technopolis group

RWTH AACHEN UNIVERSITY

LAW & INNOVATION

Fraunhofer ISI

Beauftragt durch:

Bundesministerium für Forschung, Technologie und Raumfahrt