datentreuhandverhältnisse basieren dagegen auf einer gesetzlichen Verpflichtung zur Bereitstellung der eigenen Daten mittels eines Treuhänders für einen normativ spezifizierten Kreis von Akteuren, sollten aber aufgrund des starken regulatorischen Eingriffs in die Privatautonomie bzw. der Geschäftsgeheimnisse von Unternehmen nur in geeigneten Ausnahmefällen eingesetzt werden. Zwar sind jenseits des Bereichs digitaler Datenbestände ähnliche rechtliche Verpflichtungen zur Nutzung von Treuhändern, beispielsweise etwa für Kapitalverwertungsgesellschaften, erkennbar (Specht-Riemenschneider et al. 2021). Im Kontext digitaler Datenbestände sind jedoch bisher keine solchen Verpflichtungen zur Bereitstellung von Daten durch Einzelpersonen oder Unternehmen erkennbar. Entsprechend steht die freiwillige Nutzung von Datentreuhandmodellen im Fokus der vorliegenden Studie.

Die einschlägigen rechtlichen Grundlagen sowie Möglichkeiten der technischen und organisatorischen Ausgestaltung werden in den Kapiteln 4 und 5 beleuchtet. Zunächst steht jedoch das zugrundeliegende Begriffsverständnis von Datentreuhänderschaft im Fokus des Interesses.

2.1 Enge versus weite Definition

Anhand der Literatur und der Interviews wird deutlich, dass der Begriff Datentreuhänder sowohl in einem engen als auch einem weiteren Verständnis Verwendung findet:

2.1.1 ENGES VERSTÄNDNIS: TREUHÄNDERISCHE VERWALTUNG UND NEUTRALE MITTLUNG VON DATEN

In Anlehnung an eine Bank, die für ihre Kundinnen und Kunden Vermögenswerte hält und verwaltet, verwalten Datentreuhänder gemäß dem engen Begriffsverständnis Daten für die Datengebenden in einem treuhänderischen Verhältnis. Als unabhängige dritte Partei validieren, kontrollieren und sichern sie Datenbestände der Datengebenden, teilen die Daten mit berechtigten Nutzenden im Sinne des Willens der Datengebenden und gewährleisten deren zweckgebundene Verwendung (Weirens et al. 2021).

„Eine Datentreuhand [kann entsprechend als] eine natürliche oder juristische Person oder eine Personengesellschaft [definiert werden], die den Zugang zu von Datentreugebern bereitgestellten oder bereitgehaltenen Daten nach vertraglich vereinbarten oder gesetzlich vorgegebenen Daten-Governance-Regelungen im Fremdinteresse mittelt." (Specht-Riemenschneider et al. 2021).

Dies erfordert eine entsprechende Organisation und Infrastruktur, die zugänglich gemachte Datenbestände der Treugebenden verwaltet und gemäß zuvor mit den Treugebenden festgelegten Nutzungspräferenzen Dritten bei Erfüllung der Zweckbestimmung selbstständig zur Nachnutzung verfügbar macht und dabei die Einhaltung der zuvor damit einhergehenden Nutzungsbedingungen kontrolliert. Das wird als Datenmittlung oder kurz Mittlung bezeichnet.

Das britische Open Data Institut formuliert hierzu prägnant, dass es sich bei Datentreuhändern um eine rechtlich eigenständige Entität handelt, die für Daten eine unabhängige treuhänderische Verwaltung (fiduciary stewardship) realisiert (Hardinges 2020). Entsprechend sind in diesem Begriffsverständnis die besonderen treuhänderischen Pflichten zu Transparenz, Umsicht und ungeteilter Loyalität des Datentreuhänders gegenüber den Datengebenden von höchster Bedeutung (Schneider 2022). Dabei sollte dem Datentreuhänder nach Ansicht mehrerer Interviewpartner eine vertraglich eingehegte Verfügungsmacht über die Datenweitergabe eingeräumt werden. Deshalb ist es wichtig, dass der Datentreuhänder eine neutrale Stellung innerhalb des Ökosystems einnimmt und keine Eigeninteressen an der Verwendung entwickelt. Durch die Abgabe von Entscheidungskompetenz durch die Datengebenden ist für die Umsetzung derartiger Datentreuhandmodelle ein besonders hohes Maß an Vertrauen der beteiligten Akteure, insbesondere der Datengebenden, erforderlich. Gleichzeitig können durch die treuhänderische Verwahrung die beim Austausch von Daten anfallenden Transaktionskosten in besonders hohem Maße reduziert werden, auch wenn im Rahmen der Interviews Zweifel erkennbar waren, ob vor allem Unternehmen tatsächlich flächendeckend dazu bereit sein werden, die Entscheidungskompetenz über die Weitergabe ihrer eigenen Datenbestände einer dritten Partei zu übergeben.

2.1.2 WEITES VERSTÄNDNIS: VERTRAUENS- UND SCHLICHTUNGSINSTANZ

Demgegenüber steht – auch vor dem Hintergrund der sehr voraussetzungsvollen Umsetzung eines Datentreuhänders mit eingehegter Verfügungsmacht im ursprünglichen Verständnis einer treuhänderischen Verwahrung – ein eher weites Verständnis des Begriffs Datentreuhänder. Dabei wird der Datentreuhänder allgemein im Sinne eines Trusted-third-Party-Konzepts als

Vertrauensinstanz verstanden, die als eigenständige Organisation eine Infrastruktur und gegebenenfalls dazugehörige Services anbietet, die einen vertrauenswürdigen Austausch von Daten zwischen Datengebenden und Datennehmenden ermöglichen. Eine treuhänderische Verwahrung und Mittlung der Daten im Sinne einer Fiduciary-Stewardship ist dabei aber nicht vorgesehen, sodass die am Ökosystem teilnehmenden Akteure die finale Entscheidung über die Weitergabe ihrer Daten selbst treffen müssen. Anstatt einer treuhänderischen Verwahrung und regelbasierten Weitergabe der Daten als genuiner Vertrauensmoment stellt der Datentreuhänder in diesem Verständnis klare Regeln für einen vertrauensvollen Datenaustausch bereit, kontrolliert deren Einhaltung und stellt faire Mechanismen zum Ausgleich der Interessen der beteiligten Akteure sowie Streitschlichtungsmechanismen zur Verfügung. Grundsätzlich geht es gemäß dem weiten Begriffsverständnis von Datentreuhänderschaft also darum, Daten für Dritte auf eine vertrauenswürdige und für alle Beteiligten faire Art und Weise zugänglich zu machen. Wie genau Vertrauen zwischen den beteiligten Akteuren und auch gegenüber dem Datentreuhänder geschaffen werden kann, ist dabei nach Ansicht der Interviewpartner stark von den Rahmenbedingungen des jeweiligen Anwendungsbereichs abhängig.

Um jedoch eine Beliebigkeit des Begriffs des Datentreuhänders in seinem weiten Verständnis zu vermeiden, ist darüber hinaus eine Abgrenzung zu reinen Transaktionsinfrastrukturen sinnvoll (Manohar et al. 2020). So konstituiert die bloße Bereitstellung einer technischen Infrastruktur zum bilateralen Austausch von Daten zwischen zwei Parteien – ohne die grundlegende Gewährleistung ihrer Integrität oder Qualität, ohne basale Regeln für das Teilen von Daten innerhalb des entstehenden Ökosystems oder ohne eine vermittelnde Instanz zwischen den Datengebenden und Datennutzenden – auch in diesem weiten Verständnis noch kein Moment von Datentreuhänderschaft. Entsprechend können nach Ansicht der meisten Interviewpartnerinnen bzw. Interviewpartner auch Konstrukte wie Datenmarktplätze als Datentreuhänder im weiteren Sinne verstanden werden, wenn es entsprechende Maßnahmen zur Vertrauensbildung zwischen den beteiligten Akteuren und gegenüber dem Plattformbetreiber sowie Instrumente zur Gewährleistung einer hohen Datenqualität gibt.

Zusammenfassend können Datentreuhänder – sowohl im engen als auch weiten Verständnis – also als eine Untergruppe von Datenvermittlungsdiensten (Richter 2021b) verstanden werden, die mindestens durch Maßnahmen der Vertrauensbildung oder gegebenenfalls Ausübung einer treuhänderischen Verantwortung die Nutzbarkeit von Daten ermöglichen.

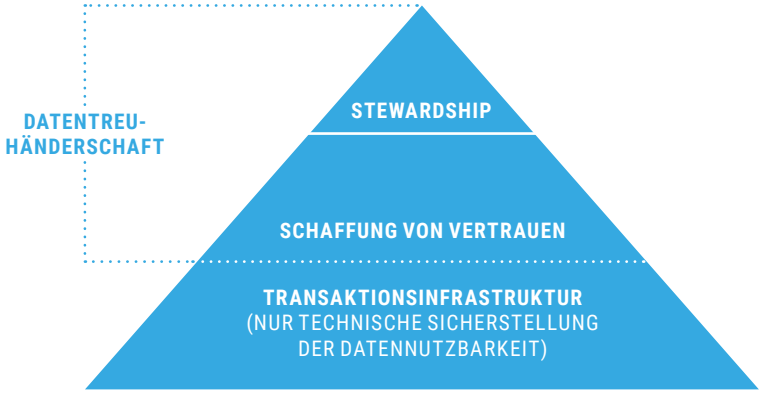

Abbildung 1: Auch wenn der Übergang zwischen reinen Transaktionsinfrastrukturen und Datentreuhändern nicht klar abgrenzbar ist, kann eine Unterscheidung anhand des Grades der aktiven Umsetzung von vertrauensbildenden Maßnahmen durch den Plattformbetreiber als Trusted-Third-Party getroffen werden.

2.2 Vertrauensfördernde Funktionen von Datentreuhändern

Die Schaffung von Vertrauen der beteiligten Akteure innerhalb des zu etablierenden Datenökosystems umfasst unterschiedliche Facetten: So müssen sich die am Ökosystem teilnehmenden Akteure auf die Qualität der bereitgestellten Datenbestände – im Sinne ihrer Aktualität, Genauigkeit sowie Verfügbarkeit in standardisierten Formaten – und deren rechtssichere Nutzbarkeit für dritte Parteien verlassen können. Gleichzeitig spielt laut Interviews das Thema Datensicherheit und deren technische Gewährleistung durch den Datentreuhänder, aber auch durch die Datennutzenden eine zentrale Rolle für vertrauensvollen Datenaustausch. Darüber hinaus wird in den Interviews auch wiederholt auf die Schaffung von Transparenz als vertrauensbildende Maßnahme referenziert – auch wenn hier unterschiedliche Bezüge hergestellt werden: Einerseits soll der Datentreuhänder Transparenz und Nachvollziehbarkeit über die Nutzung der bereitgestellten Datenbestände sicherstellen, während an anderer Stelle verstärkt auf das Erfordernis der transparenten Darstellung der Aktivitäten des Datentreuhänders und dessen Umgang mit den Daten bzw. dessen genaue Rolle im Ökosystem aufgeführt wird. In diesem Kontext ist auch die Neutralität des Datentreuhänders als zentraler Faktor für den Vertrauensaufbau zu nennen. Zuletzt sollte der Datentreuhänder nach Aussage der Interviewpartnerinnen und Interviewpartner im Sinne der Wahrnehmung vertrauensbildender Funktionen den tatsächlichen Mehrwert der Teilnahme der Datengebenden und Datennehmenden am entstehenden Ökosystem dauerhaft gewährleisten und wenn möglich ausbauen. Entsprechend können die Darstellung von funktionierenden Erfolgsbeispielen datengenerierter Mehrwerte innerhalb des mittels Datentreuhänder etablierten Ökosystems und der aktive Ökosystemaufbau Funktionen des Datentreuhänders sein, die vertrauensfördernd sind. Im nachfolgenden Abschnitt werden die einzelnen Funktionen, die Datentreuhändern zugeschrieben werden können, noch einmal im Detail behandelt. Die konkreten technischen und organisatorischen Möglichkeiten der Ausgestaltung eines Datentreuhänders werden dann in Kapitel 5 beschrieben.

Der Datentreuhänder als Bereitsteller einer vertrauenswürdigen Transaktionsinfrastruktur und vertrauensfördernder technischer Instrumente

Die basale Funktion eines Datentreuhänders zur Gewährleistung eines vertrauensvollen Datenaustauschs zwischen einzelnen Akteuren des jeweiligen Datenökosystems ist die Bereitstellung einer vertrauenswürdigen technischen Infrastruktur. Zur Wahrnehmung dieser Kernfunktion kann der Datentreuhänder unterschiedliche Elemente umsetzen, die unter die nachfolgend aufgeführten Unterfunktionen subsumiert werden können (Bundesdruckerei):

- **Instrumente für transparente, souveräne und sichere Datenbereitstellung:** Durch die übersichtliche Darstellung von Datennutzungsanfragen und erteilten Freigaben wissen die Datengebenden zu jedem Zeitpunkt, wer ihre Daten zu welchem Zweck nutzt bzw. nutzen möchte. Darüber hinaus stellt der Datentreuhänder entweder leicht nutzbare Instrumente zur Abbildung der Datenfreigabe oder deren Verweigerung zur Verfügung bzw. schafft die technischen Voraussetzungen für die Ablage konkreter Nutzungsbedingungen für den Fall einer treuhänderischen Verwahrung der Daten im engeren Verständnis eines Datentreuhänders. In jedem Fall muss der Datentreuhänder vor allem aber auch die Informationssicherheit der zugrunde liegenden Infrastruktur gewährleisten.

- **Instrumente für autorisierten Zugang und Nutzungskontrolle:** Eng mit der souveränen Datenbereitstellung verknüpft sind technische Maßnahmen zum Schutz vor unautorisiertem Datenzugriff. Durch die Registrierung neuer Ökosystemteilnehmender und deren Ausstattung mit einer Trusted-Identity soll die Nutzung von Daten für unberechtigte Dritte verhindert werden. Zudem stellt der Datentreuhänder durch geeignete technische Maßnahmen die entsprechend erteilte Freigabe zweckgebundener Nutzung der Daten sicher. Hierzu förderlich sind grundlegende Monitoring- und Logging-Funktionen, die der Datentreuhänder wahrnimmt und technisch ermöglicht (Bundesdruckerei).
- **Instrumente zur Pseudonymisierung und Anonymisierung von Datenbeständen:** Im Zusammenhang mit besonders schützenswerten und vor allem personenbezogenen Datenbeständen kann der Datentreuhänder zudem technische Instrumente zur Anonymisierung und bzw. oder Pseudonymisierung der durch die Datengebenden bereitgestellten Daten anbieten (ZVEI 2022). So soll sichergestellt werden, dass keine Rückschlüsse auf die datengebenden Unternehmen oder Einzelpersonen möglich sind und keine datenschutzrechtlichen Probleme bei der Weiterverwendung der Daten auftreten. Grundsätzlich kann die vertrauensvolle Weitergabe von digital verfügbaren Informationen hier auch ohne die Weiterleitung oder Nutzung der eigentlichen Daten mittels der Generierung von Hash-Werten oder ähnlichen Methoden erfolgen. Dabei spielt nach Aussage der meisten Interviewpartnerinnen und Interviewpartner die Verlässlichkeit der verwendeten Methoden und Instrumente – hierbei insbesondere in Datenökosystemen mit einer kleinen Anzahl von Datengebenden bzw. leicht durch die Hinzunahme weiterer Parameter identifizierbarer Unternehmen oder Einzelpersonen – eine besonders wichtige Rolle beim Vertrauensaufbau.

Der Datentreuhänder als neutraler Vertrauensanker innerhalb des Ökosystems

In Abhängigkeit der Rahmenbedingungen des jeweiligen Anwendungsfalls und der Beschaffenheit des Wettbewerbs zwischen den teilnehmenden Unternehmen und deren kultureller Offenheit gegenüber dem Konzept des Datenteilens spielt die Gewährleistung der Neutralität des Datentreuhänders eine herausragende Rolle (Lindner et al. 2021). Das Verständnis über die Ausgestaltung einer neutralen Stellung des Datentreuhänders in der Praxis divergiert jedoch in der öffentlichen Diskussion und auch in den geführten Interviews stark: Auf der einen Seite des Spektrums steht die Forderung nach einer absoluten Neutralität, in deren Sinne der Datentreuhänder keinerlei Geschäftstätigkeiten mit bereitgestellten Datenbeständen aufnehmen darf. Auf der anderen Seite wird die erforderliche Neutralität des Datentreuhänders auch teilweise als Einhaltung von zuvor festgelegten Regelungen und Vereinbarungen verstanden, die die Weiterverarbeitung und Analyse der bereitgestellten Daten – beispielsweise als Dienstleistung für die Teilnehmenden des Datenökosystems – regelbasiert ermöglichen sollen. Entsprechend soll die Verwirklichung einer neutralen Stellung des jeweils spezifischen Datentreuhänders anwendungsfallbezogen und unter Rückgriff auf die Interessen und Bedürfnisse der Teilnehmenden des Ökosystems erfolgen.[2] Jenseits dieser Frage können jedoch nach Aussage einiger Interviewpartnerinnen und Interviewpartner auch allgemeingültige Maßnahmen identifiziert werden, die einen Datentreuhänder in seiner Funktion als neutraler Vertrauensanker innerhalb des Datenökosystems unterstützen. Zum einen sollte der Datentreuhänder Regeln für die Datenbereitstellung und Datennutzung schaffen, deren Einhaltung kontrollieren und die rechtlich einwandfreie Gestaltung des notwendigen Vertragswerks gewährleisten. Zudem sollte der Zugang zu den verfügbaren Datenbeständen fair – im Sinne eines grundsätzlich offenen, diskriminierungsfreien und regelbasierten Datenaustauschs –

2 Inwieweit dieses Verständnis mit den Regelungen für Datentreuhänder als Vermittlungsdienste gemäß EU Data Governance Act vereinbar sind, wird im Kapitel 4 zu den rechtlichen Rahmenbedingungen behandelt.

gestaltet werden. Um das Vertrauen in die Integrität des Ökosystems hier nicht zu gefährden, wird dem Datentreuhänder dabei aber auch eine gewisse Selektionsfunktion im Hinblick auf die Qualität der angebotenen Daten und die Vertrauenswürdigkeit der Teilnehmenden des Ökosystems zugeschrieben.

Der Datentreuhänder als Data Facilitator

Anknüpfend an die Frage nach der Ausgestaltung der erforderlichen Neutralität eines Datentreuhänders ergeben sich in der Diskussion um die Übernahme von Aufgaben zur Verbesserung der Qualität der bereitgestellten Datenbestände sowie weiterführender datenbasierter Dienstleistungen für alle Teilnehmenden des Ökosystems oder auch nur einzelne Unternehmen, Organisationen und Einzelpersonen unterschiedliche Perspektiven. Wird für die Neutralität eines Datentreuhänders das Fehlen jeglichen Interesses an der Weiterverarbeitung der bereitgestellten Datensätze vorausgesetzt, so sollte nach Auffassung einiger Interviewpartnerinnen und Interviewpartner der Datentreuhänder keine oder nur stark eingeschränkt Aufgaben übernehmen, die eine aktive Datennutzung erfordern. Es gibt aber auch Stimmen, auch unter den Interviewpartnerinnen und Interviewpartnern, die Datentreuhändern eine aktivere Rolle – unter Einhaltung zuvor vereinbarter Regeln zur Nutzung der Daten durch den Datentreuhänder selbst und Wahrung der Interessen der beteiligten Anspruchsgruppen – als zentrale Funktion zuweisen: Hierzu zählen Instrumente und Mechanismen zur Qualitätssicherung der bereitgestellten Datensätze und zur Einhaltung vereinbarter Standards für Datentransfer durch den Datentreuhänder (Bundesregierung 2021). Dabei sind im Hinblick auf die Sensibilität der bereitgestellten Daten und deren Nutzungszweck verschiedene Stufen von Qualitätsgarantien denkbar, die durch den Datentreuhänder zu gewährleisten sind (Rat für Informationsinfrastrukturen 2020). Einige der befragten Expertinnen und Experten gehen sogar noch einen Schritt weiter und sehen die Weiterverarbeitung, Aufbereitung und Standardisierung der Datenbestände sowie die Bereitstellung von datenbasierten Anwendungen durch den Datentreuhänder als zentrale Voraussetzung für die Schaffung eines Mehrwerts für die Teilnehmenden des Ökosystems. Zudem sollten Datentreuhänder in ihrer Funktion als „Facilitator" (Arlinghaus et al. 2021) datenbasierte Beratungsdienstleistungen für die Datengebenden und Datennutzenden anbieten.

Der Datentreuhänder als Ökosystemförderer

Zudem wird mit dem Begriff des Datentreuhänders auch die Funktion eines Ökosystemförderers verbunden: Nach diesem Verständnis ist es die Aufgabe des Datentreuhänders, die datengetriebene Kollaboration und/oder das Teilen von Daten innerhalb eines spezifischen Anwendungsbereichs oder innerhalb einer konkreten Gruppe von relevanten Akteuren aktiv zu fördern. Hierzu zählt die Bereitstellung einer einfach nutzbaren und leicht zugänglichen Infrastruktur sowie die Schaffung interoperabler Datenstandards (Manohar et al. 2020). Dies gilt insbesondere für Organisationen und Unternehmen, die zwar grundsätzlich Interesse hätten an der Bereitstellung eigener Daten und der Nutzung von Daten Dritter, aber aufgrund fehlender Erfahrungen oder technischem Know-how nicht dazu in der Lage sind. Hier kann auch nach Ansicht einiger Expertinnen und Experten der Datentreuhänder in seiner Funktion als Ökosystemförderer den Onboarding-Prozess neuer Akteure vereinfachen, Unterstützung anbieten und als Motivator auftreten. Dazu gehört etwa die Bereitstellung einer einfach nutzbaren Infrastruktur und entsprechender Schnittstellen über Dienstleistungen im Sinne eines Datenschutz-as-a-Service, die auch Hilfestellungen zur Gewährleistung der Datensicherheit – vor allem für kleinere Einrichtungen und Unternehmen, die dezentral organisiert sind – umfassen (Stevens und Boden 2022). Darüber hinaus könnte der Datentreuhänder Mechanismen zum Matching bzw. der Auffindbarkeit besonders relevanter

Datensätze oder konkreter Teilnehmender des Ökosystems anbieten, um Kooperationen der beteiligten Akteure zu vereinfachen. Im Rahmen der Interviews wurde zudem das Management von zentralen Interessenkonflikten vor der eigentlichen Bereitstellung von Daten und deren Vermittlung als Aufgabe des Datentreuhänders genannt. Durch Ausübung dieser Funktion käme dem Datentreuhänder eine tragende Rolle beim Aufbau eines florierenden Datenökosystems zu.

In den Interviews wurde jedoch mehrfach darauf hingewiesen, dass die Existenz von Vertrauen in einzelne Datentreuhänder und die darauf aufbauenden Datenökosysteme stark vom jeweiligen Anwendungsbereich abhängig sind. Die zuvor aufgeführten Funktionen, die gemäß der Dokumenten- und Interviewanalyse Datentreuhänder zur Schaffung von Vertrauen übernehmen können, sind entsprechend als Sammlung zu verstehen, die unter Rückgriff auf die Gegebenheiten der jeweiligen Anwendungsbereiche in unterschiedlichen Zusammensetzungen oder Detailgraden durch einzelne Datentreuhänder übernommen werden können.

03

3 POTENZIALE UND HERAUSFORDERUNGEN

Mit der digitalen Transformation von Wirtschaft, Wissenschaft und Gesellschaft stellen hochwertige und verfügbare Daten als digitales Abbild produkt-, prozess- oder entscheidungsrelevanter Informationen sowohl für Unternehmen als auch für Forschungseinrichtungen eine zentrale Ressource dar. Ausgehend von den allgemeinen Vorteilen des Data Sharing werden in diesem Kapitel die spezifischen ökonomischen Potenziale von Datentreuhändern aufgezeigt.

3.1 Potenziale des Datenteilens

Unternehmen und Forschungseinrichtungen verfügen oft nicht direkt über alle für ihre Arbeit relevanten Daten. Das macht den Austausch von Daten mit dritten Parteien notwendig. Manche Expertinnen und Experten sehen in der Fähigkeit, Daten über Organisationsgrenzen hinweg nutzen und innerhalb von Wertschöpfungsnetzwerken austauschen zu können, einen der zentralen Faktoren für Wachstum und Erfolg von Unternehmen (Niederée 2019; Element AI und nesta 2019). Konkret sind im Hinblick auf das Teilen von Daten und deren kooperative Nutzung nachfolgend aufgeführte Potenziale erkennbar. Auch wenn die Realisierung dieser Potenziale nicht zwangsläufig mittels eines Datentreuhänders erfolgen muss, sondern auch über andere Modelle – wie etwa bilaterale Vereinbarungen – erreicht werden kann, so kann die Existenz eines Datentreuhänders die Umsetzung in der Praxis positiv beeinflussen.

Veränderte Leistungsangebote und neue Geschäftsmodelle für Unternehmen
Mit zunehmender Digitalisierung verändern sich für Unternehmen sowohl das Marktumfeld als auch die Kundenbedarfe gravierend. Die Verfügbarkeit von qualitativ hochwertigen Daten kann dabei die strategische Ausrichtung einer Unternehmung in zwei Richtungen verändern: Einerseits bilden sie die Grundlage für die Weiterentwicklung bestehender Produkt- oder Leistungsangebote und deren Ergänzung um digitale Features. Andererseits kann die aktive Datensammlung und deren Nutzung auch zur Etablierung neuer, rein digitaler Geschäftsmodelle führen (Azkan et al. 2022; Nentwig et al. 2019). Die organisationsübergreifende Verfügbarkeit von Daten und die Zunahme von grundsätzlich nutzbaren Datenquellen – insbesondere durch die Entwicklungen im Internet-of-Things – schafft dabei sowohl für Start-ups als auch für bestehende Unternehmen die Möglichkeit, sich vom reinen Produzenten oder Dienstleister hin zu datengetriebenen Software- oder Service-Unternehmen zu entwickeln (Ringel et al. 2020).

Prozess- und Leistungsoptimierung im eigenen Unternehmen
Eine Nutzung von externen Datenquellen in Kombination mit der Öffnung interner Datensilos eines jeweiligen Unternehmens kann zudem einen erheblichen Beitrag zur Optimierung von unternehmenseigenen Geschäftsprozessen und Lieferketten ermöglichen (Spiekermann und Meisel 2019). Hier kann ein vertrauensvoller Datenaustausch der wesentliche Erfolgsfaktor sein, während bei einem entsprechenden Mangel an Austausch gravierende Informationsdefizite auftreten können, die den Geschäftserfolg massiv negativ beeinflussen können (Linnartz und Leckel 2020). Die potenziell verbesserte Verfügbarkeit von Daten durch Datenteilungsmodelle – wie etwa einen Datentreuhänder – kann Unternehmen zudem dabei unterstützen, analoge Produkte und Leistungen zu verbessern sowie stärker bedarfsorientiert und individualisiert für die Kundinnen und Kunden zu entwickeln.

Potenziale der Datentreuhand bei der Windenergie
Wie hoch das ökonomische Potenzial von datenbasierter Prozess- und Leistungsoptimierung ist, zeigt ein Beispiel aus dem Bereich der erneuerbaren Energien: Rund ein Drittel der Stromherstellungskosten bei Windenergieanalagen entsteht durch den laufenden Betrieb und die Instandhaltung. Dabei entfällt nur ein Bruchteil auf die eigentlichen Materialkosten für Ersatzteile, während Stillstandzeit und Opportunitätskosten für die Wartung am stärksten ins Gewicht fallen. Datenauswertungen zur Optimierung des Betriebs von Windkraftanlagen, aber auch auf großen Datenmengen basierende Analysen im Sinne der vorausschauenden Wartung mit dem Ziel der Kostenreduktion sowie einer Erhöhung der Leistungsfähigkeit der Anlagen haben hier also eine enorme Bedeutung. Das Projekt FAIRWinDS von mehreren Fraunhofer-Instituten arbeitet daher an einem Datentreuhandmodell für Windenergieanlagen (www.iwes.fraunhofer.de/de/forschungsprojekte/aktuelle-projekte/fairwinds.html, siehe Anhang).

Datenmonetarisierung
Zunehmend bestimmen immaterielle Vermögenswerte wie produkt- und prozessbezogenes Wissen oder die Güte der Kundenbeziehungen die Wettbewerbsfähigkeit von Unternehmen maßgeblich. Aber auch Daten und deren Nutzung werden mittlerweile als immaterielle Vermögenswerte klassifiziert. Mit einer gesteigerten Wahrnehmung des Mehrwerts von Daten steigt dabei auch ihr genuiner finanzieller Wert. Entsprechend besteht grundsätzlich das Potenzial, über die Bereitstellung von Daten Erlöse zu erzielen (Rusche et al. 2019). Zur Abwicklung der dafür erforderlichen Daten- und Finanzströme kann grundsätzlich auch ein Datentreuhänder eingeschaltet werden, der dann die notwendige Infrastruktur und Vertrauensdienste anbietet.

Neben den zuvor genannten grundsätzlichen Potenzialen des Datenteilens sind aber auch spezifische Vorteile von Datentreuhandlösungen erkennbar:

3.2 Ökonomische Potenziale der Datentreuhand

Vertrauensvolle Kooperation bei hochsensiblen Daten
Nimmt der Datentreuhänder seine Funktion als neutraler Vertrauensanker innerhalb eines Datenökosystems wahr und die teilnehmenden Akteure können sich auf die Integrität der nutzbaren Datenbestände und vor allem der Datengebenden verlassen, bildet dies die Grundlage für neue Kooperationen zwischen Unternehmen bzw. neue Formen der Abwicklung von Geschäftsprozessen (D'Addario 2020). Dies gilt, wie auch in den Interviews bestätigt, insbesondere für hochsensible und den Geschäftserfolg bestimmende Daten – beispielsweise Daten über verarbeitete Stückzahlen oder Mengenangaben, die zur Abrechnung von Leistungen erforderlich sind. Aufgrund der hohen Sensibilität der Daten und ihrer Wirkung auf den finanziellen Erfolg eines Unternehmens treten hier verlässlich Interessenkonflikte auf, die durch einen Datentreuhänder sowie die dahinterstehenden technischen bzw. organisatorischen Schutzmaßnahmen vor bewusster Manipulation moderiert werden können.

Zentrale Voraussetzungen sind laut der befragten Expertinnen und Experten der verlässliche Schutz von Betriebsgeheimnissen und anderen sensiblen Daten sowie ein klar erkennbarer Mehrwert für die am entstehenden Ökosystem beteiligten Akteure. Ihr volles Potenzial können auf Datentreuhändern aufbauende Ökosysteme dann entfalten, wenn die zugrunde liegenden Modelle domänenübergreifend offen und interoperabel gestaltet werden.

Potenziale der Datentreuhand in der Forstwirtschaft
Welche Praxisrelevanz in diesem Zusammenhang vorliegt, zeigt die Forstwirtschaft: In Deutschland gibt es etwa zwei Millionen Waldbesitzer – vom kleinen Nebenerwerbswald bis hin zu staatlichen Großbetrieben – die etwa 2.000 Sägewerke und 200 Papierfabriken mit Holz versorgen. Die Holzernte wird oftmals von Lohnunternehmern im Auftrag der Waldbesitzer durchgeführt. Bei der zum Großteil voll oder teilweise mechanisierten Holzernte kommen etwa 1.600 sogenannte Harvester zum Einsatz, die bereits bei der Fällung und anschließenden Weiterverarbeitung der einzelnen Stämme eine Vielzahl von Daten zu Parametern wie Länge, Dicke und Qualität des Holzes erheben und sammeln. Trotz der Existenz dieser Daten wird aber oftmals noch jeder einzelne Stamm manuell durch den Waldbesitzer für die Erstellung der Rechnung für Sägewerke oder Papierfabriken vermessen und qualifiziert. An der Fabrik angekommen, werden die Stämme dann zur Kontrolle oftmals noch einmal durch den Abnehmer vermessen und qualifiziert. Hinter diesen Abläufen stehen klare finanzielle Interessen, da die Menge und die Güte des gefällten Holzes natürlich den anzusetzenden Preis bestimmt. Die mehrfache Vermessung trotz der bereits vorliegenden Datenbestände zeigt, dass es gerade bei hochsensiblen Daten eines neutralen Vertrauensankers bedarf, der zwischen den beteiligten Parteien vermittelt und eine Vertrauensbasis schafft. Entsprechend beschäftigt sich das Forschungsprojekt S3I-X mit dem Aufbau eines Datentreuhänders für die Forstwirtschaft (www.kwh40.de/s3i-x, siehe Anhang).

Verlässliche und rechtssichere Verfügbarkeit von qualitativ hochwertigen Daten in leicht nutzbaren Formaten
Darüber hinaus können Datentreuhänder ein probates Konstrukt sein, um einen einfach nutzbaren Zugang zu qualitativ hochwertigen, verlässlich und rechtssicher verfügbaren Daten dauerhaft sicherzustellen (Manohar et al. 2020). Kann der Datentreuhänder die rechtssichere Datennutzung im Sinne der Vereinbarkeit der Weitergabe mit geltenden Datenschutz- und Compliance-Regelungen oder dem Schutz von Geschäftsgeheimnissen vorab sicherstellen, werden nach Einschätzung der Interviewpartnerinnen und Interviewpartner viele Bedenken aufseiten der Datennutzenden ausgeräumt. Qualitätschecks und sichere sowie leicht nutzbare Systeme verbessern die Attraktivität der über den Datentreuhänder verfügbaren Daten.

Senkung von Transaktionskosten
Datentreuhänder können die Transaktionskosten einer akteursübergreifenden Datennutzung gravierend senken (Manohar et al. 2020). Potenzielle Datennutzende, insbesondere im Fall eines Datentreuhänders nach engem Begriffsverständnis, können den Datentreuhänder als direkte Ansprechperson nutzen oder über dessen technische Plattform eine Vielzahl potenziell relevanter Datengebender erreichen. So wird eine zeit- und kostenintensive bilaterale Kommunikation unnötig oder zumindest stark reduziert. Darüber entfallen bei Vorliegen eines Vertrauensverhältnisses zwischen den beteiligten Akteuren – dessen Aufbau und Erhaltung als mögliche Funktion von Datentreuhändern identifiziert wurde – hohe Transaktionskosten für die Qualitätsprüfung der Datenbestände. Je mehr Transaktionskosten dabei reduziert werden können oder komplett wegfallen, desto mehr Transaktionen werden letztendlich über den Datentreuhänder abgewickelt.

3.3 Gesellschaftliche Potenziale der Datentreuhand

Gesteigerte Datensouveränität für Einzelpersonen
Auch im Kontext von Einzelpersonen als mögliche Datengebende haben Datentreuhänder ein hohes Potenzial: Nimmt ein Datentreuhänder etwa die Betroffenenrechte von Einzelpersonen bei der Sammlung oder regelbasierten Weitergabe ihrer individuellen Daten wahr, würde laut Interviews die derzeit an vielen Stellen beobachtbare Consent-Fatigue abgeschwächt und die bisher eher als ohnmächtig wahrgenommene Stellung der Einzelpersonen gegenüber datennutzenden Unternehmen gestärkt werden. Manche Expertinnen und Experten sehen sogar noch weitere Möglichkeiten zur Verbesserung der Situation von Einzelpersonen als Datengebende: So könnten Datentreuhänder für Einzelpersonen neben der tatsächlichen Wahrnehmung der Betroffenenrechte gegenüber beteiligten Dritten auch eine Beratungsfunktion für die Datengebenden wahrnehmen. Grundsätzlich gelte dabei die Annahme: Je sensitiver die Daten sind, desto höher ist die Akzeptanz für die Einschaltung eines Datentreuhänders.

Datentreuhänder als wettbewerbs- und wirtschaftspolitisches Steuerungsinstrument
Darüber hinaus wird im öffentlichen Diskurs immer häufiger das Potenzial von Datentreuhändern als ergänzendes Steuerungsinstrument der Wettbewerbs- und Wirtschaftspolitik aufgeführt.
Ein entsprechendes Potenzial ist dabei vor allem im Hinblick auf eine gesetzlich zu verankernde, obligatorische Nutzung von Datentreuhändern in einzelnen Anwendungsbereichen zu erkennen. Durch den entstehenden Datenzugang für zuvor von der Datennutzung ausgeschlossene Unternehmen werden die Rahmenbedingungen des Wettbewerbs in der Digitalökonomie fairer gestaltet. Damit könnten Datentreuhänder ein wichtiger Baustein sein, um auftretenden Marktversagensproblemen der digitalen Plattformökonomie – wie etwa die Folgen einer datenbasierten Zementierung von Marktmacht und damit geschwächten Verhandlungspositionen vor allem kleinerer und mittlerer Unternehmen – entgegenzuwirken. Wie weitreichend derartige Verpflichtungen ausgestaltet werden, muss in jedem Einzelfall geprüft werden und entsprechend der konkreten Zielstellung muss dann die staatliche Steuerung ausgestaltet werden (Specht-Riemenschneider et al. 2021).

Datentreuhänder zur besseren Bewältigung staatlicher Aufgaben
Die Vorteile der Etablierung von Datentreuhändern werden auch im Kontext der Erfüllung staatlicher Aufgaben vermehrt diskutiert. Neben einer Sicherung der Qualität bestehender Datensätze und der Gewährleistung der Integrität eines Datums trotz der Nutzung durch verschiedenste staatliche Stellen steht hier vor allem die strukturierte Erschließung neuer bzw. bisher nur in einzelnen Silos vorliegender Datenbestände im Mittelpunkt. Im Fokus des Interesses steht dabei sowohl die Bündelung von Datenbeständen unterschiedlicher staatlicher Stellen und deren zweckgebundene Nutzbarmachung für einzelne Verwaltungseinheiten als auch die strukturierte Sammlung von Unternehmensdaten zu Kontrollzwecken mittels eines Datentreuhänders. Gerade beim letztgenannten Aspekt werden Datentreuhändern erhebliche Potenziale zugeschrieben: So bestehen bei der Ausübung staatlicher Kontroll- und Aufsichtsfunktionen aufgrund fehlender digitaler und nicht existenter bzw. wenig strukturierter Datenbestände erhebliche Verbesserungspotenziale. Gleichzeitig besteht bei der Sammlung von Daten durch staatliche Stellen aber immer auch ein erhöhtes Missbrauchspotenzial. Entsprechend könnten Datentreuhänder hier als Stellen etabliert werden, die Daten strukturiert von staatlichen Stellen, aber auch Unternehmen oder gegebenenfalls Einzelpersonen zusammenziehen und gleichzeitig deren Verwendung durch staatliche Stellen eng an die Zweckgebundenheit einer bestimmten Kontroll- oder Steuerungsfunktion knüpfen könnten.

Als nachvollziehbare Anwendungsbeispiele wurden in den geführten Interviews etwa die Kontrolle von Finanzströmen und die damit verbundene Geldwäsche- und Betrugsbekämpfung sowie die Erstellung von detaillierten Mobilfunkabdeckungskarten aufgeführt.

Einfachere und effizientere Forschung mit Daten
Datentreuhändern werden enorme Potenziale zugeschrieben, wenn es um den verbesserten Datenzugang für FuE-Aktivitäten von Forschungseinrichtungen und Unternehmen geht. Datentreuhänder als zentrale Anlaufstelle für mögliche Datennutzende vereinfachen den Zugang zu einer Vielzahl unterschiedlicher Datenquellen und können gleichzeitig die Einhaltung konkreter Regeln zu deren Verwendung – technisch und organisatorisch – umsetzen. Das Potenzial von Datentreuhändern ist dabei laut Interviews in den Anwendungsbereichen besonders groß, in denen verschiedenste Datenquellen zur Beantwortung relevanter Fragestellungen zusammengeführt werden müssen und dabei sowohl staatliche als auch privatwirtschaftliche Akteure involviert sind. Darüber hinaus können Datentreuhänder einen erheblichen Beitrag dazu leisten, die langwierigen und sehr kostenintensiven Prozesse der Aushandlung von Nutzungsrechten bzw. Verträgen zur Datenüberlassung zu Forschungszwecken deutlich zu verkürzen.

3.4 Herausforderungen für die Etablierung von Datentreuhändern

Den ökonomischen und gesellschaftlichen Vorteilen von Datentreuhändern stehen derzeit noch einige Herausforderungen gegenüber:

Mangelndes Verständnis für den Mehrwert von Daten und fehlende Erfolgsbeispiele von Datentreuhänderschaft
Die Beurteilung von Daten als wertvolle Ressource im wirtschaftlichen Wettbewerb hat sich erst in den letzten Jahren entwickelt: Am Anfang digitaler Transformationsprozesse wurden sie allgemein eher als Nebenprodukt des Übergangs vom analogen hin zum digitalen Informationsaustausch wahrgenommen (Niederée 2019). Diese Erkenntnis hat sich aber noch nicht bei allen Unternehmen durchgesetzt oder es fehlt an einer entsprechenden praktischen Umsetzung im Arbeitsalltag: Lediglich ein verschwindend geringer Teil von Unternehmen nutzt vollumfänglich die eigenen Datenbestände oder ist sogar Teil eines losen digitalen Netzwerks bzw. eines etablierten Ökosystems, in dem der Austausch von Daten selbstverständlich und proaktiv vorangetrieben wird (Otto et al. 2019a). Darüber hinaus vermissen nach Einschätzungen aus den Interviews Entscheidungsträgerinnen und Entscheidungsträger in Unternehmen oftmals praxisnahe Erfolgsbeispiele für unternehmensübergreifende Datennutzung und im Realbetrieb agierende Datentreuhänder. Hier greift die Henne-Ei-Problematik: So ist für viele Entscheidende in Unternehmen der Nutzen der Bereitstellung von eigenen Daten noch unklar und auch die Mehrwerte von extern bereitgestellten Daten in den meisten Fällen bleiben eher abstrakt. Auf der anderen Seite sind der mögliche Schaden für die eigene Reputation – beispielsweise bei rechtswidriger Weitergabe von Daten – und die finanziellen Risiken durch entsprechende Strafen, erforderliche Investitionen für die Anbindung an das mittels Datentreuhänder zu etablierende Ökosystem oder durch finanzielle Einbußen aufgrund eines erhöhten Wettbewerbs durch neue Marktteilnehmer grundsätzlich hoch. Hier müssen Datentreuhänder Lösungen finden, um die Vorbehalte der relevanten Entscheidungstragenden abzubauen.

Fehlendes Know-how und unzureichende Infrastruktur der handelnden Akteure
Jedoch fehlen oftmals die technischen und organisatorischen Voraussetzungen für die Realisierung der zuvor geschilderten Potenziale. So kann trotz einiger identifizierbarer Weiterentwicklungen flächendeckend ein gewisser Grad der Unreife von Unternehmen bei der internen Nutzung der eigenen Datenbestände, insbesondere jedoch bei der Bereitstellung von Daten für Dritte festgehalten werden (Azkan et al. 2022). Dies gilt für alle Anwendungsbereiche – auch für hochdigitalisierte Branchen wie die fertigende Industrie (Cattaneo und Francalanci 2020). (Cattaneo und Francalanci 2020). Der Aufbau einer leistungsfähigen Infrastruktur und die Bereitstellung entsprechender Schnittstellen für die Nutzung der eigenen Daten sowie deren externe Bereitstellung wird für die Unternehmen mit spürbaren Investitionskosten verbunden sein. Hinzu kommen laut Aussagen von Interviewpartnerinnen und Interviewpartnern Unsicherheiten im Hinblick auf die rechtlich einwandfreie Umsetzung des Datenaustauschs, vor allem im Hinblick auf das Thema Datenschutz, aber auch in Bezug auf Fragen der Haftung, der Ausgestaltung von Lizenzen sowie dem Schutz von Geschäftsgeheimnissen und der kartellrechtlichen Vereinbarkeit einer Weitergabe von Unternehmensdaten. Die genannten Defizite treten auch beim Aufbau und der Integration von Datentreuhandmodellen hervor. Insbesondere die technische und rechtliche Organisation von Datentreuhändern im Hinblick auf die Etablierung als Vertrauensinstanz stellt viele Akteure vor Herausforderungen. Häufig fehlt es an entsprechenden Vorerfahrungen oder branchenspezifischen Best-Practice-Lösungen, um die Potenziale des datentreuhandbasierten Data-Sharing zu heben.

Versagen von Datenmärkten: Angst vor Übervorteilung, fehlendes Vertrauen und rechtliche Unsicherheiten
Trotz des immer stärker werdenden Wunsches der Kooperation mit Mitbewerbern in einigen Branchen (Marx 2020) steht bei der Entscheidung zur Öffnung der hauseigenen Datensilos für außenstehende Dritte die Angst vor einer Übervorteilung durch den direkten Wettbewerb oder durch zusätzliche Konkurrenz seitens etablierter Technologieunternehmen im Raum. Dieser Umstand gilt insbesondere für hochsensible Geschäftsdaten wie etwa Kundenstammdaten, Ein- und Verkaufspreise sowie detaillierte Produkt- oder Prozessdaten (INFORM 2017). Um die Potenziale der systematischen Verarbeitung und Nutzung von externen Datenquellen realisieren zu können, müssen die bereitgestellten Daten zudem grundlegende Qualitätsanforderungen erfüllen. Die tatsächliche Nützlichkeit ist dabei abhängig von der Validität der Daten, ihrer Aktualität und Vollständigkeit sowie ihrer Verständlichkeit und Zugänglichkeit (Clarke 2016). Die Interviewexpertinnen und -experten haben zudem angegeben, dass gerade in wettbewerblich hart umkämpften Märkten und bei besonders sensiblen Daten in Unternehmen oftmals Zweifel an der tatsächlichen Qualität der durch Dritte zur Verfügung gestellten Daten bestehen. Die Herausforderung für Datentreuhänder besteht also darin, die Qualität der Daten glaubhaft zu gewährleisten und das faire Zusammenspiel der beteiligten Akteure zu sichern. Die vom Datentreuhänder dazu etablierten Maßnahmen müssen aber auch durch die Teilnehmenden des Ökosystems akzeptiert werden. Da die potenziellen Teilnehmenden aber oft nicht in Gänze bekannt sind, steht der Datentreuhänder oftmals vor der Herausforderung, individuelle Regeln und Sicherheitsmaßnahmen für ein Datenökosystem zu entwerfen, dessen Ausmaße er nicht final kennt. Vor dem Hintergrund dieser Herausforderungen findet eine Datenbereitstellung zwischen Unternehmen – auch gemäß den Ergebnissen einer Umfrage des Instituts der deutschen Wirtschaft im Auftrag des BDI – nur in sehr geringem Maße statt: 74 Prozent von über 500 befragten Unternehmen sehen eine Datenweitergabe an andere Unternehmen als „nicht erwünscht" an. 85 Prozent der befragten Unternehmen sehen datenschutzrechtliche Grauzonen und 84 Prozent schätzen Unklarheiten bezüglich der Nutzungsrechte an den Daten ausschlaggebend als hemmende Faktoren für das nicht erfolgende

Datenteilen ein (Röhl und Bolwin 2021). Zudem sind in den Interviews weitere Faktoren als Hindernisse aufgeführt worden, die in Kombination derzeit einen erheblichen Beitrag zu einem erkennbaren Versagen von Datenmärkten leisten bzw. deren Etablierung erheblich erschweren. Hierzu zählen eine unzugängliche und intransparente Angebotslandschaft ohne standardisierte Datenprodukte, sehr hohe Transaktionskosten und die Marktmacht dominanter – vor allem vertikal in eine Wertschöpfungskette integrierter – Unternehmen, die sich vor dem Hintergrund potenziell entstehender Konkurrenz strategisch gegen eine Weitergabe von Daten entscheiden (Falck und Koenen 2020). Ein weiterer Grund für ein Versagen von Datenmärkten ist die Dominanz weniger marktbeherrschender Akteure. Die dominierenden Unternehmen haben frühzeitig eigene Daten-Ökosysteme geschaffen, deren Zugang für andere Akteure durch sie selbst – und in den meisten Fällen stark restriktiv – gestaltet wird. Somit sind zentral wichtige Datenbestände für Produkt- und Prozessinnovationen kleiner und mittlerer Unternehmen nicht nutzbar (Collovà et al. 2021).

Überwindung des Privacy-Paradoxes und Akzeptanz von Datentreuhändern bei Einzelpersonen
Im Kontext von Daten von Einzelpersonen ist darüber hinaus die aktive Minderung des viel diskutierten Privacy-Paradoxes[3] eine zentrale Herausforderung, die durch Datentreuhänder aktiv behandelt werden muss: Wie kann die Motivation von Einzelpersonen erhöht werden, den initialen Aufwand für die Mitwirkung an einem mittels Datentreuhänder zu etablierenden Ökosystems auf sich zu nehmen (Schneider 2022). Allerdings bleibt bisher weitgehend unklar, welche Faktoren jenseits der klar erkennbaren Netzwerkeffekte großer Plattformbetreiber hier eine Rolle spielen. Eine entsprechende Aufgabe für Datentreuhänder ist in diesem Zusammenhang die Schaffung nutzungsfreundlicher technischer Oberflächen, die gleichzeitig alle relevanten Informationen enthalten und vor dem Hintergrund der bereits aufgeführten Consent-Fatigue klare Regeln für die Datennutzung durch Dritte leicht verständlich abbilden (Collovà et al. 2021).

Unklare Geschäfts- bzw. Betriebsmodelle für Datentreuhänder
Als weiteres Hemmnis sind – sowohl bei Datentreuhänderschaft im Kontext von Unternehmen bzw. Organisationen als auch bei Daten von Einzelpersonen – die Unsicherheiten im Hinblick auf die neuen Regelungen des Data Governance Act der Europäischen Union und deren potenziell negative Auswirkungen auf mögliche zusätzliche Dienste zu nennen, die durch einen Datentreuhänder erbracht werden könnten und die die Attraktivität der Teilnahme von Unternehmen oder Einzelpersonen am jeweiligen Ökosystem steigern könnten (darauf geht Kapitel 4.2 detailliert ein). Diese Unsicherheiten – gepaart mit hohen Anfangsinvestitionen für den Aufbau der erforderlichen technischen Infrastruktur, aber vor allem auch für Maßnahmen zum Aufbau eines florierenden Ökosystems – lassen laut mehreren Interviewpartnerinnen und Interviewpartnern die Etablierung von Datentreuhändern als wirtschaftlich tragfähiges Geschäftsmodell bisher wenig attraktiv erscheinen. Damit stellt die nachhaltige Finanzierung des Aufbaus und des Betriebs von Datentreuhändern eine der zentralen Herausforderungen dar (Schneider 2022).

3 Privacy-Paradox: Der scheinbare Widerspruch bei vielen Menschen zwischen allgemein bekundeten Datenschutzbedenken und dem freizügigen Teilen eigener Personendaten in sozialen Netzwerken, beim Online-Einkauf etc.

04

4 RECHTLICHE RAHMENBEDINGUNGEN

Die rechtlichen Rahmenbedingungen spielen bei der Ausgestaltung von Datentreuhandmodellen eine zentrale Rolle. Während die Organisation und Rechtsform von Datentreuhändern vorrangig durch das Zivilrecht vorgegeben werden, gewinnt die datenbezogene Gesetzgebung an Bedeutung, insbesondere auf EU-Ebene. Mit der Verabschiedung des europäischen Data Governance Act gelten künftig konkrete Vorgaben für Datenvermittlungsdienste, die Einfluss auf den Aufbau und die Funktionsweise von Datentreuhändern haben werden. Daneben ergeben sich rechtliche Implikationen aus dem Datenschutz- und Urheberrecht sowie den Regelungen zum Schutz von Geschäftsgeheimnissen.

4.1 Herleitung des Treuhandbegriffs und dessen Übertragbarkeit auf Datentreuhänder

Der Begriff Datentreuhänder (data trust) wurde erstmals in Anlehnung an die im angelsächsischen Rechtsraum anerkannte Rechtsform des Trusts genannt (Richter 2021b). In Kontinentaleuropa und insbesondere in Deutschland existieren indes keine gesetzlichen Regelungen zur Treuhänderschaft, die beispielgebend für die Rolle von Datentreuhändern sein könnten. Gemeinhin werden unter Treuhand Rechtsverhältnisse gefasst, bei denen Rechte oder Rechtsbefugnisse von einem Treugeber auf einen Treunehmer übertragen werden (Schubert 2018). Die Rechte und Pflichten des Treuhänders werden dabei vertraglich bestimmt. Der Treuhänder verpflichtet sich, die Interessen des Treugebers vertragsgemäß wahrzunehmen. Kennzeichnend für Treuhandverhältnisse ist zudem, dass die Ausübung der Treuhänderschaft fremdnützig, also im Interesse des Treugebers, erfolgt. Häufig anzutreffen sind Treuhandformen, in denen Vermögenswerte verwaltet werden. Der Treuhänder tritt dabei häufig als Stellvertreter des Treugebers auf und trifft Verfügungen in Bezug auf das jeweilige Treugut. In anderen Fällen ist die Treuhand selbst Rechteinhaberin (z. B. Eigentümerin) und kann Verfügungen im eigenen Namen vornehmen.

Die zivilrechtlichen Grundsätze der Treuhand lassen sich nur teilweise auf Datentreuhänder übertragen. Gemeinsamkeiten lassen sich vor allem in der Fremdnützigkeit und der Zweckgebundenheit der Tätigkeit ausmachen. In Bezug auf die rechtlichen Möglichkeiten, über das Treugut Daten zu verfügen, ergeben sich jedoch Unterschiede. Ein Datentreuhänder kann niemals ein Vollrecht an Daten übertragen. Daten als solche sind nicht eigentumsfähig. Da bereits der Dateninhaber kein Vollrecht oder ein anderes ausschließliches Recht an Daten hat, kann der Datentreuhänder folglich auch nicht im eigenen Namen über solche Rechtspositionen verfügen. Der Datentreuhänder hat somit nur die Möglichkeit, Entscheidungen über den Datenzugang zu treffen (Specht-Riemenschneider et al. 2021). Bei Vorliegen einer entsprechenden Vollmacht kann er Dritten Zugangs- und -nutzungsrechte an Daten einräumen. Als sonstige Gegenstände im Sinne von § 453 BGB können Daten zum Inhalt von Rechtsgeschäften gemacht werden. In solchen Datentreuhandkonstellationen werden die Rechte und Pflichten der Akteure vertraglich festgelegt. Daneben sind auch Datentreuhandmodelle denkbar, bei denen eine gesetzliche Verpflichtung besteht, Daten an eine treuhänderische Instanz zu überantworten. Derartige obligatorische Modelle werden zwar diskutiert, sind jedoch in Bezug auf Daten bislang noch nicht verwirklicht (Specht-Riemenschneider et al. 2021).

4.2 Der Data Governance Act

Mit der Verordnung über eine europäische Daten-Governance (Data Governance Act, DGA) wurde ein Anmelde- und Aufsichtsrahmen für Datenvermittlungsdienste geschaffen, der ab September 2023 in der gesamten EU unmittelbar anwendbar ist. Mit dem Data Governance Act sollen die Bedingungen für die gemeinsame Datennutzung im Binnenmarkt verbessert werden und ein harmonisierter Rahmen für den Datenaustausch geschaffen werden (ErwG 3 DGA). Ziel ist es, das Vertrauen in die gemeinsame Datennutzung zu stärken, indem Mechanismen geschaffen werden, die es den betroffenen Personen und Dateninhabern ermöglichen, Kontrolle über die sie betreffenden Daten auszuüben und sonstige Hemmnisse für eine gut funktionierende und wettbewerbsfähige datengesteuerte Wirtschaft abzubauen (ErwG 5 DGA). Ein Kernelement des DGA ist die Regulierung von Datenvermittlungsdiensten. Diesen wird eine Schlüsselrolle in der Datenwirtschaft zugeschrieben (ErwG 27 DGA). Der DGA hat perspektivisch auch Auswirkungen auf die Organisation und Ausgestaltung von Datentreuhändern, da diese als Intermediär zwischen Dateninhabenden und Datennutzenden auftreten und damit Datenvermittlungsdienste im Sinne der Verordnung anbieten. Datenvermittlungsdienste müssen sich künftig vor der Aufnahme ihrer Tätigkeit bei der zuständigen Behörde anmelden (Art. 11 Abs. 1 DGA). Neben dieser und weiteren formellen Anforderungen werden zudem konkrete Bedingungen formuliert, die bei der Erbringung von Datenvermittlungsdiensten erfüllt werden müssen:

Zweckbindung
Der Grundsatz der Zweckbindung bestimmt, dass Datenvermittlungsdienste Daten für keine anderen Zwecke verwenden dürfen, als sie den Datennutzenden zur Verfügung zu stellen. Der Datenvermittlungsdienst ist damit auf eine reine Vermittlungstätigkeit beschränkt. Metadaten, die infolge der Vermittlungstätigkeit verarbeitet werden, dürfen nur für die Entwicklung bzw. Weiterentwicklung des Vermittlungsdienstes verwendet werden. Daneben ist eine Nutzung der Daten zur Betrugsprävention und zur Gewährleistung der Informationssicherheit zulässig. Die kommerziellen Bedingungen einschließlich der Preisgestaltung dürfen darüber hinaus nicht davon abhängig gemacht werden, ob der Dateninhabende oder Datennutzende andere Dienste des Datenvermittlungsdiensts in Anspruch nimmt. Die Bereitstellung des Vermittlungsdienstes hat zudem über eine gesonderte juristische Person zu erfolgen.

Datenformate und Interoperabilität
Der Anbieter von Datenvermittlungsdiensten ist zudem verpflichtet, Daten in dem Format bereitzustellen, in dem er diese von dem jeweiligen Dateninhaber erhält. Eine Umwandlung in andere Datenformate ist zulässig, wenn dies der Verbesserung der Interoperabilität innerhalb und zwischen Sektoren dient oder wenn der Datennutzende dies verlangt. Bei der Herstellung der Interoperabilität ist der Datenvermittlungsdienst dazu angehalten, auf offene Standards zurückzugreifen (zur Definition offener Standards siehe Abschnitt 5.5.2). Daneben ist eine Umwandlung in andere Datenformate gestattet, wenn dies durch Unionsrecht vorgeschrieben ist oder wenn es der Harmonisierung mit internationalen oder europäischen Datennormen dient. Dem Dateninhaber muss jedoch die Möglichkeit eingeräumt werden, der Datenumwandlung zu widersprechen (opt-out).

Zulässige Datenaufbereitungsdienste
Im begrenzten Rahmen dürfen Datenvermittlungsdienste auch zusätzliche datenbezogene Dienste anbieten. Hiervon umfasst sind Werkzeuge und Dienste, um den Datenaustausch zu erleichtern, wie die vorübergehende Speicherung, Pflege, Konvertierung, Anonymisierung und Pseudonymisierung von Daten. Derartige Maßnahmen sind jedoch nur zulässig, wenn der Dateninhaber dies verlangt.

Weitere Pflichten
Daneben werden weitere Pflichten in Bezug auf die Erbringung von Datenvermittlungsdiensten festgelegt. Hierzu gehören u. a. die Sicherstellung, dass die Zugangsbedingungen zu dem Dienst fair, transparent und nicht diskriminierend sind. Notwendig sind zudem Maßnahmen zur Betrugsprävention, zur Absicherung der Daten im Falle der Insolvenz sowie die Ergreifung von technischen, rechtlichen und organisatorischen Maßnahmen zur Verhinderung von rechtswidrigen Datenübertragungen. Auch die Gewährleistung eines angemessenen Niveaus der Informationssicherheit gehört zum Pflichtenkatalog für Datenvermittlungsdienste.

Überwachung der Einhaltung
Die Einhaltung der Bedingungen für die Erbringung von Datenvermittlungsdiensten wird durch eine zu errichtende Aufsichtsbehörde überwacht. Bei Verstößen kann die Behörde Bußgelder verhängen oder die Einstellung des Datenvermittlungsdienstes anordnen.

Definition von Datenvermittlungsdiensten
Datenvermittlungsdienst wird definiert als ein Dienst, mit dem durch technische, rechtliche oder sonstige Mittel Geschäftsbeziehungen zwischen einer unbestimmten Anzahl von betroffenen Personen oder Dateninhabenden und Datennutzenden hergestellt werden sollen, um die gemeinsame Datennutzung, auch für die Zwecke der Ausübung der Rechte betroffener Personen in Bezug auf personenbezogene Daten, zu ermöglichen (Art. 2 Nr. 11 DGA). Hierunter fallen beispielsweise Datenmarktplätze oder Orchestrierer von Ökosystemen zur gemeinsamen Datennutzung. Die Bereitstellung von Cloud-Speichern, Analysediensten, Software zur gemeinsamen Datennutzung, Internetbrowsern oder Browser-Plug-ins sowie von E-Mail-Diensten wird von der Definition nicht umfasst, sofern mit diesen Diensten ausschließlich technische Werkzeuge zur gemeinsamen Datennutzung bereitgestellt werden, die Bereitstellung dieser Werkzeuge aber weder darauf abzielt, zwischen Dateninhabenden und Datennutzenden eine geschäftliche Beziehung herzustellen, noch dem Anbieter von Datenvermittlungsdiensten ermöglicht, Informationen über die Herstellung geschäftlicher Beziehungen zum Zwecke der gemeinsamen Datennutzung zu erlangen (ErwG 28 DGA).

Daneben werden in der Legaldefinition weitere negative Abgrenzungskriterien aufgeführt: Danach handelt es sich bei bestimmten Diensten um keine Datenvermittlungsdienste im Sinne des DGA. Hierzu gehören Dienste, in deren Rahmen Daten von Dateninhabern eingeholt und aggregiert, angereichert oder umgewandelt werden, um deren Wert erheblich zu steigern, und in deren Rahmen Lizenzen für die Nutzung der resultierenden Daten an die Datennutzenden vergeben werden, ohne eine Geschäftsbeziehung zwischen Dateninhabenden und Datennutzenden herzustellen. Ebenso wenig gelten Dienste als Datenvermittlungsdienst, wenn deren Schwerpunkt auf der Vermittlung von urheberrechtlich geschützten Inhalten liegt. Ausgenommen sind zudem Dienste, die ausschließlich von einem Dateninhaber genutzt werden, um die Verwendung von im Besitz dieses Dateninhabers befindlichen Daten zu ermöglichen, oder die von mehreren juristischen Personen

in einer geschlossenen Gruppe genutzt werden – einschließlich Lieferanten- oder Kundenbeziehungen oder vertraglich festgelegte Kooperationen – insbesondere wenn deren Hauptziel darin besteht, Funktionen von Gegenständen und Geräten im Zusammenhang mit dem Internet der Dinge sicherzustellen. Von der Definition ausgenommen sind zudem Datenvermittlungsdienste, die von öffentlichen Stellen ohne die Absicht der Herstellung von Geschäftsbeziehungen angeboten werden.

Datentreuhänder als Datenvermittlungsdienst
Ob und inwieweit Datentreuhanddienste künftig in den Anwendungsbereich des DGA fallen, hängt maßgeblich davon ab, wie der Dienst ausgestaltet ist und welche Aufgaben er innerhalb eines Datenökosystems übernimmt. Die Herstellung einer Geschäftsbeziehung zwischen Dateninhabenden und Datennutzenden zur Ermöglichung einer gemeinsamen Datennutzung wird in vielen Konstellationen erfüllt sein. Dies betrifft insbesondere klassische Datenmarktplätze, Datendrehscheiben sowie Plattformen zum Austausch von Daten innerhalb bestimmter Sektoren und Branchen. Abzugrenzen sind jedoch solche Datentreuhandkonstruktionen, die nicht darauf ausgerichtet sind, Geschäftsbeziehungen zwischen Dateninhabenden und einer unbegrenzten Anzahl von Datennutzenden zu vermitteln. Dies wären in diesem Kontext beispielsweise Zusammenschlüsse von mehreren juristischen Personen in einer geschlossenen Gruppe, etwa zur Steuerung von Lieferanten- oder Kundenbeziehungen. Von den Regelungen des DGA sind zudem Datentreuhandkonstellationen ausgeschlossen, die ausschließlich technische Werkzeuge zur gemeinsamen Datennutzung bereitstellen, diese Bereitstellung jedoch nicht explizit auf die Herstellung einer Geschäftsbeziehung ausgerichtet ist. Das Merkmal der Herstellung einer Geschäftsbeziehung fehlt auch dann, wenn ein Datentreuhänder einen Dienst anbietet, der ausschließlich den Zweck hat, Daten des Dateninhabers für diesen vorzuhalten, nicht jedoch an Dritte weiterzugeben.

4.3 Die möglichen Auswirkungen des Data Governance Act auf die Entwicklung von Datentreuhandmodellen

Der DGA wird zukünftig einen großen Einfluss auf die Konzeption und Ausgestaltung von Datentreuhändermodellen haben. Als Datenvermittlungsdienste unterliegen diese in den meisten Fällen den formellen und materiellen Anforderungen des DGA. Datentreuhandmodelle, die ohnehin auf dem Konzept eines neutralen Vermittlers aufgebaut sind, werden dementsprechend weniger Schwierigkeiten bei der Umsetzung der Anforderungen haben. Dies betrifft vor allem das Erfordernis der Neutralität und Zweckbindung der Datennutzung. Datentreuhänder, die neben der reinen Datenmittlung auch weitere datenbezogene Dienste anbieten, stehen zukünftig vor der Herausforderung, die Vorgaben des DGA im Rahmen ihres Geschäfts- oder Betriebsmodells zu berücksichtigen. Hier können insbesondere die Anforderungen der Neutralität und Zweckbindung zu Umsetzungsschwierigkeiten führen. Dienste der Datenvermittlung wären zudem streng von anderen Bereichen zu trennen. Plattformen, die beispielsweise zusätzliche datenbasierte Produkte anbieten, müssen dafür Sorge tragen, dass diese nicht akzessorisch zu der Datenvermittlung stehen. Das bedeutet, dass die Inanspruchnahme des Vermittlungsdienstes auch ohne Nutzung weiterer datenbezogener Dienste möglich sein muss. In der Folge stellt sich auch die Frage, ob die reine Vermittlung von Daten einen wirtschaftlich tragfähigen Betrieb zulässt. Zumal die datenbezogenen Dienste, welche nach dem DGA zulässig sind, sich auf Werkzeuge und Dienste im Bereich Datenpflege, Konvertierung, Anonymisierung und Pseudonymisierung beschränken. Dem begrenzten wirtschaftlichen Nutzen stehen nicht unerhebliche Pflichten gegenüber, deren

Verletzung zudem sanktioniert werden kann. Der DGA-konforme Aufbau bzw. die Umgestaltung der Governance-Strukturen könnten daher auf einige Akteure abschreckend wirken. Es ist damit abzuwarten, ob das Konzept des Datenvermittlungsdienstes in der Praxis trägt und die vom Gesetzgeber intendierten Impulse für die Datenwirtschaft eintreten.

4.4 Weitere Regelungsbereiche

Neben den Vorgaben des Data Governance Act sind bei der Ausgestaltung von Datentreuhandmodellen auch weitere gesetzliche Regelungen zu berücksichtigen. Bezugspunkte ergeben sich insbesondere aus dem Datenschutz- und dem Urheberrecht sowie den Regelungen zum Schutz von Geschäftsgeheimnissen.

4.4.1 DATENSCHUTZRECHT

Die für die Datentreuhand kennzeichnende Fremdnützigkeit der Aufgabenerfüllung führt zu der Frage, inwieweit eine datenschutzrechtliche Interessenswahrnehmung mit den Regelungen des Datenschutzrechts im Einklang stehen. Im Rahmen des Data Governance Act wird die Rolle von Datenvermittlungsdiensten für personenbezogene Daten hervorgehoben. Anbieter solcher Dienste wollen demnach die Handlungsfähigkeit betroffener Personen und insbesondere die Kontrolle von Einzelpersonen in Bezug auf die sie betreffenden Daten verbessern. Dies umfasst die Unterstützung bei der Ausübung ihrer datenschutzrechtlichen Betroffenenrechte, u. a. in Bezug auf die Erteilung oder den Widerruf ihrer Einwilligung, das Recht auf Auskunft, Löschung oder Datenübertragbarkeit (ErwG 30 DGA). Der Verordnungsgeber sieht damit die Wahrnehmung der datenschutzrechtlichen Betroffenenrechte sowie die Übernahme von Einwilligung bzw. Widerruf derselben als mögliches Betätigungsfeld von Datenvermittlungsdiensten an. Gleichzeitig soll der Regelungsbereich der europäischen Datenschutz-Grundverordnung (DSGVO) unangetastet bleiben und die datenschutzrechtlichen Vorgaben im Konfliktfall Vorrang gegenüber den Regelungen des DGA haben (ErwG 4 DGA). Betrachtet man die Regelungen der DSGVO im Einzelnen, zeigen sich mögliche Konfliktpotenziale, die einer treuhänderischen Wahrnehmung von Datenschutzrechten entgegenstehen könnten.

Einwilligung

Soll ein Datentreuhänder im Namen der betroffenen Person eine Einwilligung abgeben, so muss die hierfür notwendige Vollmacht selbst die Anforderungen an eine wirksame Einwilligung erfüllen. Das bedeutet insbesondere, dass die Einwilligung zur Rechteausübung zweckbestimmt und in informierter Weise abgegeben werden muss (Kühling 2021). Die Erteilung einer Blanko-Vollmacht in dem Sinne, dass der Datentreuhänder im Namen der betroffenen Person in jedwede Verarbeitungsszenarien einwilligen kann, ist nicht möglich. Ausnahmen von dem Erfordernis der Bestimmtheit der Einwilligung werden nur dort als zulässig erachtet, wo es um die Einwilligung zur Verarbeitung von personenbezogenen Daten für Zwecke der wissenschaftlichen Forschung

geht.[4] In Erwägungsgrund 33 der DSGVO trägt der Gesetzgeber dem Umstand Rechnung, dass im Forschungskontext der genaue Zweck der Datenverarbeitung zum Zeitpunkt der Datenerhebung häufig noch nicht feststeht. Insofern kann die betroffene Person in derartigen Konstellationen ihre Einwilligung auch im Hinblick auf unbestimmte Forschungszwecke erteilen (broad consent). Vor diesem Hintergrund sind Szenarien denkbar, in denen der Datentreuhänder Datenzugangsentscheidungen trifft, obwohl zum Zeitpunkt der Datenerhebung die genauen Forschungsziele noch nicht feststehen. Eine weitere Hürde im Hinblick auf die datenschutzrechtliche Zulässigkeit von Einwilligungserklärungen ist das Gebot der Informiertheit. Dieses sieht vor, dass die betroffene Person die Auswirkungen der Erteilung ihrer Einwilligung abschätzen können muss (Kühling und Buchner 2020). Hieran fehlt es aber, wenn die einzelnen Verarbeitungsszenarien zum Zeitpunkt der Erteilung noch nicht absehbar sind. Mängel in der Informiertheit der Einwilligung führen zu deren Unwirksamkeit.

Wahrnehmung von Betroffenenrechten

In Bezug auf die Wahrnehmung von Betroffenenrechten können Datentreuhänder eine wichtige Rolle einnehmen. Zu den Betroffenenrechten zählen u. a. das Recht auf Auskunft, Berichtigung, Löschung und Datenübertragbarkeit. Inwieweit Dritte die datenschutzrechtlichen Betroffenenrechte stellvertretend ausüben können, ist umstritten. Befürworter verweisen auf die informationelle Selbstbestimmung der betroffenen Person, die eine Stellvertretung hinsichtlich der Betroffenenrechte gebieten (Kühling 2021). Demgegenüber wird vertreten, dass die Geltendmachung von Betroffenenrechten nicht ohne Modifikation der DSGVO möglich sei (Specht-Riemenschneider et al. 2021). Die Frage, ob und in welchem Umfang die Wahrnehmung von Betroffenenrechten zulässig ist, ist mit einer gewissen Rechtsunsicherheit behaftet. Gleichzeitig wird deutlich, dass die Regelungsbereiche des DGA und der DSGVO nicht eindeutig aufeinander abgestimmt sind. Die im DGA angedachte Verbesserung der Rechtewahrnehmung lässt sich jedenfalls nicht ohne Weiteres mit den Vorgaben der DSGVO vereinbaren.

4.4.2 URHEBERRECHT

Neben dem Datenschutzrecht müssen auch die Vorschriften des Urheberrechtsgesetzes (UrhG) bei der Konzeption und dem Betrieb von Datentreuhandmodellen berücksichtigt werden. Daten können in Form einer Datenbank über die Regelungen des UrhG geschützt sein. Dies betrifft zum einen Datensammlungen, die aufgrund einer schöpferischen Leistung ein urheberrechtlich geschütztes Werk darstellen. Zum anderen wird die Investition in eine Datenbank durch das Leistungsschutzrecht des Datenherstellers geschützt (§§ 87a ff UrhG). In beiden Konstellationen erhält der Rechtinhaber Verwertungsrechte an der Datenbank. Folglich kann anders als bei Einzeldaten auch eine Lizenzierung an Dritte erfolgen. In diesem Kontext könnte ein Datentreuhänder entsprechende Nutzungsrechte an Dritte einräumen oder auf Geheiß des Rechteinhabers gegen

4 Die Verarbeitung von personenbezogenen Daten zu Forschungszwecken erfährt in der DSGVO an mehreren Stellen eine Privilegierung. Eine Weiterverarbeitung zu Forschungszwecken widerspricht beispielsweise nicht dem Grundsatz der Zweckbindung. Es wird in diesem Zusammenhang unterstellt, dass die Weiterverarbeitung mit dem ursprünglichen Zweck der Datenverarbeitung vereinbar ist (Art. 5 Abs. 1 lit. b) DSGVO). Die Verarbeitung von Gesundheitsdaten ist zudem, trotz des grundsätzlichen Verarbeitungsverbots nach Art 9 Abs. 2 lit. j) DSGVO zulässig, sofern hiermit wissenschaftliche Forschungszwecke verfolgt werden und eine entsprechende gesetzliche Erlaubnis zur Datenverarbeitung besteht. Voraussetzung für die Zulässigkeit einer Datenverarbeitung zu Forschungszwecken statuiert Art. 89 DSGVO, der u. a. vorsieht, dass geeignete Garantien für die Rechte und Freiheiten der betroffenen Person vorgesehen werden müssen. Um in den Genuss des datenschutzrechtlichen Forschungsprivilegs zu kommen, muss Klarheit darüber bestehen, ob die beabsichtigte Datenverarbeitung tatsächlich im Zusammenhang mit einer Forschungsaktivität steht. Der Begriff Forschung wird innerhalb der DSGVO nicht definiert. Grundsätzlich wird der Begriff weit verstanden und umfasst neben der akademischen Forschung und Grundlagenforschung auch die Anwendungsforschung und die privatwirtschaftliche Forschung (vgl. ErwG 159 DSGVO). Um eine extensive Beanspruchung des Forschungsprivilegs zu vermeiden, bedarf es im Hinblick auf die wissenschaftliche Tätigkeit einer Unabhängigkeit des Forschenden in der Gestalt, dass allein der wissenschaftliche Erkenntnisgewinn im Vordergrund steht (Weichert: Die Forschungsprivilegierung in der DSGVO(ZD 2020, 18) Weichert 2020a). Damit sind Konstellationen ausgeschlossen, in denen der Prozess der Erkenntnisgewinnung auf wirtschaftliche Zwecke fokussiert (Weichert 2020b). Somit kann sich auch industrielle Forschung auf das Forschungsprivileg berufen, sofern sichergestellt ist, dass keine Einflussnahme auf den Erkenntnisprozess erfolgt oder eine Unterordnung unter wirtschaftliche oder sonstige Interessen ausgeschlossen werden kann.

Verletzungshandlungen vorgehen. Umgekehrt wäre eine Datenvermittlung, etwa in Form einer Vervielfältigung von Datenbanken, unzulässig, wenn hierdurch Urheberrechte Dritter verletzt werden. Zu beachten ist auch, dass Dienste, die auf die Vermittlung urheberrechtlich geschützter Inhalte ausgerichtet sind, keine Datenvermittlungstätigkeit im Sinne des DGA ausüben (Art. 2 Nr. 11 lit. b) DGA). Besteht die Tätigkeit des Datentreuhänders im Kern in der Vermittlung von urheberrechtlich geschützten Datensammlungen, greifen die Vorgaben des DGA nicht ein.

4.4.3 GESCHÄFTSGEHEIMNISSCHUTZ

Der Schutz von Geschäftsgeheimnissen spielt im Kontext von Datentreuhandmodellen eine wichtige Rolle. Dateninhaber werden sensible Unternehmensinformationen nur dann teilen, wenn die notwendigen technischen Schutzmaßnahmen gegeben sind. Daneben müssen die Bedingungen des Datenzugangs- und der Datennutzung rechtssicher gestaltet werden. In Bezug auf Geschäftsgeheimnisse sind dabei die Vorgaben des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG) zu berücksichtigen. Geschäftsgeheimnisschutz besteht nur in Bezug auf Informationen, die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber sind (§ 2 Nr. 1 lit. b) GeschGehG). Hierzu gehören neben technischen Schutzmaßnahmen auch vertragliche Sicherungsmechanismen (Hohn-Hein und Barth 2022). Der Geheimnisinhaber muss auf vertraglicher Ebene alles in seiner Macht stehende tun, um auf die Sicherung des Geheimnisses hinzuwirken (Partsch und Rump 2020). Hinsichtlich der Angemessenheit der Geheimhaltungsmaßnahmen ist der Geheimnisinhaber beweispflichtig. Um gegen Rechtsverletzungen vorgehen zu können, muss er darlegen und nachweisen können, dass die Geheimhaltungsmaßnahmen angemessen waren. Die nicht unerheblichen Anforderungen des GeschGehG gebieten es, dass Datenzugangs- und -nutzungsentscheidungen auf einer soliden vertraglichen Basis zwischen den Parteien vereinbart werden. Dies umfasst die Vorgaben, dass der Datentreuhänder selbst und gegebenenfalls der Datenempfänger zu entsprechenden Geheimhaltungsmaßnahmen verpflichtet wird. Der vertraglichen Ausgestaltung des Treuhandverhältnisses kommt folglich eine große Bedeutung zu.

4.5 Aktuelle Diskussionen zur Weiterentwicklung des regulatorischen Rahmens

Neben dem Data Governance Act werden auch auf nationaler Ebene Handlungsoptionen diskutiert, wie der Gesetzgeber die Entwicklung von Datentreuhandmodellen voranbringen kann. Genannt werden in diesem Zusammenhang vor allem wettbewerbsrechtliche Instrumente, wie die Privilegierung von Datentreuhändern in Form einer Freistellung von kartellrechtlichen Vorschriften. Im Bereich von bestimmten Sektoren, die zwingend einen vertrauenswürdigen Datenaustausch erfordern, wird zudem eine Verpflichtende Zugangsgewährung zugunsten von Datentreuhändern angedacht (Blankertz et al. 2020). Darüber hinaus wird auch eine Verpflichtung zur Gewährung von Datenzugang diskutiert. Zwar ist im Rahmen der 10. Novelle des Gesetzes gegen Wettbewerbsbeschränkungen für spezielle wettbewerbsrechtliche Konstellationen ein entsprechendes Zugangsrecht vorgesehen. Allerdings besteht dieser Anspruch nur im Falle von missbräuchlichem Verhalten durch marktbeherrschende Unternehmen und auch nur, wenn eine entsprechende Feststellung durch das Bundeskartellamt vorliegt. Relevanter dürfte in diesem Zusammenhang der von der EU-Kommission vorgelegte Entwurf des Data Act sein, der Nutzende von Produkten und Dritten ein Recht auf Datenzugang einräumt. Durch die verbesserte Datenverfügbarkeit insgesamt könnten auch neue Einsatzszenarien für Datentreuhänder entstehen.

05

5 UMSETZUNGSKONZEPTE

Datentreuhänder können wie festgestellt eine Reihe unterschiedlicher Funktionen wahrnehmen. Entsprechend ihrer Zusammenstellung sind verschiedene Formen der Ausgestaltung von Datentreuhändern denkbar. Die Grundlage für die Ausgestaltung eines Datentreuhänders bilden dabei fünf entscheidungsrelevante Faktoren (Ruhaak und Kapoor 2022) (siehe Abbildung 2):

Abbildung 2: Entscheidungsrelevante Faktoren für die Ausgestaltung von Datentreuhändern (in Anlehnung an Ruhaak et al. 2021)

Dabei wird deutlich, dass – wie auch im etwas weiter gefassten Diskurs zum Thema „Data Sharing" (Lindner et al. 2021) – ein alleiniger Fokus auf die technische Ausgestaltung von Datentreuhändern und der dahinterstehenden Infrastruktur nicht erfolgsförderlich sein wird. Stattdessen bedarf es einer integriert ausgerichteten Betrachtung der aufgeführten Faktoren und der Ableitung aufeinander abgestimmter technischer und nicht-technischer Lösungsbausteine des jeweils konkreten Datentreuhandmodells. Wie wichtig eine integrierte Herangehensweise jenseits eines reinen Technikfokus zur erfolgreichen Umsetzung von Datentreuhändern und anderen Formen des Datenteilens ist, zeigt eindrücklich die integrierte und interdisziplinäre Ausrichtung des Data Space Support Centre (DSSC), das als Unterstützungsstruktur für Akteure aus der Praxis durch Förderung der Europäischen Union im Herbst 2022 ins Leben gerufen wurde (https://dssc.eu/).

5.1 Anspruchsgruppenanalyse

Sowohl anhand der Literatur (Ruhaak und Kapoor 2022; Lindner et al. 2021) als auch auf Basis der geführten Interviews wird deutlich, dass die erfolgreiche Etablierung von nachhaltig funktionierenden Datentreuhandmodellen stark von der Erfüllung von Bedürfnissen der beteiligten Anspruchsgruppen abhängt. Hierzu zählen insbesondere Umfang, Qualität und Sensitivität der zugrunde liegenden Datenbasis, die Verfügbarkeit der Daten sowie die konkrete Form der nutzbaren Formate. Hinzu kommen anspruchsgruppenspezifische Anforderungen an die technische Sicherheit der zugrunde liegenden Infrastruktur, der akzeptierte Modus der Aufnahme neuer Akteure sowie die zugrunde liegenden Regeln des Zugriffs- und Nutzungsrechtemanagements. Zudem spielen gerade beim Aufbau von Datentreuhändern die relative Größe der beteiligten Akteure und die konkrete Wettbewerbssituation eine herausragende Rolle. Vor dem Hintergrund der Erkenntnis, dass der erfolgreiche Aufbau von Datentreuhändern durch die Existenz mindestens eines oder mehrerer klar abgrenzbarer und mehrwertstiftender Anwendungsfälle erleichtert wird, wird so eine intensive Anspruchsgruppenanalyse erforderlich. Hierzu können beispielsweise Methoden wie etwa das Tangible Ecosystem Design (Tamanini et al. 2020) nützlich sein.

5.2 Governance

Als zweiter wichtiger Baustein zum Aufbau von Datentreuhändern als nachhaltig tragfähiger Organisation gilt es, dessen Governance-Strukturen und -Prozesse im Sinne der Bedürfnisse der beteiligten Akteure vertrauenswürdig zu gestalten. Auf Basis der Literatur und der Interviews wurden dabei folgende organisatorische Elemente bzw. Maßnahmen als besonders förderlich identifiziert.

Festlegung und Kommunikation grundlegender Verhaltensregeln für die Teilnahme am Ökosystem

Ein erster Ansatz ist die im Idealfall auf den Ergebnissen der zuvor genannten Anspruchsgruppenanalyse aufbauende Konzeption, Festlegung und anschließende Kommunikation grundlegender Verhaltensregeln für potenzielle Datengebende und Datennehmende, aber auch für den Datentreuhänder selbst, die in Einklang mit den geltenden rechtlichen Rahmenbedingungen formuliert werden. Diese Grundregeln im Sinne eines Code-of-Conduct beschreiben die Rahmenbedingungen für die Bereitstellung und Nutzung von Daten, aber vor allem auch den Umgang der beteiligten Akteure miteinander. Als zentraler Bestandteil eines Katalogs von Verhaltensregeln kann dabei die Festlegung von legitimen Nutzungszwecken – beispielsweise aufgeteilt im Hinblick auf die Kategorien der wirtschaftlichen Verwertung oder für Forschung und Entwicklung – genannt werden. Um die Überprüfbarkeit der Zweckbindung bei der Datennutzung zu sichern, bedarf es darüber hinaus gegebenenfalls der Festlegung von Kontrollmaßnahmen zu deren Einhaltung und auch Sanktionsmechanismen. Hierunter sind ebenfalls Prozesse zur Streitschlichtung beteiligter Akteure sowie interne oder gegebenenfalls auch externe Auditierung zu subsumieren (Sundararajan 2020). Zudem sollten die Regeln und Mechanismen zur Gewährleistung einer für den jeweiligen Anwendungsfall erforderlichen Datenqualität aufgeführt werden. Vor dem Hintergrund der Tatsache, dass Daten sowohl in ihrer Sensibilität als auch hinsichtlich der geplanten Nutzungen und den jeweils damit verbundenen Bedingungen große Unterschiede aufweisen können, kann es sich hier anbieten, verschiedene Stufen von Qualitätsgarantien vorzusehen (Rat für Informationsinfrastrukturen 2020). Darüber hinaus sollte klar festgelegt werden, wie und durch wen die Entscheidung zur Datenfreigabe innerhalb des Ökosystems getroffen werden wird. Hier sind verschiedene Formen,

gegebenenfalls auch abhängig von legitimen Zwecken, in unterschiedlichen Konstellationen möglich (Ruhaak und Kapoor 2022):

- individuelle Zustimmung durch die Datengebenden zu jeder einzelnen Anfrage,
- direkte Abstimmung durch alle Datengebenden nach Konsens oder zuvor festgelegten Mehrheitsregeln im Rahmen eines Gremiums,
- Übertragung der Entscheidungsbefugnis an ein spezifiziertes Gremium von Repräsentanten aus dem Kreis der Datengebenden oder
- Übertragung der Entscheidungsbefugnis zur Datenfreigabe auf den Datentreuhänder – nach zuvor spezifizierten Regeln und klar umrissenen Nutzungszwecken.

Darüber hinaus sollten die grundlegenden Verhaltensregeln auch eine transparente Darstellung der durch den Datentreuhänder angebotenen Dienstleistungen und dem damit möglicherweise verbundenen Interesse an der regelbasierten Nutzung der bereitgestellten Datensätze in Einklang mit den geltenden Bestimmungen des DGA sowie den damit verbundenen Geschäfts- und Finanzierungsmodellen enthalten.

Ausgestaltung und Kontrolle konkreter Nutzungsbedingungen und vertragliche Verankerung
Die zuvor aufgeführten Verhaltensregeln bzw. Leitlinien erfordern dann in der Regel in den einzelnen Anwendungsfällen eine vertragliche Präzisierung. Je nach Ausgestaltung des jeweiligen Datentreuhänders können die beteiligten Vertragsparteien und die Aufgaben des Datentreuhänders variieren. Datentreuhänder können zunächst als Vermittlungsinstanz auftreten und ein bilaterales Vertragsverhältnis zwischen Datengebenden und Datennehmenden anbahnen und begleiten. Der Datentreuhänder kann dabei unterstützend Vertragsmuster oder Lizenzvereinbarungen zur Verfügung stellen, um das Vertrauen in die Transaktion zu stärken und die Aufwände für die beteiligten Akteure zu minimieren. Zudem verpflichtet sich der Datentreuhänder gegenüber den datengebenden und datennehmenden Akteuren zur Erbringung der Vermittlungsleistung (z. B. mittels der Bereitstellung der technischen Infrastruktur). In anderen Konstellationen obliegt es dem Datentreuhänder selbst, Entscheidungen über den Datenzugang zu treffen. Dabei ist der Datentreuhänder verpflichtet, die jeweiligen Zugangsentscheidungen gemäß den vorab festgelegten Vertragsbedingungen im Interesse des Datengebenden zu treffen. Die Ausgestaltung der Rollen und Aufgaben wird somit primär durch vertragliche Vereinbarungen festgelegt.

Die vertraglich vereinbarten Nutzungsbedingungen bilden entsprechend die „AGB der Datenökonomie“ (Otto und Burmann 2021), die im Detail regeln, unter welchen Umständen und zu welchem Zweck die bereitgestellten Daten von wem genutzt werden dürfen. Unter Einhaltung der geltenden gesetzlichen Rahmenbedingungen besteht dabei – vor allem im Hinblick auf den Datenaustausch zwischen Unternehmen – eine relativ große Gestaltungsfreiheit. Eine Übersicht über mögliche Aspekte einer entsprechenden Vereinbarung bieten die von der International Data Spaces Association (IDSA) erarbeiteten Regelklassen (Otto und Burmann 2021; Steinbuß 2021):

- Datennutzung erlauben/verbieten,
- Datennutzung beschränken auf Nutzergruppen bzw. Nutzungszwecke,
- Datennutzung bei Eintritt eines bestimmten Ereignisses beschränken,
- Datennutzung innerhalb eines bestimmten Zeitintervalls erlauben,
- Datennutzung n-mal erlauben,
- Daten nach Nutzung löschen und
- Datennutzung protokollieren.

Im Rahmen der Initiative Plattform Industrie 4.0 des BMWK wurden zudem Teilnahmebedingungen für eine Plattform zum Data Sharing zwischen Industrieunternehmen erstellt. Diese Teilnahmebedingungen (Borges et al. 2021) stellen vertragliche Regelungen für Industrie-4.0-Plattformen als Muster dar und beinhalten auch Regelungen zu Datennutzungsrechten. Der dazugehörige Leitfaden und die dazugehörigen rechtlichen Hintergründe erläutern die einzelnen Regelungsinhalte der Musterbedingungen (Plattform Industrie 4.0 2021).

Die Einhaltung der vertraglich vereinbarten Nutzungsbedingungen sollte durch die Einführung geeigneter organisatorischer und technischer Maßnahmen durch den Datentreuhänder gewährleistet werden. Ein hybrider Ansatz ist etwa die Verankerung der Nutzungsbedingungen in der Open Digital Rights Language (ODRL), die eine interoperable Beschreibung, Interpretation sowie die Durchsetzung der vertraglichen Regeln ermöglicht (Otto und Burmann 2021).

5.3 Anreizsysteme

Als weiterer wichtiger Faktor zum Aufbau von Vertrauen durch die organisatorische Ausgestaltung des Datentreuhänders ist die Entwicklung und Umsetzung konkreter Maßnahmen zum Aufbau eines funktionierenden Ökosystems zu nennen. Dabei kann das vorbildhafte Vorgehensmodell Data Trust Lifecycle des britischen Open Data Institute für den Aufbau eines datentreuhand-basierten Ökosystems mit seinen Phasen Konzeption, Entwicklung und Etablierung eines Datentreuhänders herangezogen werden (Hardinges et al. 2019) (siehe Abbildung 3).

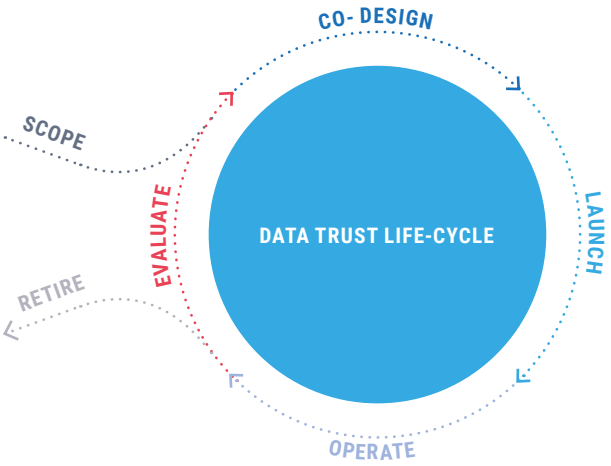

Abbildung 3: Der Data Trust Lifecycle des Open Data Institute (nach Hardinges et al. 2019)

Aufbauend auf der Anspruchsgruppenanalyse (scope) sollten klar abgrenzbare Nutzungsszenarien für einzelne Datentypen innerhalb eines vorab definierten Anwendungsbereichs erarbeitet und mit den Teilnehmenden des Ökosystems vereinbart werden (co-design). Es muss deutlich werden, welche Akteure unter Nutzung eines Datentreuhänders zusammengebracht werden sollen, welchen konkreten Mehrwert eine Teilnahme bietet und welche Maßnahmen zum Schutz der beteiligten Akteure und zum fairen Ausgleich ihrer Interessen durch den Datentreuhänder ergriffen werden. Ein probates Mittel zum Aufbau von Vertrauen und einer nachhaltig wachsenden Anzahl von teilnehmenden Akteuren kann dabei – entgegen der bekannten Logik der schnellen Skalierung von Plattformmodellen und den damit einhergehenden Netzwerkeffekten – laut Interviewpartnerinnen und Interviewpartnern die etwas verlangsamte, organische Einbindung neuer Akteure in das entstehende Ökosystem sein (launch). So kann beispielsweise durch intensive Onboarding-Prozesse zur Gewährleistung der Einhaltung der zuvor geschilderten Verhaltensregeln und möglicher technischer Sicherheitsanforderungen für neue Datengebende oder Datennutzende das Wachstum des entstehenden Ökosystems bewusst gebremst werden. Gleichzeitig dient dieses Vorgehen, insbesondere beim Austausch von Unternehmensdaten, dem Kennenlernen der beteiligten Akteure und schafft in kleinen, aber konkreten Nutzungsszenarien das notwendige Vertrauen für die weitere Skalierung (operate). Eine regelmäßige Überprüfung der Nutzungsszenarien und der Prozesse (evaluate) dient der kontinuierlichen Weiterentwicklung der Plattform, die gegebenenfalls auch zur Aufgabe des Konzepts (retire) führt. Erfahrungen aus der Praxis zeigen, dass solche Ansätze vor allem dann funktionieren, wenn die teilnehmenden Akteure im Hinblick auf Größe und Interesse eher ähnlich sind und es keinen einzelnen dominanten Akteur gibt (Falck und Koenen 2020).

5.4 Geschäfts- und Betriebsmodelle

Zentral für die Vertrauenswürdigkeit eines Datentreuhänders sind die konkret verankerte Trägerschaft der dahinterstehenden Organisation sowie die zugrunde liegenden Geschäfts- bzw. Betriebsmodelle inklusive der erforderlichen Monetarisierungsstrukturen (Otto und Burmann 2021). Die Bereitstellung der für die Vermittlung erforderlichen Infrastruktur sowie die Verwaltung und gegebenenfalls Aufbereitung von Daten sind mit Investitionen und laufenden Kosten verbunden, die im Hinblick auf eine nachhaltige Etablierung des darauf aufbauenden Ökosystems gedeckt werden müssen. Hier sind unterschiedliche Konstrukte denkbar: Einerseits können private Akteure Infrastruktur und Dienste eines Datentreuhänders gegen eine monetäre Kompensation anbieten. Hier sind wiederum zwei Konstellationen denkbar: Entweder wird ein Datentreuhänder als gewinnorientiertes Unternehmen organisiert oder die Gewinnerzielungsabsicht wird durch die Wahl einer entsprechenden Organisationsform – beispielsweise als gemeinnützige GmbH oder gemeinnütziger Verein – ausgeschlossen (Blankertz und Specht-Riemenschneider 2021). Andererseits besteht die Möglichkeit direkter staatlicher Trägerschaft von Datentreuhändern und die damit verbundene Übernahme der erforderlichen Investitionen und der laufenden Betriebskosten – mit oder ohne eine Erhebung von Gebühren. Grundsätzlich sind hier auch Mischformen denkbar.

5.4.1 FINANZIERUNG UND PREISMODELL

Zur Finanzierung des Betriebs stehen Datentreuhändern hierzu grundsätzlich drei Finanzierungsströme zur Verfügung: Neben der Trägerschaft durch ein Partnernetzwerk oder durch einen einzelnen Netzwerkakteur, wie etwa einen Verband zur Realisierung des Plattformbetriebs, ist auch die Finanzierung durch Dritte, etwa in der Form von öffentlichen Fördergeldern, direkte öffentliche Finanzierung oder finanzielle Unterstützungen durch private Stiftungen, zu nennen. Darüber hin-

aus ist auch Generierung von Umsätzen durch die Bepreisung der Datennutzung denkbar. Dabei sind laut Interviews folgende Preismodelle, auch in Kombination, denkbar:

- Subskriptionsmodell oder auch Fixpreismodell für eine bestimmte Zeitspanne und ein festes Set an Datensätzen,
- Paketpreismodell für vordefinierte Datenpakete und eine bestimmte Zeitspanne,
- Pay-per-Use-Modell,
- Mitgliedschaften (freie Nutzung oder Tauschgeschäft),
- Transaktionsgebühren,
- progressives Preismodell je nach Nutzungsintensität der Datenbestände oder
- Gebühren für weitere Dienstleistungen wie etwa Infrastruktur, Datenaufbereitung, Datenanalysen oder Beratung.

Gerade bei Transaktions- oder volumenabhängigen Preismodellen ist besonders auf die Verankerung der Neutralität des Datentreuhänders zu achten, da hier ansonsten ein Interessenskonflikt zwischen der schnellen Vergrößerung des Transaktionsvolumens und dem Schutz der Datengebenden wahrscheinlich ist und somit auch das Vertrauen in die Integrität des Datentreuhänders in Zweifel gezogen werden kann (Blankertz und Specht-Riemenschneider 2021). Darüber hinaus ist aus Sicht der Expertinnen und Experten zu prüfen, ob im Rahmen der geltenden rechtlichen Regelungen, vor allem im Hinblick auf den Data Governance Act und auf Basis der Präferenzen der teilnehmenden Anspruchsgruppen, ein Angebot weiterführender Dienstleistungen, beispielsweise Infrastruktur, Analyse oder Beratung, möglich bzw. erwünscht ist. Denn nimmt der Datentreuhänder eine zu passive Rolle im Zusammenspiel der beteiligten Akteure ein oder kann er seine aktiven Unterstützungsleistungen aufgrund fehlender Refinanzierung nicht aufrechterhalten, wird die Zielerreichung eines für alle Seiten nachhaltig mehrwertstiftenden Datenökosystems zunehmend schwierig. Eine vertikale Integration von Datentreuhändern kann dabei grundsätzlich als unproblematisch eingestuft werden, wenn eine bevorzugte Datennutzung durch den Treuhänder und eine Besserstellung eigener Dienste gegenüber Dritten vermieden wird (Blankertz und Specht-Riemenschneider 2021). Dies kann durch die Schaffung einer belastbaren Governance-Struktur und deren kontrollierte Einhaltung erreicht werden.

Die Einschätzung des finanziellen Wertes von Daten spielt für die Etablierung von Datentreuhändern in der Praxis eine zentrale Bedeutung: Nicht nur können anhand des Wertes der Daten das Missbrauchspotenzial eingeschätzt und in Relation entsprechend angemessene Sicherungsmaßnahmen umgesetzt werden, sondern der Wert kann auch eine zentrale Größe für die Etablierung tragfähiger Geschäfts- bzw. Betriebsmodelle sein. Eine allgemeingültige Formel zur Berechnung individueller Datenwerte ist zwar noch nicht erkennbar, jedoch können drei Ansatzpunkte mit unterschiedlichen Schwerpunkten identifiziert werden (Spiekermann 2019):

- **Wert für Wiederbeschaffungskosten:** Eine Möglichkeit der Annäherung an den monetären Wert von eigenen oder fremden Datenbeständen bildet die Betrachtung der Kostenseite. Hierzu werden alle Kosten zusammengerechnet, die für die Beschaffung von Dritten beziehungsweise die eigene Erstellung, Speicherung, Pflege, Aufbereitung, Verfügbarmachung und Archivierung der Daten anfallen. So lässt sich dann ein Betrag für die sogenannten Wiederbeschaffungskosten einzelner Datensätze ermitteln.

- **Nutzwert-Berechnung:** Daneben ist es möglich, den finanziellen Wert von Daten über die sogenannte Nutzwert-Methode zu berechnen. Hierbei werden nicht wie zuvor beschrieben die Kosten für die Beschaffung bzw. Sammlung der Daten selbst herangezogen, sondern die Potenziale bewertet, die sich mit der Nutzung der Daten ergeben. Zentrale Bewertungskriterien sind hier beispielsweise Prozessoptimierungen und dadurch bedingte Kosteneinsparungen. Dieses Verfahren findet bereits Anwendung bei Ermittlung immaterieller Vermögenswerte wie etwa Lizenzen oder Patenten.
- **Marktwert:** Während die beiden zuvor genannten Ansätze aus unterschiedlichen Perspektiven die Innensicht der jeweils handelnden Akteure repräsentieren, folgt der Ansatzpunkt des Marktwertes der Bereitschaft externer Akteure, tatsächlich für die Nutzung angebotener Datenbestände zu bezahlen. Durch die steigende Verfügbarkeit von Daten auf allen verschiedenen Plattformen und Marktplätzen gibt es hier vermehrt Vergleichsangebote, die zur Ermittlung eines Marktwertes genutzt werden können.

Jeder der drei genannten Ansatzpunkte kann, auch in Kombination, für die Realisierung von Datentreuhändern relevant werden. Dies gilt insbesondere für die Umsetzung eines fairen Interessensausgleichs zwischen Datengebenden und Datennehmenden inklusive der möglichen Monetarisierung einzelner Datentransaktionen, für die Festlegung der erforderlichen Schutzniveaus durch den Datentreuhänder und insbesondere für die initiale Beratung von potenziellen Datengebenden als Teil des gegebenenfalls erforderlichen Onboarding-Prozesses.

5.4.2 PRIVATE TRÄGERSCHAFT

Angesichts des Zwangs zur Wirtschaftlichkeit, denen privatwirtschaftliche Datentreuhänder unterworfen sind, wird diesem Modell in den Interviews eine höhere Agilität und stärkere Bedarfsorientierung gegenüber den beteiligten Akteuren attestiert. Gleiches gilt für den grundsätzlich stärker ausgeprägten Willen zur Förderung eines nachhaltigen Datenökosystems, da hiermit eine gesteigerte Attraktivität des Datentreuhänders als Plattform und folglich höhere finanzielle Erlöse verbunden werden (Blankertz und Specht-Riemenschneider 2021). Aufgrund hoher anfänglicher Investitionskosten für die Bereitstellung der erforderlichen Infrastruktur für den Datenaustausch und insbesondere des zeitaufwendigen und kostenintensiven Ökosystemaufbaus (ZVEI 2022) in Verbindung mit einem stark restriktiven Datenschutzrecht und vor allem den noch herrschenden Unsicherheiten im Hinblick auf die Realisierbarkeit ergänzend monetarisierbarer Dienstleistungen des Datentreuhänders im Lichte des DGA wird die Etablierung nachhaltiger Geschäfts- und Finanzierungsmodelle durchaus kritisch diskutiert. Zudem könnte nach Einschätzung der Expertinnen und Experten das Angebot konkreter Dienstleistungen durch den Datentreuhänder und das damit einhergehende starke wirtschaftliche Verwertungsinteresse seitens des Datentreuhänders ein fundamentales Hindernis für den Aufbau von Vertrauen der Datengebenden und Datennehmenden in die Neutralität der Plattform sein. Hier muss in jedem Fall eine Abwägung erfolgen, welche Service-Angebote benötigt und akzeptiert werden.

5.4.3 STAATLICHE TRÄGERSCHAFT

Gerade etwa in der Aufbauphase kann eine stärkere finanzielle Beteiligung der öffentlichen Hand förderlich für die erfolgreiche Etablierung des Datentreuhänders sein (Schneider 2022). Die positiven Effekte gehen dabei über die rein monetäre Unterstützung hinaus. Die staatliche Trägerschaft bzw. die Trägerschaft durch vorwiegend öffentlich finanzierte Forschungseinrichtungen kann laut Interviews für die potenziellen Datengebenden und Datennutzenden auch einen erheblichen Vertrauensvorschuss in den Datentreuhänder darstellen und damit seine Akzeptanz erhöhen.

Darüber hinaus wird die Möglichkeit der Etablierung staatlicher Treuhandstellen als Instrument der Wettbewerbs- oder Innovationspolitik als potenziell relevant diskutiert: Ein derartiges Eingreifen des Staates, vor allem in Form von Datenteilungspflichten, bedarf dabei für den jeweiligen Sektor einer klaren Rechtfertigung. Ein staatlich getragener oder zumindest staatlich zertifizierter Datentreuhänder könnte aber hier gerade in Märkten mit hoher Marktmacht und der damit verbundenen Konzentration verfügbarer Daten einzelner Teilnehmer eine für Wettbewerb und Innovationskraft förderliche Wirkung entfalten (Blankertz et al. 2020). Auf der anderen Seite kann kritisch angeführt werden, dass Datentreuhänder in staatlicher Trägerschaft aufgrund eventuell fehlender Agilität und Technologienähe, Infrastruktur und Dienste nicht bedarfsgerecht an die Bedürfnisse der relevanten Akteursgruppen anpassen können. Zudem werden von manchen Interviewpartnerinnen und Interviewpartnern für staatlich getragene Datentreuhänder mögliche Machtkonzentrationen beim Staat und damit einhergehende Missbrauchspotenziale befürchtet. Gerade in den Anwendungsfällen jedoch, in denen der Staat selbst sensible, aber auch für Forschung und Wirtschaft hoch relevante Daten hält und bisher nicht oder nur rudimentär zur Verfügung stellt, könnten Datentreuhänder staatlicher Stellen aber auch eine positive Wirkung entfalten bzw. könnte die Mitwirkung staatlicher Stellen an hybriden, gemeinsam mit der Privatwirtschaft getragenen Modellen eine integrative Lösung darstellen.

Öffentlich getragene Datentreuhänder
Ein Praxisbeispiel für ein im Aufbau befindliches Datentreuhandmodell, das vorerst staatlich getragen wird, ist das Projekt EuroDaT – European Data Trustee. Zielstellung des öffentlich geförderten Vorhabens ist der Aufbau eines Datentreuhänders für hoch relevante und gleichzeitig höchst sensible Finanz- und Finanztransaktionsdaten. Mit seiner Trägerschaft will das Land Hessen während der Aufbauphase die Neutralität des Datentreuhänders sicherstellen (www.eurodat.org). Das Zentrum für Krebsregisterdaten des Robert Koch-Instituts soll zukünftig auch klinische Daten aus den Krebsregistern als Datentreuhänder bereitstellen (Robert Koch-Institut 2021). Ebenfalls in einem Treuhandmodell plant das Kraftfahrt-Bundesamt die Bereitstellung von Daten des Zentralen Fahrzeugregisters für die Forschung (Kraftfahrt-Bundesamt 24.05.2022).

5.4.4 SONDERFORM DATENGENOSSENSCHAFT

Jenseits der Trägerschaft des Datentreuhänders durch einen staatlichen oder privatwirtschaftlichen Akteur sind aber auch alternative Formen der gemeinschaftlichen Trägerschaft denkbar. Hier werden in der aktuellen Diskussion allen voran genossenschaftliche Modelle angeführt. Genossenschaften sind dabei eine Organisationsform, in der sich Mitglieder zusammentun, um kollektive Entscheidungen über gemeinsame Vermögenswerte zu treffen. Dabei gelten folgende Grundprinzipien: Die Mitgliedschaft basiert auf einer freiwilligen Entscheidung der handelnden Akteure und der Zugang steht grundsätzlich allen Akteuren offen. Die Mitglieder treffen nach zuvor festgelegten Mehrheitsregeln demokratische Entscheidungen. Dabei zählt das Prinzip der Wahlgleichheit und die Stimmen der teilnehmenden Mitglieder haben unabhängig von ihrer Größe das gleiche Gewicht. Werden durch den Betrieb der Genossenschaft finanzielle Überschüsse erwirtschaftet, werden die Erlöse an die Mitglieder ausgeschüttet. Darüber hinaus erlaubt die Struktur der Genossenschaft den Mitgliedern, ihre Ressourcen und Vermögenswerte in Einklang basierend auf den eigenen Werten und gemäß kollektiv festgelegten Regeln zu verwalten. Darüber hinaus sind Streitschlichtungsmechanismen ein wichtiger Bestandteil von Genossenschaften

(Ruhaak und Kapoor 2022). Datengenossenschaften werden entsprechend als kollektive Organisationsform verstanden, in denen sich Einzelpersonen und/oder Unternehmen zur Verwaltung und Nutzung von Daten als immateriellem Vermögenswert zusammenschließen, aber auch staatliche Stellen als Mitglieder aktiv werden können. Der europäische Gesetzgeber sieht Datengenossenschaften dabei vor allem als besonders nützliche Instrumente zur Verbesserung der Verhandlungsposition von Einzelpersonen gegenüber datennutzenden Unternehmen und für die Integration von kleineren und mittleren Unternehmen in Wertschöpfungsprozesse der Datenökonomie an (Europäische Union 2022). Insbesondere für kleine und mittelständische Unternehmen bietet eine Datengenossenschaft im Sinne eines gemeinschaftlich getragenen Datentreuhänders erkennbare Vorteile: Durch gezielte Kooperationen mit anderen Unternehmen entlang der Wertschöpfungskette – etwa im Kontext von IoT-Ökosystemen einzelner Branchen – können gemeinsam Daten· innovation gefördert und datengetriebene Wertschöpfungspotenziale gehoben werden, ohne dass die beteiligten ihre Selbstständigkeit aufgeben müssen oder abhängig von großen Plattformbetreibern werden (Weber et al. 2021).

Aufgrund der durch die Mitglieder gestalteten Regeln besteht hier einerseits grundsätzlich der Vorteil der erhöhten Flexibilität bei der Ausgestaltung des Leistungsumfangs des Datentreuhänders und durch die gemeinsame Eigentümerschaft sowie die kollektiv steuerbaren Rahmenbedingungen der Datenbereitstellung können zusätzliche Anreize zur Mitwirkung für die Mitglieder geschaffen werden.

Andererseits sind genossenschaftliche Modelle im Hinblick auf die erfolgreiche Etablierung sehr voraussetzungsvoll und zeitaufwendig: So müssen eine Vielzahl von Akteuren mit teilweise stark divergierenden Interessen zur Mitwirkung überzeugt und die Regeln des Ökosystems kollektiv abgestimmt werden.

Datengenossenschaften im Pilotbetrieb

Es sind schon erste Ansätze zur Umsetzung von Datengenossenschaften in unternehmerischen Kontexten erkennbar, wie etwa das vom Ministerium für Wirtschaft, Arbeit und Tourismus Baden-Württemberg geförderte Pilotprojekt „Datengenossenschaften: Digitale Datenräume zur Kooperation von KMUs" (https://www.datengenossenschaft.com/, Weber et al. 2022b). Grundlage für die Projektergebnisse war die pilothaften Umsetzung von drei Datengenossenschaften im Kontext unterschiedlicher unternehmerischer Wertschöpfungsketten. Dabei wurde das Konzept der Datengenossenschaft im Kontext des datenbasierten Managements von Kühl- und Schmierstoffen (KSS) im produzierenden Gewerbe, für das Risikomanagement für holzverarbeitende Betriebe und im Zusammenhang der verbesserten Energieeffizienz industrieller Wäschereibetriebe getestet. Die zentralen Erkenntnisse der pilothaften Umsetzungen sind in der Form eines Verrechnungskonzepts für Leistungen und Services einer Datengenossenschaft (Hörnig und Kühlem 2022) und eines Leitfadens, der die Initiierung und Ausgestaltung von Datengenossenschaften in der Praxis erleichtern soll (Weber et al. 2022a), öffentlich verfügbar.

5.5 Technik und Standards

Aufbauend auf einer vertrauensfördernden Organisationsstruktur und den darin festgehaltenen Regeln für die Bereitstellung von Daten und deren regelbasierte Nutzung, muss ein Datentreuhänder eine geeignete technische Infrastruktur zur Verfügung stellen. Die Auswahl und Implementierung geeigneter technischer Elemente stellt damit einen zentral wichtigen Erfolgsfaktor für das nachhaltige Vertrauen der Datengebenden und Datennehmenden sowohl in den Datentreuhänder als auch in das entstehende Datenökosystem dar. Eine vertrauensfördernde technische Architektur sollte dabei aber nachfolgend aufgeführte Eigenschaften der zur Verfügung gestellten Datenbestände grundsätzlich gewährleisten können (Collovà et al. 2021):

- **Sicherheit und Schutz:** Nur Akteure in den dafür vorgesehenen Rollen sollen Daten bereitstellen, sie bearbeiten oder nutzen können. Darüber hinaus sollte durch geeignete Steuerungs- und Überwachungsmechanismen sichergestellt werden, dass Daten nicht versehentlich oder wegen unzulässiger Bearbeitung in ihrer Form oder ihrem Inhalt verändert werden, sodass sie nicht mehr erkennbar oder nutzbar sind.
- **Langlebigkeit:** Die betreffenden Daten sollten durch die Realisierung geeigneter technischer Maßnahmen innerhalb vordefinierter Zeitspannen tatsächlich zur regelbasierten Nutzung zur Verfügung stehen.
- **Zuverlässigkeit:** Es sollte technisch gewährleistetet werden, dass bereitgestellte Daten überwacht und nicht zugelassene Daten zurückgewiesen werden. Diese Zulassung betrifft sowohl die Qualität der Inhalte als auch Mechanismen zur Verhinderung krimineller technischer Aktivitäten.
- **Standardisierung:** Die verwendeten technischen Komponenten sollten sicherstellen, dass Daten in bekannten und durch die beteiligten Akteure verstandenen Formaten effizient austauschbar sind.
- **Durchsuch- und Nachvollziehbarkeit:** Zudem bedarf es geeigneter technischer Elemente, die es einerseits Datennutzenden ermöglichen, innerhalb der Gesamtmenge der verfügbaren Daten die für sie oder ihn relevanten Bestände zu identifizieren und andererseits die vom Treuhänder getätigten Datenoperationen, etwa für die Qualitätssicherung, nachvollziehbar zu dokumentieren.

Die hier angegebenen Eigenschaften vertrauenswürdiger Datenräume sichern direkt oder indirekt die Erfüllung der Bedürfnisse der Teilnehmenden des durch den Datentreuhänder geförderten Ökosystems. Vor dem Hintergrund ihres hohen Abstraktionsgrads ist für die Ausgestaltung von Datentreuhändern die Operationalisierung einzelfallspezifisch relevanter, technischer Komponenten erforderlich. Die Bandbreite denkbarerer technischer Elemente für IT-Architekturen konkreter Datentreuhänder ist dabei sehr weit gefächert. In Anlehnung an die technischen Bausteine der International Data Spaces Association können technische Elemente aber generell unter drei große Kategorien subsumiert werden (Nagel und Lycklama 2021):

- **Datensouveränität:** bestehend etwa aus technischen Elementen des Identitätsmanagements, der Zugangs- und Nutzungskontrolle sowie technischen Komponenten zur Realisierung eines verlässlichen Datenaustauschs.
- **Dateninteroperabilität:** bestehend etwa aus technischen Elementen wie Schnittstellen, Datenformaten sowie Methoden zum Nachvollzug der Datennutzung.
- **Datenwertschöpfung:** bestehend etwa aus Metadatenformaten, Datensuchfunktionen und Methoden zur automatisierten Kontrolle und Abrechnung der Datennutzung.

Aus dem Kontext der Debatte um die Etablierung europäischer Datenräume sind verschiedene Initiativen erkennbar, die bereits mit der Entwicklung und Streuung von entsprechenden technischen Komponenten begonnen haben. Zu nennen sind hier etwa die Plattform Industrie 4.0, Connecting Europe Facility Digital, FIWARE und auch die International Data Spaces Association (Nagel und Lycklama 2021). Insbesondere die Referenzarchitektur der IDSA (Otto et al. 2019b) beschreibt in einem im europaweiten Vergleich bereits sehr weit fortgeschrittenen Modell eine Vielzahl von unterschiedlichen Komponenten, die technisch für einen sicheren und vertrauensvollen Datenaustausch erforderlich sind. Zentrale technische Bausteine sind unter anderem die Connector-Software zum Anschluss an den entstehenden Datenraum, der Broker als Anwendung für die Suche nach relevanten Datenbeständen und deren vorherige Bereitstellung sowie das sogenannte Clearing House als Abrechnungsdienst. Die Auswahl, Zusammenstellung und Etablierung konkreter technischer Komponenten ist dabei aber immer vom konkreten Anwendungsfall abhängig und sollte gemäß den konkreten Zielen des jeweiligen Datentreuhänders aufbauend auf den Bedürfnissen der konkreten Zielgruppe von Ökosystemteilnehmenden erfolgen. In den nachfolgenden Abschnitten wird der aktuelle Diskussionsstand zu technischen Elementen für einen vertrauensvollen Datenaustausch aufgeführt, die für die Gestaltung von konkreten Datentreuhändern grundsätzlich relevant sein können.[5]

5.5.1 DATENSOUVERÄNITÄT

Von der Zugangs- zur Nutzungskontrolle

Im Kontext der Informationssicherheit umfasst der Begriff der Zugangskontrolle (access control) alle technischen Maßnahmen, die Daten vor unberechtigtem Zugriff schützen und die lediglich die Verfügbarmachung an berechtigte Nutzende gewährleisten. Hier sind in der Praxis verschiedene technische Modellklassen erkennbar: So gibt es unter anderem Modelle der Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC) oder Attribute-based Access Control (ABAC), wobei die beiden letztgenannten Modelle mittlerweile am einschlägigsten sind. Als konkretes Beispiel ist hier der XACML-Standard (eXtensible Access Control Markup Language) anzuführen, der auch im Rahmen der IDSA-Initiative Anwendung finden wird (Steinbuß 2021). Unter dem Begriff Nutzungskontrolle (usage control) wird dagegen eine Erweiterung der Kontrollmechanismen verstanden, durch die auch nach der initialen Zugänglichmachung von Daten deren konkrete Verwendung technisch kontrollierbar bleiben soll. Da es sich im Gegensatz zur Zugangskontrolle nicht um eine binäre Ja-Nein-Entscheidung über die Verfügbarmachung einzelner Datenbestände, sondern um die dauerhafte Überwachung der Einhaltung festgelegter Nutzungsbedingungen geht, ist die technische Umsetzung einer effektiven Nutzungskontrolle noch einmal deutlich herausfordernder, auch wenn hier verschiedene technische Maßnahmen der Verschlüsselung oder die erforderliche Installation von Kontrollanwendungen aufseiten der Datennutzenden denkbar sind.

Hier gehen Datentreuhänder deutlich über die einfacheren Plattformen für Datentransaktionen hinaus: Während Letztere vor allem eine effektive Zugriffskontrolle bereitstellen müssen, können bei den Treuhändern glaubwürdige technische Maßnahmen zur Nutzungskontrolle gemäß zuvor festgelegten Bedingungen ein zentrales Vertrauensmoment bilden. Im Idealfall wird durch die technische Infrastruktur des Datentreuhänders direkt die Einhaltung der rechtlichen Rahmenbedingungen sowie der bilateralen Vereinbarungen zwischen Datengebenden und Datennutzenden kontrolliert.

5 Die aktuelle Arbeitsversion 4.1 der IDS-Referenzarchitektur findet sich auf Github: https://github.com/International-Data-Spaces-Association/IDS-RAM_4_0.

Die Auswahl an bereits verfügbaren oder derzeit in der Entwicklung befindlichen technischen Instrumenten zur Umsetzung einer effektiven Nutzungskontrolle ist groß. So stellt etwa die International Data Spaces Association verschiedene technologische Bausteine bereit oder arbeitet gerade an deren Finalisierung (Steinbuß 2021):

- **MYDATA Control Technologies:** Aufbauend auf dem IND2UCE-Framework für Datennutzungskontrolle des Fraunhofer IESE, soll durch MYDATA die Datensouveränität durch das Monitoring von relevanten Datenströmen, die Maskierung und Anonymisierung von Datenbeständen sowie deren partielle Filterung gestärkt werden.
- **LUCON – Logic Based Usage Control:** Bei LUCON handelt es sich um ein technisches Instrument zur Umsetzung regelbasierter Datennutzung und zur Kontrolle von Datenströmen zwischen Endpunkten innerhalb von Datenökosystemen auf Basis zuvor festgelegter Nutzungsbedingungen. So sollen aufbauend auf Apace Camel Datensendungen kontrolliert und präferenzbasiert durchgeführt werden.
- **Degree (D°):** Anders als bei MYDATA und LUCON geht es bei Degree (D°) nicht um die effektive Kontrolle bestehender Datenaustauschprozesse, sondern es handelt sich um eine domänenspezifische Programmiersprache zur Entwicklung von Anwendungen zur Datenverarbeitung (sogenannte Data Apps). Dadurch soll die Implementierung einer effektiven Nutzungskontrolle für Daten direkt Teil des Codes der verarbeitenden Anwendungen werden. Grundlage ist die Programmiersprache Java.

Weitere technologische Gestaltungsoptionen für eine Nutzungskontrolle sind etwa der sogenannte Open Policy Agent (Eknert 2021) der Cloud Native Computing Foundation oder die Kontrollinstrumente der SOLID-Initiative (Steinbuß 2021).

Effektive Methoden der Pseudonymisierung bzw. Anonymisierung von Daten

Dazu kommen für eine effektive Nutzungskontrolle technische Methoden zur Pseudonymisierung bzw. Anonymisierung der durch die Datengebenden bereitgestellten Daten. Die Anonymisierung ist die derartige Veränderung von Daten, dass sie nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand wieder der ursprünglichen Datenquelle zugeordnet werden können. Bei der Pseudonymisierung wird der Name oder ein anderes Identifikationsmerkmal des Datengebenden ersetzt, um die Feststellung der Identität der Datenquelle auszuschließen oder wesentlich zu erschweren. Zur Förderung von Vertrauen der Datengebenden kann ein Datentreuhänder sowohl Verfahren zur Pseudonymisierung als auch zur Anonymisierung einsetzen (Jäschke et al. 2018).

Zum Zweck der Pseudonymisierung können kryptografische Techniken wie Hashing oder Verschlüsselung genutzt werden, um aus Ursprungsdaten Pseudonyme abzuleiten. Andere Verfahren setzen auf zufallsgenerierte oder manuell erstellte Werte, um Pseudonyme und die damit verknüpften Nutzdaten von den Vertrauensdaten zu separieren. Grundsätzlich sind dabei auch Kombinationen unterschiedlicher Techniken möglich. Pseudonymisierte Daten bieten dabei oft einen akzeptablen Kompromiss zwischen der Erhaltung der Nutzbarkeit der Daten auf der einen Seite und dem Schutz sensibler Datenbestände auf der anderen Seite. Die Verwendung von Pseudonymen ist besonders für Anwendungen interessant, bei denen für die Datenanalysen eine eindeutige, differenzierte Zuordnung zu Personen oder anderen schützenswerten Identitäten wie Unternehmen, aber keine Kenntnis der dahinterliegenden realen Identitäten erforderlich ist. Für solche Fälle kann die Erzeugung von Pseudonymen auch über einen Datentreuhänder im Sinne einer Trusted-third-Party im Hinblick auf eine Funktionstrennung realisiert werden: Der Datentreuhänder sorgt

dafür, dass der Datenempfänger alleine die entkoppelten Pseudonyme keiner Realidentität mehr zuordnen kann. Dies setzt allerdings ein hohes Maß an Vertrauen in Integrität und Sicherheitskompetenzen des Datentreuhänderdienstes voraus, da durch die Einnahme der Schlüsselposition ein besonders hohes Risiko eines Machtmissbrauchs im eigenen Interesse besteht und Lücken in der Datensicherheit besonders schwerwiegend wirken (Aichroth et al. 2020). Zudem kann kritisch angeführt werden, dass in Anwendungsbeispielen mit wendigen Datengebenden und eher einzigartigen Datensätzen sowie in Verbindung mit einer wachsenden Menge an verfügbaren Daten zur Verschneidung mit pseudonymisierten Datenbeständen die Rückbeziehbarkeit immer eine reale Bedrohung für die Vertrauenswürdigkeit des gesamten Datentreuhänderdienstes darstellt.

Ziele der Anonymisierung von personen- oder auch organisationsbezogenen Daten (Jäschke et al. 2018) sind die Verhinderung der Zuordnung eines ganzen Datensatzes (idendity disclosure) oder einzelner Einträge eines Datensatzes (attribute disclosure) und die Rückverfolgbarkeit der Integration einzelner Personen oder Organisationen als Teil größerer Datenbestände (membership disclosure). Grundsätzlich ist auch hier eine Vielzahl von technischen Verfahren bekannt, mit denen Daten anonymisiert werden können. Die Auswahl der effektivsten Methode hängt dabei maßgeblich von dem Format der zu schützenden Daten sowie dem Nutzungszweck inklusive der damit verbundenen Frage nach der Vertrauenswürdigkeit der Partei ab, die die Daten nutzen möchte. Je nach Anwendungsfall können statische, dynamische oder interaktive Verfahren genutzt werden. Neben der technischen Eignung des Anonymisierungsverfahrens sollte immer untersucht werden, ob das Verfahren geeignet ist, alle erkennbaren Risiken für Personen oder Organisationen effektiv zu reduzieren, deren Daten anonymisiert werden sollen. Alle Parameter des Anonymisierungsverfahrens sollten anhand nachvollziehbarer und transparenter Kriterien gewählt werden. Hinsichtlich des Schutzniveaus bei gleichzeitig guter Nutzbarkeit der Daten können jedoch die Anonymisierungsverfahren t-Closeness und Differential-Privacy als grundsätzlich besonders effektiv eingestuft werden. Das Ziel von t-Closeness besteht darin, den möglichen Datengewinn eines Angreifers in Bezug auf die sensitiven Teilelemente des Datensatzes zu reduzieren. Durch das Verfahren sollen Informationen über den Zusammenhang von Daten, die eine Rückverfolgbarkeit auf Personen oder Unternehmen ermöglichen, mit sensitiven Attributen reduziert werden. Technische Maßnahmen, die dem Konzept der Differential Privacy folgen, zeichnen sich durch die Zugabe einer zufallsgenerierten Änderung des Datenbestandes im Sinne eines intendierten „Rauschens" aus. Bei Differential-Privacy-Verfahren ist lediglich darauf zu achten, dass durch die gewollte Veränderung der Daten keine so große Verfälschung eintritt, dass die Datenbestände am Ende für den Datennutzenden unbrauchbar werden. Andere Methoden zur Anonymisierung können auch genutzt werden, weisen aber etwa im Fall der Verfahren k-Anonymität und l-Diversity ein zu hohes Risiko der Zuordenbarkeit von einzelnen Datengebenden auf oder nehmen etwa beim sogenannten Slicing von Datenbeständen eine zu starke Verfälschung der Rohdaten und eine damit einhergehende Verminderung der Datenqualität in Kauf (Jäschke et al. 2018; Aichroth et al. 2020).

Ausgestaltung des Datenzugangs und der Dateninfrastruktur

Zur Steigerung der Datensouveränität der Datengebenden muss darüber hinaus die konkrete Ausgestaltung des Datenzugangs und der dafür erforderlichen Infrastruktur durch den Datentreuhänder in den Blick genommen werden. Bei der Konzeptionierung, technischen Entwicklung und Implementierung eines Datentreuhänders muss entsprechend eine wesentliche Frage gestellt werden: Wo sollen die durch die Datengebenden bereitgestellten Daten gespeichert werden? Durch welche Art von technischer Infrastruktur des Datentreuhänders am besten ein vertrauenswürdiger Datenzugang sichergestellt werden kann, hängt vom Einzelfall ab. Die Umsetzung in

der Praxis sollte sich im konkreten Einzelfall sowohl nach der Sensibilität der Daten und dem Nutzungszweck als auch nach der Zusammensetzung der am Ökosystem teilnehmenden Akteure als Datengebende und Datennehmende richten (Blankertz 2021). Dabei stehen die Generierung von Skaleneffekten, die Vermeidung von Interessenkonflikten und potenzieller Machtmissbrauch sowie Sicherheitsaspekte im Spannungsverhältnis zueinander (Blankertz et al. 2020).

Zentrale Datenhaltung. Bei der zentralen Speicherung werden die durch die Datengebenden bereitgestellten Daten direkt durch den Datentreuhänder auf seiner eigenen Infrastruktur gespeichert. Entsprechend ist der Datentreuhänder direkt dafür verantwortlich, den Zugriff auf die angefragten Datenbestände zu realisieren sowie die Sicherheit und dauerhafte Verfügbarkeit der Daten zu gewährleisten. Eine zentrale Speicherung beim Datentreuhänder ermöglicht grundsätzlich eine effektivere und weniger aufwendige Verwaltung der Daten innerhalb des jeweiligen Ökosystems sowie die regelbasierte Analyse zum Nutzen der Ökosystemteilnehmenden, ist aber auch mit höheren Risiken verbunden: Handelt es sich etwa um personenbezogene Daten, ist der Datenschutz schwieriger zu gewährleisten, wenn Daten direkt und unverschlüsselt mit einer Datentreuhand geteilt werden. Außerdem kann durch die Zusammenführung großer Datenmengen eine Machtposition für den Datentreuhänder entstehen, die einen Missbrauch der eigenen Position fördern kann. Zudem ist das Sicherheitsrisiko gegenüber externen Angriffen bei zentral vorgehaltenen Daten größer, da der potenzielle Schaden bei einer zentralen Datensammlung deutlich höher ausfällt als bei einer dezentralen Ablage (Blankertz 2021). Diese Risiken müssen entsprechend durch ergänzende technische sowie auch organisatorische Maßnahmen adressiert und an die Teilnehmenden des Ökosystems transparent kommuniziert werden, um hier kein Vertrauensproblem entstehen zu lassen.

Dezentrale Datenhaltung. Bei einer dezentralen Datenhaltung gibt es die Möglichkeit, die Daten lediglich punktuell über den Datentreuhänder zugänglich zu machen oder die Daten in nicht rekonstruierbaren Elementen temporär zusammenzuführen – wenngleich die hierfür erforderlichen Technologien ungleich aufwendiger umsetzbar sind als bei einer zentralen Speicherung (Blankertz 2021). Weitere potenzielle technische Handlungsoptionen sind laut Interviews durchsuchbare Metadatenkataloge des Datentreuhänders inklusive der Abwicklung des eigentlichen Datenaustauschs direkt zwischen Datengebenden und Datennutzenden, die Bereitstellung der Möglichkeit von Zero-Knowledge-Proofs durch den Datentreuhänder. Außerdem kann durch den Datentreuhänder technisch ein dezentraler Datenzugang über die Schaffung gesicherter Container für die Analyse der bereitgestellten Daten durch zuvor durch den Datennutzenden gesendete Analyseprogramme oder KI-Algorithmen (compute to data) bzw. verteilte Verfahren des Maschinenlernens (federated learning) bereitgestellt werden (Rat für Informationsinfrastrukturen 2021). Grundsätzlich sind für die dezentrale Datenhaltung auch Distributed-Ledger-Technologien anwendbar – auch wenn hier in den geführten Interviews deutliche Zweifel an der Sinnhaftigkeit angeführt wurden, die vor allem aufgrund einer mangelhaften Skalierbarkeit ohne hohe negative externe Effekte zurückzuführen sind.

Entsprechend sind für beide Arten der Datenhaltung sowohl gute Argumente als auch potenziell vertrauenshemmende Aspekte erkennbar. Je nach konkretem Anwendungsfall und den Gegebenheiten aufseiten der Ökosystemteilnehmenden sind demnach auch hybride Modelle aus zentraler und dezentraler Datenhaltung möglich. So können die Bedürfnisse der Ökosystemteilnehmenden

flexibler adressiert werden, technisch weniger weit entwickelte Akteure leichter eingebunden werden und gegebenenfalls unterschiedliche Datentypen als vertrauensschaffende Maßnahme an unterschiedlichen Orten gehalten werden.

Zertifizierte Informationssicherheit
Um Unsicherheiten bei (potenziellen) Ökosystemteilnehmenden, insbesondere hier der Datengebenden, weiter zu reduzieren und Vertrauen in die Gewährleistung adäquater Sicherheitsstandards durch den Datentreuhänder aufzubauen, kann gegebenenfalls auch eine externe Zertifizierung der IT- und Informationssicherheit ein wichtiges Element darstellen. Als mögliche Zertifizierungsoptionen für Datentreuhänder können hier die internationale Norm für das Informationssicherheits-Managementsystem ISO/IEC 27001, das internationale Rahmenwerk für die IT-Governance COBIT (Control Objectives for Information an Related Technology), der Kriterienkatalog Cloud Computing C5 des Bundesamts für Sicherheit in der Informationstechnik oder die SOC-Prüfung (System and Organization Controls) des American Institute of Certified Public Accountants angeführt werden (Naybzadeh 2021; Klotz 2019). Zwar werden bei derartigen Zertifizierungsverfahren auch nichttechnische Aspekte wie etwa physische Zutrittskontrollen zu den Räumlichkeiten der informations- und datenverarbeitenden Organisation adressiert, aber der Fokus der Zertifizierungskriterien liegt dabei zumeist auf sicheren digitalen Infrastrukturen, Netzsicherheit, dem sicheren Austausch von Daten und dem Schutz vor externen Angriffen. Als umfangreiche Darstellung der technisch und gegebenenfalls auch organisatorisch umzusetzenden Schutzmaßnahmen kann in diesem Zusammenhang der Anhang A der ISO/IEC 27001 angeführt werden (Kersten et al. 2021).

5.5.2 DATENINTEROPERABILITÄT

Die Gewährleistung von Interoperabilität ist eine zentrale Aufgabe für Datentreuhänder. Nur so können Daten innerhalb des entstehenden Ökosystems effektiv und effizient genutzt werden (Shiohira und Dale-Jones 2019). Der Begriff der Interoperabilität ist dabei nicht eindeutig definiert und kann sowohl eher eng im Sinne einer technischen Interoperabilität – ausgestaltet in einer interoperablen technischen Infrastruktur sowie Datenformaten, Metadaten und Taxonomien – als auch eher breit im Sinne einer Offenheit und einem semantischen Verständnis der handelnden Akteure gegenüber Austausch von Daten verstanden werden (Collovà et al. 2021). Zusammenfassend kann Dateninteroperabilität entsprechend als Fähigkeit technischer Systeme sowie deren Nutzerinnen und Nutzer beschrieben werden, Daten einfach und effektiv auszutauschen und aus den geteilten Daten einen Mehrwert zu generieren. Wenngleich organisatorische Maßnahmen zur Verbesserung der Kollaboration und Schaffung neuer Anreize zur Mitwirkung am Ökosystem sowie zur Verbreitung von Wissen und Know-how innerhalb des Ökosystems hier einen wichtigen Baustein für die Schaffung von Vertrauen und damit dem Willen zur Etablierung tatsächlicher interoperabler Systeme und Prozesse darstellen (Goldstein et al. 2018), bilden die technischen Aspekte die Grundlage für die tatsächliche Umsetzung in der Praxis.

Vorgehens- und Referenzmodelle
Als nützliches Vorgehensmodell zur Adressierung beider Perspektiven auf dem Weg zu einem interoperablen Datenökosystem kann hier das GSBPM-Modell (Generic Statistical Business Process Model) der Wirtschaftskommission für Europa der Vereinten Nationen angeführt werden (Shiohira und Dale-Jones 2019; Vereinte Nationen 2021). Jedoch enthält das GSBPM-Modell noch keine technischen Spezifikationen von Systemen oder Datenformaten.

Hier geht das Referenzarchitekturmodell der International Data Spaces Association einen Schritt weiter und bietet neben einem generellen Governance-Modell und einer Implementationsstrategie für Datenräume auch technische Standards zur Gewährleistung von Interoperabilität. So soll für Unternehmen im Datenraum Datensicherheit, Datenschutz und Datensouveränität unter gleichen Wettbewerbsbedingungen gewährleistet werden, indem Vorgaben zur Ausgestaltung vertrauenswürdiger Datenräume und die dafür erforderlichen Zugangspunkte klar festgelegt werden. Die Schaffung von Vertrauen zwischen den verschiedenen Akteuren ist dabei zentrales Ziel der IDSA. Die Bereitstellung und Nutzung von Daten mittels des in der Praxis umzusetzenden Referenzarchitekturmodells soll dabei auf Basis von Datensouveränität der Datengebenden, Partizipation, Offenheit und einer föderierten Infrastruktur erfolgen (Collovà et al. 2021). Obwohl das Engagement der IDSA nicht dezidiert auf die Etablierung von Datentreuhändern abzielt, spiegeln viele Elemente des Referenzrahmens die Vorteile wider, die auch durch datentreuhandbasierte Ökosysteme realisiert werden können. Durch die breite Unterstützung der IDSA durch sowohl Forschungseinrichtungen als auch vor allem zahlreiche Industriepartner sehen die Initiatoren hier eine realistische Chance, dass sich das IDS-Referenzarchitekturmodell als De-facto-Marktstandard für den souveränen Austausch von Daten etablieren wird (Fraunhofer-Gesellschaft 2022). Entsprechend bieten sich die hier genutzten technischen Komponenten – wie etwa die Konnektorenarchitektur, die die Verbindung zu den Datenquellen der Datengebenden herstellt, Metadaten zu den Datenquellen und zu den Nutzungsbedingungen der Daten verwaltet und den Transfer der Daten inklusive der Nutzungsbedingungen technisch abwickelt (Nagel und Lycklama 2021; Otto et al. 2019b) – als Blaupause für die Gestaltung von Datentreuhandstrukturen an. Gleiches gilt für die laufenden Aktivitäten rund um das Projekt GAIA-X, die zu einem Großteil auf den Vorarbeiten der IDSA aufbauen. Jedoch wurde in den Interviews auch die Befürchtung geäußert, dass die beiden Initiativen aufgrund ihrer Größe und der Vielzahl an beteiligten Akteuren nur langsam zu konkreten technischen Bausteinen kommen, wodurch die Nutzung als Standards für den Aufbau von Datentreuhändern in der Praxis schwieriger sei.

Die Rolle von Standards für die Etablierung von Datentreuhändern

Standards können für die Entwicklung und vor allem die nachhaltige Etablierung von Datentreuhändern und den damit verbundenen Datenökosystemen eine zentrale Rolle spielen. Dabei haben Standards für ganz unterschiedliche Elemente von Datentreuhändern großes Potenzial: Neben standardisierten Daten- und Metadatenformaten stehen hier auch die grundlegende Semantik der Daten, die Ausgestaltung technischer Schnittstellen für die Übertragung der Daten, aber auch die Qualität der Datenbestände im Fokus. Darüber hinaus sind auch Standards für kryptografische Sicherheitsfunktionen bzw. für die Pseudonymisierung und Anonymisierung von Datenbeständen von Bedeutung, insbesondere bei klar erkennbarem Personenbezug. Etablierte und breit genutzte Standards für Datenformate und Metadatenformate sind eine Voraussetzung für effizientes Datenmanagement und eine effektive Datenanalyse. In einigen Branchen haben sich bereits Standards durchgesetzt, andere starten erst jetzt mit der Entwicklung. Wirkmächtige Standards sollten dabei drei Voraussetzungen erfüllen: Zum einen sollten sie frei nutzbar und leicht für die Mitglieder des Ökosystems implementierbar sein. Die Datenformate sollten zudem nicht nur auf die Bedürfnisse eines Akteurs zugeschnitten sein und außerdem einen klaren Rückbezug zum Ziel der Standardsetzung herstellen (Shiohira und Dale-Jones 2019).

Je offener Standards – etwa für Datenformate oder Schnittstellen – sind, desto einfacher ist der reibungslose Austausch von Daten und die Verknüpfung verschiedener Systeme der am Ökosystem teilnehmenden Akteure. Der Grundsatz der Offenheit ist dann erfüllt, wenn die beteiligten Datengebenden und Datennehmenden grundsätzlich die Möglichkeit haben, an der Entwicklung der Standards mitzuwirken und deren Details einzusehen. Ferner sollte entweder die Nutzung des Standards lizenzfrei sein oder eine Lizenzierung des Standards sollte zu fairen, angemessenen und nicht diskriminierenden Bedingungen (FRAND: fair, reasonable and non-discriminatory terms) möglich sein (Europäische Kommission 2017).

Sollten aber aufgrund zu langer Abstimmungszyklen oder widerstrebender Interessen zwischen unterschiedlichen Ökosystemteilnehmenden im konkreten Anwendungsfall keine standardisierten Datenformate vorhanden sein und sollte auch mittels Datentreuhänder keine Einigung erzielbar sein, können als Alternative auch Ontologien bzw. Vokabularien für die heterogenen Datenbestände genutzt werden. Der Datentreuhänder kann hier entsprechend als Übersetzer gemäß zuvor klar kommunizierten Ontologien fungieren und den Datenaustausch trotz unterschiedlichster Formate orchestrieren.

Als relevanter Metadatenstandard kann unter anderem DCAT (Data Catalogue Vocabulary) angeführt werden (Nagel und Lycklama 2021; González Morales und Orrell 2018). Standardisierte Datenformate und Metadatenstrukturen bilden anschließend die Grundlage für die einfache Entwicklung und Implementierung von Programmierschnittstellen, die die Nutzung der mittels Datentreuhänder verfügbaren Daten erleichtern (Gonzalez und Orell 2018). Ein Beispiel für eine bereits vorliegende Standardschnittstelle für Datenaustausch ist etwa der Context Broker, der im Rahmen des EU-Programms Connecting Europe Facility entstanden ist (Nagel und Lycklama 2021).

Dagegen gibt es keinerlei festgelegte Normen oder Standards für die im Kontext von Datentreuhänderschaft zentralen Prozesse der Anonymisierung bzw. Pseudonymisierung. Wie hinreichend belastbare Verfahren in der Praxis ausgestaltet werden sollen, wurde bisher weder durch den Gesetzgeber noch durch Industriestandards konkretisiert (Richter 2021a). Lediglich sind erste Ansätze zur Standardisierung in Form von Arbeitspapieren oder Handreichungen vonseiten des IKT-Branchenverbands Bitkom (Aichroth et al. 2020) bzw. einer Arbeitsgruppe des Digital-Gipfels aus dem Jahr 2019 (Schwartmann und Weiß 2019) erkennbar und können als Orientierungshilfe bei der Etablierung von Datentreuhändern genutzt werden. Für die Gewährleistung der Informationssicherheit gibt es dagegen etablierte Verfahren (siehe Abschnitt 5.5.1).

Standards können dabei entweder projektbezogen beim Aufbau eines konkreten Datentreuhänders entworfen werden, wodurch sie flexibler sind und besser auf die vorliegenden Bedürfnisse der Ökosystemteilnehmenden abgestimmt werden können, oder es werden bestehende Standards übernommen, wodurch ihre Interoperabilität und damit die Skalierbarkeit der Lösungen gesteigert wird (Shiohira und Dale-Jones 2019). In der Literatur wird jedoch betont, dass solche Standards wahrscheinlich eher in kollektiven Standardsetzungsverfahren oder gegebenenfalls durch marktmächtige Unternehmen gesetzt werden als durch einzelne Projekte (Specht-Riemenschneider und Kerber 2022).

5.5.3 DATENWERTSCHÖPFUNG

Zuletzt können Datentreuhänder in Abhängigkeit des jeweiligen Anwendungsfalls technische Lösungen für die Ökosystemteilnehmenden bereitstellen, die die Realisierung direkter Mehrwerte für die Datengebenden und Datennutzenden ermöglichen. Hierzu zählen nach Aussage von Expertinnen und Experten einerseits einfach nutzbare Softwarelösungen zur Hinterlegung und einfache Konfigurationen der Bedingungen durch die Datengebenden, unter denen die bereitgestellten Daten genutzt werden können sollen. In Verbindung mit technischen Komponenten zum transparenten Monitoring der Nutzung der bereitgestellten Daten entsteht so technisch die Möglichkeit, übersichtliche Dashboards für die Teilnehmenden des Ökosystems bereitzustellen sowie Abrechnungs- und Streitschlichtungsmechanismen umsetzen zu können. Darüber hinaus bedarf es technischer Suchinstrumente zur Identifikation relevanter Datenbestände (Nagel und Lycklama 2021). Diese können etwa in Form von durchsuchbaren Metadatenkatalogen oder auch aktiven Matching-Protokollen ausgestaltet werden. Hinzu kommt die Etablierung eines leicht adaptierbaren Workflows für die Datenbereitstellung und Datennutzung durch den Datentreuhänder inklusive der Ermöglichung der Integration unterschiedlichster Ökosystemteilnehmender und Datenquellen. Dazu ist eine technische Anbindung unterschiedlicher Systeme und sehr wahrscheinlich auch bis zu einem gewissen Grad die Transformation der unterschiedlichen Datenformate erforderlich, um im Sinne der leichten Nutzbarkeit nachhaltig Vertrauen in das entstehende Ökosystem aufzubauen. Dafür sind aber zahlreiche Technologien, Standards und Normen vorhanden (Nagel und Lycklama 2021). Als weiteres technisches Element zur Realisierung von Datenwertschöpfung durch den Datentreuhänder kann in Einklang mit den geltenden rechtlichen Bestimmungen und auch den Interessen der Ökosystemteilnehmenden das Angebot von datenbasierten Analysediensten aufgeführt werden. In Abhängigkeit der Rahmenbedingungen des konkreten Anwendungsfalls kann es sich dabei um statistische Auswertungen oder um Anwendungen des Maschinenlernens handeln (Nagel und Lycklama 2021).

06

6 ERSTE BEISPIELE AUS DER PRAXIS

Trotz der breiten Fachdebatte zu Datentreuhändern erweist sich die Identifikation und Analyse von konkreten Praxisbeispielen als Herausforderung. Darüber hinaus unterliegen weiterführende Detailinformationen zu verwendeten Methoden, Standards und dem Geschäft von Datentreuhandlösungen oftmals einem privilegierten Zugang (siehe u. a. Manohar et al. 2020). Die vorliegende Analyse erster Praxisbeispiele unternimmt den Versuch, auf Basis verlässlicher, öffentlich verfügbarer Informationen einen Überblick zu verwendeten technischen und organisatorischen Elementen von Datentreuhandlösungen zu liefern, die in Deutschland oder Europa nutzbar sind. Methodisch fußt die Sammlung der nachfolgend aufgeführten Fallbeispiele auf einer Sichtung der vorhandenen Publikationslandschaft, der Analyse der geführten Interviews sowie einer strukturierten Online-Recherche nach weiteren Fallbeispielen. Zudem wurden die Praxisbeispiele aus einer früheren Studie zu in der Praxis erkennbaren Data-Sharing-Plattformen und Datenmarktplätzen (Lindner et al. 2021) dahingehend überprüft, ob sie gegebenenfalls in einem engen oder auch weiten Verständnis als Datentreuhänder kategorisiert werden können. Als Informationsquellen dienen dabei die Darstellungen des eigenen Internetauftritts sowie, wenn vorhanden, publizistische Beiträge oder wissenschaftliche Einzelfallstudien der einzelnen Datentreuhänder und der dazugehörigen Plattform. Aufgenommen wurden Datentreuhänder, die über tragfähige Geschäfts- und Betriebsmodelle sowie über eine ausreichend große Anzahl von Teilnehmenden im Realbetrieb verfügen. Weitere Praxisbeispiele für Datentreuhänder, die sich jedoch noch in der Konzeptions- oder Aufbauphase befinden, sind im Anhang aufgeführt. Bei der Mehrheit dieser Beispiele handelt es sich um staatlich geförderte Pilotprojekte, die ein Datentreuhandmodell für klar abgrenzbare Anwendungsfälle konzipieren, umsetzen und auf Basis eines ersten Testbetriebs Chancen, Mehrwerte und Hindernisse von Datentreuhänderschaft in der Praxis evaluieren. Darüber hinaus werden auch in der Aufbau- bzw. Wachstumsphase befindliche Plattformen wie etwa der Mobility Data Space oder CenTrust angeführt.

Die Analyse der identifizierbaren Fallbeispiele von Datentreuhändern im Realbetrieb wurde dabei entsprechend folgenden Kriterien durchgeführt:

- Anwendungsbereich,
- Trägerschaft,
- Marktreife des Datentreuhänders,
- auf der Plattform umgesetzter enger oder weiter Datentreuhandbegriff und
- Instrumente zur Vertrauensbildung.

6.1 Caruso Dataplace

Der Caruso Dataplace wurde Anfang 2017 als Ergebnis einer Initiative einiger unabhängiger Anbieter des freien Markts für Autoersatzteile ins Leben gerufen und verfolgt seitdem das Ziel, hochwertige Daten des Automobil- und Mobilitätssektors zur Verfügung zu stellen. Basis hierfür sind Offenheit, Nicht-Diskriminierung jeglicher Marktteilnehmer sowie Fairness. Die Neutralität der Plattform soll durch eine diversifizierte Struktur der mehr als 20 Anteilseigner aus dem Automobilsektor gewährleistet werden. Auf der Plattform werden fahrzeuginterne Daten zur Verfügung gestellt, welche datenbasierte Dienstleistungen im Mobilitätssektor ermöglichen, wie beispielsweise im Kfz-Servicegeschäft, beim Carsharing über Apps oder bei Versicherungen, die je nach Fahrprofil maßgeschneiderte Policen anbieten können. Zudem wird ein Entwicklungsportal angeboten, das die technische Integration der Daten aufseiten der Unternehmenskunden – auch bei eingeschränkten technischen oder personellen Möglichkeiten – erleichtern soll. Die Monetarisierung des Geschäftsmodells der Plattform erfolgt über ein vierstufiges Mitgliedschaftsmodell. Darüber hinaus gibt es unter der Kategorie On-Demand individuelle Angebote einschließlich exklusiver Datenzugänge zu Herstellerdaten oder zusätzlicher Beratungsleistungen zur technischen Integration oder zur Konzeption datenbasierter Services.

KATEGORIE	AUSPRÄGUNG
Anwendungsbereich	Fahrzeugdaten
Trägerschaft	Privatwirtschaftliches Unternehmen: Caruso GmbH, Ismaning
Marktreife	Regelbetrieb
Enger vs. weiter Datentreuhandbegriff	Weiter Datentreuhandbegriff
Neutralitätsverständnis des Datentreuhänders	Angebot datenbasierter Dienstleistungen und Services
Vertrauensstiftende Maßnahmen	Geteilte Eigentümerschaft durch 20 – teilweise im Wettbewerb stehende – Akteure
Website	www.caruso-dataplace.com

Tabelle 1 Merkmale der Plattform Caruso Dataplace

6.2 CSDR

Die Plattform CSDR (ClinicalStudyDataRequest) ermöglicht den Zugang zu Daten klinischer Studien auf Patient:innen-Level, die von 13 der weltweit führenden Pharmaunternehmen zu Forschungszwecken untereinander und mit der Forschungsgemeinschaft geteilt werden. Neun Jahre nach der Gründung im Jahr 2013 sind Datensätze von mehr als 3.000 klinischen Studien verfügbar. Der Betrieb der Plattform wird über den technischen Drittanbieter ideaPoint (Tochter des US-Unternehmens Anaqua, das Software und Dienstleistungen für das IP-Management anbietet) realisiert. Der Zugriff erfolgt auf Anfrage registrierter Nutzender, deren Forschungsvorschläge vorab jeweils durch ein unabhängiges Gremium von Gutachtenden freigegeben werden müssen. Ebenso ist eine Gegenzeichnung der detaillierten Datennutzungsvereinbarung von CSDR notwendig. Die Daten werden zum Großteil zentral innerhalb einer sicheren Arbeitsumgebung gespeichert und nach der Freigabe für insgesamt zwölf Monate zur Verfügung gestellt. In der Arbeitsumgebung können die Daten durch integrierte statistische Auswertungssoftware genutzt werden. Aber auch der direkte Austausch der Daten zwischen Datengebenden und Nutzenden wird organisatorisch unterstützt. Die Finanzierung erfolgt über die Mitgliedsbeiträge der institutionellen Mitglieder, Stiftungen und öffentlichen Forschungsförderungsinstitutionen. Eine Gebühr für die individuelle Nutzung wird nicht erhoben.

KATEGORIE	AUSPRÄGUNG
Anwendungsbereich	Gesundheitsdaten
Trägerschaft	Privatwirtschaftliches Unternehmen: Anaqua Inc., Boston MA
Marktreife	Regelbetrieb
Enger vs. weiter Datentreuhandbegriff	Enger Datentreuhandbegriff
Neutralitätsverständnis des Datentreuhänders	Keine Datennutzung durch den Betreiber
Vertrauensstiftende Maßnahmen	Gutachtendengremium, Datenanalyse nur in geschlossener Umgebung
Website	www.clinicalstudydatarequest.com

Tabelle 2 Merkmale der Plattform CSDR

6.3 Data Intelligence Hub

Der Data Intelligence Hub (DIH) ist eine branchen- und industrieübergreifende Sharing-Plattform, betrieben von der Deutschen Telekom. Das Ziel des DIH ist es, Unternehmen eine ganzheitliche Übersicht über frei verfügbare, zum Austausch oder direkt zum Kauf stehende Daten zu bieten, deren Nutzung den Unternehmen zur Optimierung eigener Prozesse entlang der Wertschöpfungskette oder der Entwicklung innovativer datengetriebener Geschäftsmodelle dienen sollen. Auf einer sicheren Dateninfrastruktur können branchenübergreifend nicht-personenbezogene Daten zwischen verschiedenen Akteuren ausgetauscht werden. Zu diesem Zweck werden durch den Betreiber ergänzend verschiedene Analysetools zur Verfügung gestellt, um die unternehmenseigenen Daten in Kombination mit den auf der Plattform verfügbaren Daten mit Methoden des Machine Learning zu verarbeiten und zu strukturieren. Der Data Intelligence Hub erhebt den Anspruch, als erste Plattform die Sicherheitsvorgaben der International Data Spaces Association (IDSA) zu erfüllen. Dazu nimmt der DIH die Rolle als neutraler Vertrauensanker ein, ermöglicht die Wahl zwischen einer zentralen oder dezentralen Datenhaltung zur Gewährleistung der Datensouveränität und setzt eine Zertifizierung der Teilnehmenden um.

KATEGORIE	AUSPRÄGUNG
Anwendungsbereich	Domänenübergreifend, kein spezifischer Anwendungsbereich
Trägerschaft	Privatwirtschaftliches Unternehmen: T-Systems International GmbH, Frankfurt am Main
Marktreife	(Früher)Regelbetrieb
Enger vs. weiter Datentreuhandbegriff	Weiter Datentreuhandbegriff
Neutralitätsverständnis des Datentreuhänders	Neutral
Vertrauensstiftende Maßnahmen	Effektive Instrumente zur Sicherung der Datensouveränität mittels MY Data Control Technologies, Teilnehmerzertifizierung
Website	https://dih.telekom.net

Tabelle 3 Merkmale der Plattform Data Intelligence Hub

6.4 Hilo MRM – Maritime Risk Management

Seit 2017 bündelt und analysiert die britische Hilo MRM Daten aus der maritimen Schifffahrt, um im Sinne eines vorausschauenden Risikomanagements Vorhersagen zu Unfällen auf See für einzelne Schiffe treffen zu können. Hilo MRM ist als Pilotprojekt von zehn Industriepartnern aus der Reederei-Wirtschaft gestartet und wurde mittlerweile in ein eigenständiges, nicht-gewinnorientiertes Unternehmen überführt. Im Jahr 2022 sind hochsensible Daten von 55 Reederei-Unternehmen in der geschützten Umgebung von Hilo MRM verfügbar.

KATEGORIE	AUSPRÄGUNG
Anwendungsbereich	Risikodaten aus der Schifffahrt
Trägerschaft	Privatwirtschaftliches, nicht-gewinnorientiertes Unternehmen: Hilo Maritime Risk Management Ltd., London
Marktreife	(Früher)Regelbetrieb
Enger vs. weiter Datentreuhandbegriff	Weiter Datentreuhandbegriff
Neutralitätsverständnis des Datentreuhänders	Aktive Datennutzung zur Realisierung datenbasierter Beratungsangebote
Vertrauensstiftende Maßnahmen	Zertifizierte Informationssicherheit gemäß ISO 27001, Anonymisierung
Website	www.hilomrm.com

Tabelle 4 Merkmale der Plattform Hilo MRM

6.5 Otonomo

Das israelische Unternehmen Otonomo hat die gleichnamige cloudbasierte Plattform zum Austausch von Connected Car Data und deren Monetarisierung entwickelt und aufgebaut. Die Plattform ermöglicht es Automobilherstellern, Drittanbietern sowie Fahrerinnen und Fahrern innerhalb eines Ökosystems Daten auszutauschen. Otonomo agiert dabei als neutraler Akteur und ermöglicht Drittanbietern einerseits den leichten Zugang zu hochwertigen Daten und andererseits erhalten Automobilhersteller und auch die Fahrenden Kontrolle über die Verfügbarkeit durch ein transparentes Rechtemanagement. Insgesamt stehen Datensätze von mehr als 18 Millionen Personen- und Nutzfahrzeugen aus den USA, Kanada, Asien und Europa zur Verfügung.

KATEGORIE	AUSPRÄGUNG
Anwendungsbereich	Fahrzeugdaten
Trägerschaft	Privatwirtschaftliches Unternehmen: Otonomo Technologies Ltd., Tel Aviv
Marktreife	Regelbetrieb
Enger vs. weiter Datentreuhandbegriff	Weiter Datentreuhandbegriff
Neutralitätsverständnis des Datentreuhänders	Aktive Bearbeitung bzw. Redaktion der Daten zur Aggregation und Qualitätssicherung
Vertrauensstiftende Maßnahmen	Transparentes Rechtemanagement
Website	https://otonomo.io

Tabelle 5 Merkmale der Plattform Otonomo

6.6 SPOCC

Die Plattform SPOCC (Single Point of Content and Communication) erhebt den Anspruch, die zentrale Datenplattform für die deutsche Schuh- und Lederwarenbranche zu sein und das professionelle Datenmanagement von Marketing-Inhalten zu ermöglichen. SPOCC wurde 2019 als Kooperationsprojekt der Warenwirtschaftsanbieter ETOS, Brandt Software-Produkte und Ariston Informatik in Kooperation mit dem Bundesverband der Schuh- und Lederwarenindustrie, HDS/L ins Leben gerufen, um Hersteller und Händler miteinander zu vernetzen und diesen die Arbeit mit digitalen Inhalten zu erleichtern. Über die offene Datenplattform, die vom European-Clearing-Center betrieben wird, können Hersteller Materialien wie Foto-, Grafik- und Videodateien oder Produktstammdaten und Marketinginformationen nutzerbezogen dem stationären Handel zur Verfügung stellen. Nutzungsrechte und Nutzungszeiträume der Daten können per Drag und Drop verwaltet werden.

KATEGORIE	AUSPRÄGUNG
Anwendungsbereich	Produktdaten
Trägerschaft	Privatwirtschaftliches Unternehmen: European-Clearing-Center GmbH & Co. KG, Bergkamen
Marktreife	Regelbetrieb
Enger vs. weiter Datentreuhandbegriff	Weiter Datentreuhandbegriff
Neutralitätsverständnis des Datentreuhänders	Neutral
Vertrauensstiftende Maßnahmen	Einfaches und transparentes Management der Nutzungsrechte
Website	www.spocc.io

Tabelle 6 Merkmale der Plattform SPOCC

6.7 Vivli

Im Jahr 2015 haben sich das Multi-Regional Clinical Trials Center (MRCT) des Brigham and Women's Hospital und die Harvard University zusammen mit Partnern aus der pharmazeutischen Industrie und der medizinischen Forschung das Ziel gesetzt, eine unabhängige Plattform für das Teilen klinischer Versuchsdaten zu konzipieren und gemeinsam umzusetzen. Im Juli 2018 wurde als Resultat die nicht-gewinnorientierte Plattform Vivli gestartet, die heute Daten von mehr als 6.300 klinischen Studien 38 institutioneller Mitglieder aus der pharmazeutischen Industrie verfügbar gemacht hat. Laut eigener Aussage ist Vivli damit die größte Datenaustauschplattform für klinische Studien weltweit. Zusätzlich bietet die Plattform eine spezialisierte Suchmaschine und eigene Datenanalyseinstrumente für die Nutzenden an. Der Zugriff auf einzelne Datensätze ist nur für verifizierte Nutzende möglich, deren qualifizierte Anfrage durch den Datengebenden bestätigt werden muss. Die Finanzierung erfolgt über die Mitgliedsbeiträge der institutionellen Mitglieder und Stiftungen.

KATEGORIE	AUSPRÄGUNG
Anwendungsbereich	Gesundheitsdaten
Trägerschaft	Privatwirtschaftliches, nicht-gewinnorientiertes Unternehmen: Vivli, Inc., Cambridge, MA
Marktreife	Regelbetrieb
Enger vs. weiter Datentreuhandbegriff	Enger Datentreuhandbegriff
Neutralitätsverständnis des Datentreuhänders	Keine Datennutzung durch den Betreiber
Vertrauensstiftende Maßnahmen	IT-Sicherheitszertifizierung gemäß SOC 2 (System and Organization Controls), Expertengremium (Independent Review Panel)
Website	https://vivli.org/

Tabelle 7 Merkmale der Plattform Vivli

6.8 VTH eData-Pool

Der eData-Pool ist eine Datenaustauschplattform des Verbands Technischer Handel (VTH) zwischen Herstellerunternehmen und technischen Händlern in Deutschland, Österreich und der Schweiz. Die Hersteller sind hierbei für die Einstellung und die Pflege ihres Sortiments und der dazugehörigen Daten im Sinne der Aktualität, Vollständigkeit und Richtigkeit verantwortlich. Händler erhalten wiederum qualitativ hochwertige Produktdaten für technische Bedarfsartikel in einem einheitlichen Format. Unter der Verwendung einheitlich definierter Sachmerkmale und mit der entsprechenden Anreicherung der einzelnen Datenbestände sowie deren abschließenden Kontrolle können Handelsunternehmen auf Datensätze mit den benötigten Attributen zugreifen – ohne selbst einen zu großen Prüfaufwand zu haben. Der Zugriff auf die Daten erfolgt über Datenfeeds, die die Händler mit den Stammdateninformationen der Produkte versorgen. Jeder Feed erfordert dabei eine individuelle Freigabe durch den jeweiligen Hersteller. Laut eigener Darstellung nehmen bereits mehr als 40 Herstellerunternehmen aus unterschiedlichen Industrien und mehr als 50 Handelsunternehmen das Angebot des eData-Pools in Anspruch. Durch regelmäßige Anwendertreffen soll die Zusammenarbeit weiter zwischen Datengebenden und Datennutzenden verbessert werden.

KATEGORIE	AUSPRÄGUNG
Anwendungsbereich	Produktdaten für technische Bedarfsartikel
Trägerschaft	Fachverband für den technischen Handel in Deutschland, Österreich und der Schweiz: VTH Verband Technischer Handel e.V., Düsseldorf
Marktreife	Regelbetrieb
Enger vs. weiter Datentreuhandbegriff	Weiter Datentreuhandbegriff
Neutralitätsverständnis des Datentreuhänders	Neutral (bis auf Qualitätssicherung der Daten)
Vertrauensstiftende Maßnahmen	Community-Building durch Anwendermaßnahmen
Website	www.vth-verband.de/vth-eservices/vth-edata-pool

Tabelle 8 Merkmale der Plattform VTH eData-Pool

07

7 EIN ZWISCHENFAZIT ZUM STATUS QUO

Trotz der klar erkennbaren Vorteile von Datentreuhändern als Vertrauensanker innerhalb von Datenökosystemen und sehr umfangreicher konzeptioneller Vorarbeiten stecken viele Bemühungen zum Aufbau entsprechender Strukturen mit wenigen Ausnahmen noch in der Konzeptions- oder der frühen Aufbauphase. Dieser Rückschluss wird durch die oft sehr begrenzte Informationslage zu bestehenden Datentreuhandangeboten untermauert. Auf Basis der vorliegenden Informationen kann aber für die bestehenden Praxisbeispiele festgehalten werden, dass durchaus für unterschiedliche Trägerschaftskonzepte Platz am Markt ist.

Es ist klar erkennbar, dass Datentreuhandmodelle mit einem Fokus auf einer konkreten Branche oder sogar einem sehr spezifischen Anwendungsfall innerhalb einer Branche grundsätzlich eher in der Lage sind, die Bedürfnisse ihrer potenziellen Ökosystemteilnehmenden effektiver zu adressieren und einen echten Mehrwert zu generieren. Insbesondere schon länger existierende Plattformen wie SPOCC und VTH eData-Pool mit einem sehr klaren Branchenbezug und dem Fokus auf weniger schützenswerte Produktdaten werden in der Diskussion noch zu oft übersehen. Insgesamt decken die für diese Studie identifizierten tätigen Plattformen und Projekte die Branchen Gesundheit, Luftfahrt, produzierendes Gewerbe, Logistik, Automobilindustrie und Mobilität ab.

Entsprechend kann gefolgert werden, dass die Stakeholder- und Nutzenanalyse als Basis der Ökosystementwicklung des jeweiligen Datentreuhänders zusammen mit einem aktiven Community-Building zentrale Aufgaben der dahinterstehenden Organisation darstellen. Wesentlicher Erfolgsfaktor ist ein langsamer, aber nachhaltiger Ökosystemaufbau anhand konkreter und möglichst spezifischer Anwendungsfälle organisationsübergreifender Datennutzung mit konkreten finanziellen oder nicht direkt monetären Vorteilen für die Teilnehmenden des Ökosystems. Neben der Einigung auf ein klares Ziel inklusive entsprechendem Mehrwert für die beteiligten Akteure sollte ein Datentreuhänder über eine vertrauensfördernde und klar geregelte Governance-Struktur verfügen und durch transparente Finanzierungsstrukturen nachhaltig den eigenen Erhalt und damit die Existenz des entstehenden Datenökosystems sichern.

Je nach Anwendungsfall ergibt sich dadurch eine Vielfalt möglicher vertrauensfördernder Funktionen, die von Datentreuhändern in Abgrenzung zu reinen Datentransaktionsinfrastrukturen übernommen werden sollten:

- Sicherstellung des Datenschutzrechts,
- Funktionen für Anonymisierung & Pseudonymisierung umsetzen,
- Qualitätssicherung von Daten,
- Verwaltung von Zugangsrechten und Konfliktmanagement,
- Vorgabe einheitlicher Standards für den Datentransfer,
- Community-Building und
- wenn notwendig als tatsächliche Stewardship die Überprüfung von Berechtigung der Nutzungsanfragen und präferenzbasierte Verfügbarmachung der angefragten Daten bei Vorliegen der entsprechenden Voraussetzungen.

Oftmals wird über die Etablierung von Datentreuhändern noch zu stark technikfokussiert diskutiert. Ein Datentreuhänder ist weniger als ein Betreiber einer Kombination technischer Komponenten zu verstehen, sondern vielmehr als Ermöglicher eines Datenökosystems, der zuerst die Bedürfnisse, Ängste und Zweifel der teilnehmenden Akteure verstehen und diese dann auch mit technischen Lösungen adressieren muss. Das dafür erforderliche Wissen und Know-how zu technischen Komponenten ist in der Regel vorhanden, jedoch stellt die bedarfsgerechte Zusammenstellung der einzelnen Komponenten im konkreten Anwendungsfall eine erhebliche Herausforderung dar. Zudem sind sowohl das Aufsetzen der entsprechenden technischen Infrastruktur, insbesondere aber das dringend erforderliche und zeitintensive Community-Building mit erheblichen Investitionskosten verbunden, die perspektivisch gedeckt werden müssen. Der frühzeitigen Entwicklung von tragfähigen Betriebs- und Geschäftsmodellen kommt daher eine entscheidende Bedeutung zu. Hier können Unterstützungsangebote – wie etwa das im Oktober 2022 auf europäischer Ebene ins Leben gerufene Data Spaces Support Centre – die Etablierung von Datentreuhändern als Ökosystemförderer der jeweiligen Datenräume während der Aufbauphase erleichtern.

Zu beobachten bleibt die Rechtspraxis des europäischen Data Governance Act, der das Angebot von erweiterten Service-Angeboten vermutlich eher einschränkt. Gerade privatwirtschaftlich getragene Datentreuhänder müssen hier gegebenenfalls noch ihre Geschäftsmodelle anpassen.

08

8 LITERATURVERZEICHNIS

Aichroth, Patrick; Battis, Verena; Dewes, Andreas; Dibak, Christoph; Doroshenko, Vadym; Geiger, Bernd et al. (2020): Anonymisierung und Pseudonymisierung von Daten für Projekte des maschinellen Lernens. Eine Handreichung für Unternehmen. Hg. v. Bitkom. Berlin. Online verfügbar unter https://www.bitkom.org/sites/default/files/2020-10/201002_lf_anonymisierung-und-pseudonymisierung-von-daten.pdf, zuletzt geprüft am 23.11.2022.

Arlinghaus, Tim; Kus, Kevin; Kajüter, Patricia; Teuteberg, Frank (2021): Datentreuhandstellen gestalten: Status quo und Perspektiven für Geschäftsmodelle. Designing Data Trustees: Status quo and Perspectives for Business Models. In: HMD Praxis der Wirtschaftsinformatik 58 (3), S. 565–579. Online verfügbar unter https://link.springer.com/article/10.1365/s40702-021-00727-x#citeas, zuletzt geprüft am 23.11.2022.

Azkan, Can; Gür, Inan; Hupperz, Marius; Gelhaar, Joshua; Gieß, Anna; Groß, Tobias et al. (2022): Anreizsysteme und Ökonomie des Data Sharing. Handlungsfelder des unternehmensübergreifenden Datenaustausches und Status quo der deutschen Wirtschaft. Hg. v. Fraunhofer ISST. Dortmund. Online verfügbar unter https://ieds-projekt.de/wp-content/uploads/2022/03/IEDS-Whitepaper-1.pdf.

Blankertz, Aline (2021): Vertrauliche Datentreuhand. Wie die Datentreuhand effektiv Daten schützen und sichern kann. In: Datenschutz und Datensicherheit 16 (12), S. 789–810. Online verfügbar unter https://www.springerprofessional.de/vertrauliche-datentreuhand/19898838, zuletzt geprüft am 23.11.2022.

Blankertz, Aline (2022): Warum Wettbewerbspolitik auch die Privatsphäre berücksichtigen muss. In: Michael Friedewald, Michael Kreutz und Marit Hansen (Hg.): Selbstbestimmung, Privatheit und Datenschutz. Gestaltungsoptionen für einen europäischen Weg. Wiesbaden: Springer Vieweg (DuD-Fachbeiträge), S. 11–32. Online verfügbar unter https://link.springer.com/chapter/10.1007/978-3-658-33306-5_2, zuletzt geprüft am 23.11.2022.

Blankertz, Aline; Braunmühl, Patrick von; Kuvez, Pencho; Richter, Frederick; Richter, Heiko; Schallbruch, Martin (2020): Datentreuhandmodelle. Themenpapier. Hg. v. Stiftung Neue Verantwortung. Berlin. Online verfügbar unter https://www.stiftung-nv.de/de/publikation/datentreuhandmodelle, zuletzt geprüft am 23.11.2022.

Blankertz, Aline; Specht-Riemenschneider, Louise (2021): Neue Modelle ermöglichen. Regulierung für Datentreuhänder. Hg. v. Heinrich-Böll-Stiftung. Berlin (böll.brief – Grüne Ordnungspolitik, 16). Online verfügbar unter https://www.boell.de/sites/default/files/2021-08/bo%23776ll.brief%20G16%20Neue%20Modelle%20ermo%23776glichen.pdf, zuletzt geprüft am 23.11.2022.

Borges, Georg; Duisberg, Alexander; Haas, Philipp; Keil, Ulrich; Payer, Christine; Schweinoch, Martin; Wittek, Nick (2021): Teilnahmebedingungen für eine Industrie 4.0 Plattform. Hg. v. Plattform Industrie 4.0. Online verfügbar unter https://www.plattform-i40.de/IP/Redaktion/DE/Downloads/Publikation/RTB%20-%20Mustervertrag.html, zuletzt aktualisiert am 13.04.2021, zuletzt geprüft am 23.11.2922.

Buchner, Benedikt; Haber, Anna C.; Hahn, Horst K.; Kusch, Harald; Prasser, Fabian; Sax, Ulrich; Schmidt, Carsten Oliver (2021): Das Modell der Datentreuhand in der medizinischen Forschung. In: Datenschutz und Datensicherheit 45, S. 806–810. Online verfügbar unter https://link.springer.com/article/10.1007/s11623-021-1534-y, zuletzt geprüft am 29.11.2022.

Bundesdruckerei: Data trustee. Data trustee platform with a trust center service on demand. Online verfügbar unter https://www.bundesdruckerei-gmbh.de/en/solutions/data-trustee, zuletzt geprüft am 29.11.2022.

Bundesregierung (2021): Datenstrategie der Bundesregierung. Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum. Bundeskanzleramt. Berlin. Online verfügbar unter https://www.bundesregierung.de/breg-de/suche/datenstrategie-der-bundesregierung-1845632, zuletzt geprüft am 29.11.2022.

Cattaneo, Gabriella; Francalanci, Chiara (2020): Story 9 – Scaling up data-driven innovation: European industry requirements and the role of European data spaces. Hg. v. Europäische Kommission. Luxemburg (Update of the European Data Market). Online verfügbar unter https://datalandscape.eu/data-driven-stories/story-9-scaling-data-driven-innovation-european-industry-requirements-and-role, zuletzt geprüft am 29.11.2022.

Cattaneo, Gabriella; Micheletti, Giogio; Glennon, Mike; La Croce, Carla; Mitta, Chrysoula (2020): The European data market monitoring tool. Key facts & figures, first policy conclusions, data landscape and quantified stories. Hg. v. Europäische Kommission. Brüssel. Online verfügbar unter https://op.europa.eu/en/publication-detail/-/publication/3ad92ee6-c70f-11ea-adf7-01aa75ed71a1/language-en, zuletzt geprüft am 29.11.2022.

Clarke, Roger (2016): Big data, big risks. In: Information Systems Journal 26 (1), S. 77–90. DOI: 10.1111/isj.12088.

Collovà, Patrizio; Marti, Michael; Schwarz Badertscher, Daniel; Wäspi, Flurina; Wenger, Nicolai (2021): Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung. Hg. v. Bundesamt für Kommunikation. Bern. Online verfügbar unter https://arbor.bfh.ch/id/eprint/16789, zuletzt geprüft am 29.11.2022.

D'Addario, Josh (2020): Seven reasons why businesses should be sharing data. Open Data Institute. Online verfügbar unter https://theodi.org/article/seven-reasons-why-businesses-should-be-sharing-data/, zuletzt geprüft am 19.10.2022.

Demary, Vera; Fritsch, Manuel; Goecke, Henry; Lichtblau, Karl; Schmitz, Edgar (2019): Bereitschaft der deutschen Unternehmen für die Teilhabe an der Datenwirtschaft. Gutachten im Rahmen des BMWi-Verbundprojektes DEMAND. Hg. v. Institut der deutschen Wirtschaft. Köln. Online verfügbar unter https://www.iwkoeln.de/studien/vera-demary-manuel-fritsch-henry-goecke-alevtina-krotova-karl-lichtblau-edgar-schmitz-bereitschaft-der-deutschen-unternehmen-fuer-die-teilhabe-an-der-datenwirtschaft.html.

Eknert, Anders (2021): Eine Einführung in Open Policy Agent und Styra DAS. Hg. v. Cloudical Deutschland. Online verfügbar unter https://the-report.cloud/eine-einfuhrung-in-open-policy-agent-und-styra-das, zuletzt geprüft am 19.10.2022.

Element AI; nesta (2019): Data Trusts – A new tool for data governance. London. Online verfügbar unter https://hello.elementai.com/rs/024-OAQ-547/images/Data_Trusts_EN_201914.pdf, zuletzt geprüft am 29.11.2022.

Europäische Kommission (2017): Anhang der Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Europäischer Interoperabilitätsrahmen – Umsetzungsstrategie, vom 23.03.2017. Online verfügbar unter https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0018.02/DOC_3&format=PDF, zuletzt geprüft am 07.12.2022.

Europäische Union (2022): VERORDNUNG (EU) 2022/868 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt). Hg. v. Amtsblatt der Europäischen Union. Online verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R0868&from=EN#d1e1715-1-1.

Falck, Oliver; Koenen, Johannes (2020): Rohstoff „Daten": Volkswirtschaftlicher Nutzen von Datenbereitstellung – eine Bestandsaufnahme. Hg. v. ifo Institut. München (ifo Forschungsberichte, 113/2020). Online verfügbar unter https://www.ifo.de/DocDL/ifo_Forschungsberichte_113_RohstoffDaten.pdf, zuletzt geprüft am 29.11.2022.

Fraunhofer-Gesellschaft (2022): International Data Spaces als globaler de facto Marktstandard für die souveräne Nutzung von Daten. München. Online verfügbar unter https://www.data-spaces.fraunhofer.de/de/InternationalDataSpaces/idsa.html, zuletzt geprüft am 29.11.2022.

Goldstein, Elena; Gasser, Urs; Budish, Ryan (2018): Data Commons Version 1.0: A Framework to Build Toward AI for Good. A roadmap for data from the 2018 AI for Good Summit. Hg. v. Bergmann Klein Center for Internet & Society. Online verfügbar unter https://medium.com/berkman-klein-center/data-commons-version-1-0-a-framework-to-build-toward-ai-for-good-73414d7e72be, zuletzt geprüft am 20.10.2022.

González Morales, Luis Gerardo; Orrell, Tom (2018): Data interoperability: A practitioner's guide to joining up data in the development sector. Hg. v. Vereinte Nationen. Online verfügbar unter https://repository.oceanbestpractices.org/handle/11329/1971, zuletzt geprüft am 29.11.2022.

Hardinges, Jack (2020): Data trusts in 2020. Hg. v. Open Data Institute. Online verfügbar unter https://theodi.org/article/data-trusts-in-2020, zuletzt geprüft am 20.10.2022.

Hardinges, Jack; Wells, Peter; Blandford, Alex; Jeni Tennison (2019): Data trusts: lessons from three pilots (report). Hg. v. Open Data Institute. Online verfügbar unter https://theodi.org/article/odi-data-trusts-report/, zuletzt geprüft am 29.11.2022.

Hohn-Hein, Nicolas; Barth, Günter (2022): § 2 GeschGehG. In: Jörg Fritzsche, Reiner Münker und Christoph Stollwerck: Beck'scher Online-Kommentar UWG. 18. Edition. München: C.H. Beck.

Hörnig, Lisa; Kühlem, Melanie (2022): Verrechnungskonzept für Datengenossenschaften (Daten eG). Univ. Stuttgart. Online verfügbar unter https://www.datengenossenschaft.com/wp-content/uploads/2022/12/Verrechnungskonzept-fuer-Datengenossenschaften_final.pdf.

Hottelet, Ulrich (2021): Daten-Intermediäre: Die noch unbekannten Wesen. Heise Online. Online verfügbar unter https://www.heise.de/news/Daten-Intermediaere-Die-noch-unbekannten-Wesen-5072344.html, zuletzt geprüft am 20.10.2022.

INFORM (2017): Data Sharing als wichtiger Erfolgsfaktor für die Supply Chain. Umfrage von INFORM präsentiert Status Quo, Hürden und Zukunftsaussichten. Online verfügbar unter https://www.inform-software.de/news/news-details/news/data-sharing-als-wichtiger-erfolgsfaktor-fuer-die-supply-chain, zuletzt aktualisiert am 20.10.2022, zuletzt geprüft am 20.10.2022.

Jäschke, Thomas; Reiter, Julius; Methner, Olaf (2018): Für immer anonym: Wie kann De-Anonymisierung verhindert werden? Hg. v. ABIDA-Projekt. Online verfügbar unter https://www.abida.de/sites/default/files/ABIDA Gutachten F%C3%9CR IMMER ANONYM.pdf, zuletzt geprüft am 29.11.2022.

Kersten, Heinrich; Klett, Gerhard, Reuters; Jürgen; Schröder, Klaus-Werner (2021): IT-Sicherheitsmanagement nah der neuen ISO 27001. ISMS, Risiken, Kennziffern, Controls. Wiesbaden: Springer Vieweg.

Klotz, Michael (2019): IT-Compliance nach COBIT 2019. Fachhochschule Stralsund. Stralsund (SIMAT Arbeitspapiere, 11-19-034). Online verfügbar unter http://hdl.handle.net/10419/204448, zuletzt geprüft am 01.12.2022.

Kraftfahrt-Bundesamt (24.05.2022): Forschungsdatenzentrum im Kraftfahrt-Bundesamt – Millionen anonymisierte Registerdaten für die Forschung. Pressemitteilung Nr. 21/2022. Flensburg. Online verfügbar unter https://www.kba.de/DE/Presse/Pressemitteilungen/Allgemein/2022/pm21_2022_FDZ.html, zuletzt geprüft am 29.11.2022.

Kühling, Jürgen (2021): Der datenschutzrechtliche Rahmen für Datentreuhänder. Was ist zu tun? In: Datenschutz und Datensicherheit – DuD (12), S. 783–788. Online verfügbar unter https://www.springerprofessional.de/der-datenschutzrechtliche-rahmen-fuer-datentreuhaender/19898836.

Kühling, Jürgen; Buchner, Benedikt (2020): Art. 7, Rn. 59. In: Jürgen Kühling und Benedikt Buchner: Datenschutz-Grundverordnung BDSG. Kommentar. 3. Auflage. München: C.H. Beck.

Kühling, Jürgen; Buchner, Benedikt (2021): Datentreuhänder. In: Datenschutz und Datensicherheit 16 (12), S. 777. Online verfügbar unter https://www.springerprofessional.de/datentreuhaender/19898830, zuletzt geprüft am 29.11.2022.

Lindner, Maximilian; Straub Sebastian; Kühne, Bettina (2021): How to Share Data? Data-Sharing-Plattformen für Unternehmen. Betriebswirtschaftliche und juristische Grundlagen, aktuelle Praxisprojekte, erste Handlungsempfehlungen. Eine Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie im Rahmen der Begleitforschung zum Technologieprogramm „Smarte Datenwirtschaft". Hg. v. iit. Berlin. Online verfügbar unter https://vdivde-it.de/de/publikation/how-share-data-data-sharing-plattformen-fuer-unternehmen.

Linnartz, Maria; Leckel, Anja (2020): Data Sharing im Supply-Chain-Management: Ein Assistenzsystem für die Bewertung und Gestaltung der Offenheit und des Vertrauensniveaus zwischen Supply-Chain-Partnern. In: Zeitschrift für wirtschaftlichen Fabrikbetrieb 115 (9), S. 563–566. DOI: 10.3139/104.112396.

Manohar, Siddharth; Ramesh, Aditi; Kapoor, Astha (2020): Data Stewardship – Taxonomy and use cases. Hg. v. Aapti Institute. Bengaluru. Online verfügbar unter https://thedataeconomylab.com/2020/06/24/data-stewardship-a-taxonomy/, zuletzt geprüft am 20.10.2022.

Marx, Uwe (2020): Der Maschinenbau hinkt digital hinterher. In: FAZ, 18.08.2020. Online verfügbar unter https://www.faz.net/aktuell/wirtschaft/der-maschinenbau-hinkt-digital-hinterher-16958284.html, zuletzt geprüft am 30.11.2022.

Mehr Fortschritt wagen. Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit. Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP (2021). Online verfügbar unter https://www.bundesregierung.de/breg-de/service/gesetzesvorhaben/koalitionsvertrag-2021-1990800, zuletzt geprüft am 29.11.2022.

Nagel, Lars; Lycklama, Douwe (2021): Design Principles for Data Spaces. International Data Spaces Association. Berlin. Online verfügbar unter https://design-principles-for-data-spaces.org/, zuletzt geprüft am 29.11.2022.

Naybzadeh, Milan (2021): Standards und Zertifizierungen für Cloud-Services. Hochschule Stralsund. Stralsund (SIMAT Arbeitspapiere, 13-21-039). Online verfügbar unter http://hdl.handle.net/10419/234595, zuletzt geprüft am 01.12.2022.

Nentwig, Stefan; Saft, Danilo; Taphorn, Christoph (2019): Mehrwerte aus Daten – Potenziale und Handlungsoptionen für den Mittelstand. Hg. v. EffizienzCluster Management. Köln. Online verfügbar unter https://www.mittelstand-digital.de/MD/Redaktion/DE/Publikationen/mehrwerte-aus-daten.pdf?__blob=publicationFile&v=2, zuletzt geprüft am 29.11.2022.

Niederée, Michael (2019): Data Sharing: Die Zukunft der Wertschöpfung in der Datenökonomie. Hg. v. KPMG.

Otto, Boris; Burmann, Anja (2021): Europäische Dateninfrastrukturen. In: Informatik Spektrum 44 (4), S. 283–291. DOI: 10.1007/s00287-021-01386-4.

Otto, Boris; Korte, Tobias; Azkan, Can; Spiekermann, Markus; Lis, Dominik; Gelhaar, Joshua et al. (2019a): Data Economy. Status Quo der deutschen Wirtschaft & Handlungsfelder in der Data Economy. Hg. v. Fraunhofer ISST. Dortmund. Online verfügbar unter https://www.demand-projekt.de/paper/DEMAND-DataEconomicsAndManagementOfDataDrivenBusiness(WhitePaper).pdf, zuletzt geprüft am 29.11.2022.

Otto, Boris; Österle, Hubert (2016): Corporate Data Quality: Voraussetzung erfolgreicher Geschäftsmodelle. Berlin, Heidelberg: Springer Gabler. Online verfügbar unter https://link.springer.com/book/10.1007/978-3-662-46806-7, zuletzt geprüft am 29.11.2022.

Otto, Boris; Steinbuss, Sebastian; Teuscher, Andreas; Lohmann, Steffen (2019b): IDS Reference Architecture Model. Version 3.0. Hg. v. International Data Spaces Association. Berlin.

Partsch, Christoph; Rump, Lauritz (2020): Auslegung der „angemessenen Geheimhaltungsmaßnahme" im Geschäftsgeheimnis-Schutzgesetz. In: Neue Juristische Wochenschrift 73 (3), S. 118–221.

Plattform Industrie 4.0 (2021): Vertragsleitfaden für Industrie 4.0 Plattformen. Online verfügbar unter https://www.plattform-i40.de/IP/Redaktion/DE/Downloads/Publikation/Leitfaden-Mustervertrag.html, zuletzt geprüft am 30.11.2022.

Rat für Informationsinfrastrukturen (Hg.) (2020): Datentreuhandstellen gestalten – Zu Erfahrungen aus der Wissenschaft. RFII-Stellungnahme. Göttingen. Online verfügbar unter https://rfii.de/download/rfii-stellungnahme-zu-datentreuhandstellen/, zuletzt geprüft am 29.11.2022.

Rat für Informationsinfrastrukturen (Hg.) (2021): Datentreuhänder: Potenziale, Erwartungen, Umsetzung. Workshop der AG Datentreuhänderschaft des RfII am 25. September 2020. Zusammenfassender Workshop-Bericht. Göttingen. Online verfügbar unter https://rfii.de/download/rfii-workshopbericht-datentreuhaender-potenziale-erwartungen-umsetzung-februar-2021/, zuletzt geprüft am 29.11.2022.

Richter, Frederick (2021a): Die Datentreuhand, das (noch) unbekannte Wesen. In: Datenschutz-Berater 45 (2), S. 47–48. Online verfügbar unter https://www.ruw.de/suche/dsb/Die-Datentreuhand-das-noch-unbekannte-Wesen-81e949b0f3674fffa994162f9b989f9f?crefresh=1, zuletzt geprüft am 29.11.2022.

Richter, Heiko (2021b): Europäisches Datenprivatrecht: Lehren aus dem Kommissionsvorschlag für eine „Verordnung über europäische Daten-Governance". In: Zeitschrift für Europäisches Privatrecht 29 (3), S. 634–666. Online verfügbar unter https://pure.mpg.de/pubman/faces/ViewItemOverviewPage.jsp?itemId=item_3337081, zuletzt geprüft am 29.11.2022.

Ringel, Michael; Baeza, Ramon; Grassl, Florian; Panandiker, Rahool; Harnoss, Johann (2020): The Most Innovative Companies 2020. The serial Innovation Imperative. Hg. v. Boston Consulting. Online verfügbar unter https://web-assets.bcg.com/img-src/BCG-Most-Innovative-Companies-2020-Jun-2020-R-4_tcm9-251007.pdf, zuletzt geprüft am 29.01.2022.

Robert Koch-Institut (2021): Neue Daten, neue Aufgaben: Beim ZfKD werden künftig auch klinische Daten aus den Krebsregistern zusammengeführt. Online verfügbar unter https://www.krebsdaten.de/Krebs/DE/Content/Publikationen/Kurzbeitraege/Archiv2021/2021_5_Kurzbeitraege_Gesetzesaenderung_zusammenfuehrung.html;jsessionid=14FEAB960C960A140839242D87A43E1C.internet051, zuletzt aktualisiert am 25.10.2022, zuletzt geprüft am 25.10.2022.

Röhl, Klaus-Heiner; Bolwin, Lennart (2021): Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse? Gutachten im Auftrag des BDI. Institut der deutschen Wirtschaft. Köln. Online verfügbar unter https://www.iwkoeln.de/studien/klaus-heiner-roehl-lennart-bolwin-wo-stehen-die-unternehmen-in-der-datennutzung-und-was-sind-ihre-groessten-hemmnisse.html, zuletzt geprüft am 30.11.2022.

Ruhaak, Anouk; Kapoor, Astha (2022): What is data stewardship, and how could it address questions of power imbalance in the data economy? Israel Public Policy Insitute. Online verfügbar unter https://www.ippi.org.il/what-is-data-stewardship-and-how-could-it-address-questions-of-power-imbalance-in-the-data-economy/, zuletzt aktualisiert am 03.10.2022, zuletzt geprüft am 25.10.2022.

Rusche, Christian; Krotova, Alevtina; Spiekermann, Markus (2019): Die ökonomische Bewertung von Daten. Hg. v. Institut der deutschen Wirtschaft. Köln (IW-Analysen, 129). Online verfügbar unter https://www.iwkoeln.de/studien/alevtina-krotova-christian-rusche-die-oekonomische-bewertung-von-daten.html, zuletzt geprüft am 29.11.2022.

Schneider, Ingrid (2022): Datentreuhandschaft durch Intermediäre. Chancen, Herausforderungen und Implikationen. Hg. v. Verbraucherzentrale NRW. Online verfügbar unter https://www.verbraucherforschung.nrw/sites/default/files/2022-02/zth-2-schneider-datentreuhandschaft-durch-intermediaere.pdf, zuletzt geprüft am 29.11.2022.

Schubert, Claudia (2018): §164 Rn. 59. In: Claudia Schubert, Christian Armbrüster, Frank Bayreuther, Jan Busche, Dorothee Einsele, Christina Stresemann und Harm Peter Westermann: Münchener Kommentar zum Bürgerlichen Gesetzbuch. 8. Auflage. München: C.H. Beck.

Schwartmann, Rolf (2020): Datenmanagement- und Datentreuhandsysteme. Ein Arbeitspapier der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2020. Hg. v. Weiß Steffen. Gesellschaft für Datenschutz und Datensicherheit e.V., Bundesministerium des Innern, für Bau und Heimat. Bonn. Online verfügbar unter https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und-datentreuhandsysteme.pdf?__blob=publicationFile&v=2, zuletzt geprüft am 30.11.2022.

Schwartmann, Rolf; Weiß, Steffen (Hg.) (2019): Entwurf für einen Code of Conduct zum Einsatz DS-GVO konformer Pseudonymisierung. Ein Arbeitspapier der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2019. Fokusgruppe Datenschutz. Online verfügbar unter https://www.gdd.de/downloads/aktuelles/whitepaper/Fokusgruppe_Datenschutz-Entwurf_CoC_Pseudonymisierung_V1.0.pdf, zuletzt geprüft am 30.11.2022.

Shiohira, Kelly; Dale-Jones, Barbara (2019): Interoperable Data Ecosystems. An international review to inform a South African innovation. Hg. v. JET Education Services und merSETA. Johannesburg. Online verfügbar unter https://www.jet.org.za/resources/interoperable-data-ecosystems.pdf, zuletzt geprüft am 30.11.2022.

Specht-Riemenschneider, Louise; Blankertz, Aline; Sierek, Paskal; Schneider, Ruben; Knapp, Jakob; Henne Theresa (2021): Die Datentreuhand – Ein Beitrag zur Modellierung und rechtlichen Strukturierung zwecks Identifizierung der Regulierungserfordernisse für Datentreuhandmodelle. In: MMR-Beilage (6), 25-48.

Specht-Riemenschneider, Louise; Kerber, Wolfgang (2022): Designing Data Trustees – A Purpose-Based Approach. Datentreuhänder – Ein problemlösungsorientierter Ansatz. Hg. v. Konrad-Adenauer-Stiftung. Berlin. Online verfügbar unter https://www.kas.de/documents/252038/16166715/Designing+Data+Trustees+-+A+Purpose-Based+Approach.pdf/ffadcb36-1377-4511-6e3c-0e32fc727a4d, zuletzt geprüft am 29.11.2022.

Spiekermann, Markus (2019): Chancen und Herausforderungen in der Datenökonomie. In: Aus Politik und Zeitgeschichte 69 (24-26), S. 16–21. Online verfügbar unter https://www.bpb.de/shop/zeitschriften/apuz/292341/chancen-und-herausforderungen-in-der-datenoekonomie/, zuletzt geprüft am 25.10.2022.

Spiekermann, Markus; Meisel, Lukas (2019): Datenmarktplätze. Plattformen für Datenaustausch und Datenmonetarisierung in der Data Economy. Hg. v. Fraunhofer ISST. Dortmund. Online verfügbar unter https://www.isst.fraunhofer.de/content/dam/isst-neu/documents/Publikationen/Datenwirtschaft/2019-2_ISST-Bericht_Datenmarktplaetze-ISSN-0943-1624.pdf, zuletzt geprüft am 29.11.2022.

Steinbuß, Sebastian (Hg.) (2021): Usage Control in the International Data Spaces. International Data Spaces Association. Berlin. Online verfügbar unter https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Position-Paper-Usage-Control-in-the-IDS-V3.pdf, zuletzt geprüft am 25.10.2022.

Stevens, Gunnar; Boden, Alexander (2022): Warum wir parteiische Datentreuhänder brauchen. Zum Modell der Datentreuhänderschaft als stellvertretende Deutung der Interessen individueller und kollektiver Identitäten. Hg. v. Verbraucherzentrale NRW. Düsseldorf. Online verfügbar unter https://www.verbraucherforschung.nrw/sites/default/files/2022-02/zth-06-stevens-boden-warum-wir-parteiische-datentreuhaender-brauchen.pdf, zuletzt geprüft am 30.11.2022.

Sundararajan, Preethi (2020): Developing standards for accountability in data stewardship. Aapti Institute. Online verfügbar unter https://thedataeconomylab.com/2020/09/18/developing-standards-for-accountability-in-data-stewardship/, zuletzt aktualisiert am 18.09.2020, zuletzt geprüft am 25.10.2022.

Tamanini, Jill-valerie; Koch, Matthias; Nass, Claudia (2020): Digitale Ökosysteme virtuell greifbar machen geht nicht? – Doch!. Fraunhofer IESE. Online verfügbar unter https://www.iese.fraunhofer.de/blog/digitale-oekosysteme-greifbar-machen/, zuletzt aktualisiert am 25.08.2020, zuletzt geprüft am 25.10.2022.

Vereinte Nationen (Hg.) (2021): Generic Statistical Business Process Model – GSBPM. Version 5.1. Genf. Online verfügbar unter https://statswiki.unece.org/display/GSBPM/GSBPM+v5.1, zuletzt geprüft am 30.11.2022.

Weber, Patrick; Groß, Nikolas; Grieser, Franziska (2021): Genossenschaften als rechtlicher Rahmen für IoT-Ökosysteme – Datengenossenschaften. In: Hohenheimer Genossenschaftsforschung, S. 34–47. Online verfügbar unter https://geno.uni-hohenheim.de/fileadmin/einrichtungen/geno/HGF/HGF_2021.pdf.

Weber, Patrick; Keller, Alexandra; Wertling, Maximilian; Renken, Sebastian; Groß, Nikolas; Kühlem, Melanie et al. (2022a): Checkliste Datengenossenschaft. Kooperative Geschäftsmodelle – Von der Initiierung über die Ausgestaltung der Kooperation bis hin zur eigenen Rechtsform. Baden-Württembergischer Genossenschaftsverband; Ferdinand-Steinbeis-Institut; Univ. Stuttgart. Online verfügbar unter https://www.datengenossenschaft.com/wp-content/uploads/2022/12/BWGV_Broschuere_Checkliste_Datengenossenschaften_Web.pdf, zuletzt geprüft am 10.01.2023.

Weber, Patrick; Werling, Maximilian; Tank, Ann; Baars, Henning (2022b): Institutionalisierung digitaler Ökosysteme in der Rechtsform einer Genossenschaft: Case Study im produzierenden Kontext. In: HMD Praxis der Wirtschaftsinformatik 59, S. 1353–1365. Online verfügbar unter https://link.springer.com/article/10.1365/s40702-022-00898-1, zuletzt geprüft am 07.12.2022.

Weichert, Thilo (2020a): Die Forschungsprivilegierung in der DS-GVO. In: Zeitschrift für Datenschutz 10, S. 18–23.

Weichert, Thilo (2020b): DS-GVO Art. 9 Rn. 129. In: Jürgen Kühling und Benedikt Buchner: Datenschutz-Grundverordnung BDSG. Kommentar. 3. Auflage. München: C.H. Beck.

Weirens, Jeffery; Bondar, Michael; Lee, Jennifer (2021): New models for building digital trust. An interview with MIT's Sandy Pentland. Deloitte. Online verfügbar unter https://www2.deloitte.com/us/en/insights/topics/digital-transformation/the-importance-of-digital-trust-qa.html, zuletzt aktualisiert am 05.04.2021, zuletzt geprüft am 25.10.2022.

ZVEI (2022): Data Sharing Models in the Electro and Digital Industry. Positionspapier. Frankfurt a.M. Online verfügbar unter https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2022/Juni/Data_Sharing_Models/ZVEI_Data_Sharing_Models_in_the_Electro_and_Digital_Industry.pdf, zuletzt geprüft am 29.11.2022.

ANHANG

ANHANG

In Deutschland tätige Datentreuhänder-Projekte

Die folgenden Projekte und Plattformen umfassen in Deutschland geplante bzw. nutzbare Datentreuhänder-Angebote sowohl im engeren als auch im weiteren Verständnis. Alle Informationen beruhen auf Angaben der Anbieter.

Konzeptionsphase: Datentreuhänder in Konzeption, Entwicklung oder Pilotierung ohne größere Anzahl externer Nutzerinnen und Nutzer

Aviation Data Hub	
Anwendungsbereich	Produktdaten
Trägerschaft	AVIATION DataHub GmbH (Lufthansa AG)
Marktreife	Aufbauphase
Informationen	www.aviation-datahub.com
EuroDat	
Anwendungsbereich	Finanzdaten
Konsortium	d-fine GmbH, Atos Information Technology GmbH, Deloitte GmbH, DFKI, Univ. Frankfurt, Leibniz-Institut für Finanzmarktforschung SAFE e.V., Lexemo GmbH, TechQuartier, T-Systems International GmbH, Univ. des Saarlandes, Wirtschaftsministerium Hessen, Zentrum verantwortungsbewusste Digitalisierung
Marktreife	Forschungsprojekt (BMWK)
Informationen	www.eurodat.org
FAIRWinDS	
Anwendungsbereich	Felddaten von Windenergieanlagen
Konsortium	Fraunhofer IWES, Fraunhofer IAIS, Fraunhofer IEE, Fraunhofer IMW, Fraunhofer ISST
Marktreife	Forschungsprojekt (BMBF)
Informationen	www.iwes.fraunhofer.de/de/forschungsprojekte/aktuelle-projekte/fairwinds.html
MANDAT	
Anwendungsbereich	Unternehmensdaten
Konsortium	DATEV eG, Univ. Erlangen-Nürnberg, KIT
Marktreife	Forschungsprojekt (Bundesministerium für Forschung und Bildung, BMBF)
Informationen	www.datev.de/web/de/presse/pressemeldungen/meldungen-2022/sensible-unternehmensdaten-selbstbestimmt-und-sicher-teilen
S3I-X	
Anwendungsbereich	Daten aus der Forstwirtschaft
Konsortium	RIF Institut für Forschung und Transfer, RWTH Aachen, der nexoma GmbH, ComConsult GmbH
Marktreife	Forschungsprojekt (Bundesministerium für Forschung und Bildung, BMBF)
Informationen	www.kwh40.de/s3i-x

TRANSIT	
Anwendungsbereich	Logistikdaten
Konsortium	Univ. Leipzig, Institut für Angewandte Informatik, fox-Courier GmbH
Marktreife	Forschungsprojekt (Bundesministerium für Forschung und Bildung, BMBF)
Informationen	https://transit-project.de/
Trusted Data Center	
Anwendungsbereich	Betriebsdaten von Automobilen
Trägerschaft	TÜV Rheinland
Marktreife	Pilotprojekte in Vorbereitung
Informationen	www.tuv.com/landingpage/de/smart-mobility/themen/trusted-data-center.html

Tabelle 9 Datentreuhänder-Projekte in Konzeption, Entwicklung oder früher Pilotierung

Aufbauphase: Datentreuhänder im Aufbau mit erkennbarer Anzahl externer Nutzerinnen und Nutzer

Cen Trust	
Anwendungsbereich	Gesundheitsdaten
Trägerschaft	Bundesdruckerei GmbH
Marktreife	Regelbetrieb für erste medizinische Forschungsprojekte
Informationen	www.bundesdruckerei-gmbh.de/de/loesungen/datentreuhaender
Logistics.Cloud	
Anwendungsbereich	Logistikdaten
Trägerschaft	Lobster Logistics Cloud GmbH
Marktreife	Regelbetrieb für erste Unternehmenskunden
Informationen	www.logistics.cloud
Mobility Data Space	
Anwendungsbereich	Mobilitätsdaten
Trägerschaft	DRM Datenraum Mobilität GmbH
Marktreife	Regelbetrieb mit ersten Datenangeboten
Informationen	https://mobility-dataspace.eu/de#c16

Tabelle 10 Im Aufbau befindliche Datentreuhänder-Angebote im frühen Praxisbetrieb

Regelbetriebsphase: etablierte Datentreuhänder-Angebote im Realbetrieb
Nähere Angaben zu den hier genannten Plattformen finden sich im Kapitel 6.

Caruso Dataplace	
Anwendungsbereich	Fahrzeugdaten
Trägerschaft	Caruso GmbH
Marktreife	Regelbetrieb
Informationen	www.caruso-dataplace.com
CSDR	
Anwendungsbereich	Gesundheitsdaten
Trägerschaft	Anaqua Inc.
Marktreife	Regelbetrieb
Informationen	www.clinicalstudydatarequest.com
Data Intelligence Hub	
Anwendungsbereich	Domänenübergreifend, kein spezifischer Anwendungsbereich
Trägerschaft	T-Systems International GmbH
Marktreife	(Früher) Regelbetrieb
Informationen	https://dih.telekom.net
Hilo HRM	
Anwendungsbereich	Risikodaten aus der Schifffahrt
Trägerschaft	Hilo Maritime Risk Management Ltd.
Marktreife	(Früher) Regelbetrieb
Informationen	www.hilomrm.com
Otonomo	
Anwendungsbereich	Fahrzeugdaten
Trägerschaft	Otonomo Technologies Ltd.
Marktreife	Regelbetrieb
Informationen	https://otonomo.io
SPOCC	
Anwendungsbereich	Produktdaten
Trägerschaft	European-Clearing-Center GmbH & Co. KG
Marktreife	Regelbetrieb
Informationen	www.spocc.io

Vivli	
Anwendungsbereich	Fahrzeugdaten
Trägerschaft	Caruso GmbH
Marktreife	Regelbetrieb
Informationen	www.caruso-dataplace.com
VTH eData-Pool	
Anwendungsbereich	Produktdaten für technische Bedarfsartikel
Trägerschaft	Fachverband für den technischen Handel in Deutschland, Österreich und der Schweiz: VTH Verband Technischer Handel e.V., Düsseldorf
Marktreife	Regelbetrieb
Informationen	www.vth-verband.de/vth-eservices/vth-edata-pool

Tabelle 11 Etablierte Datentreuhänder-Angebote im Regelbetrieb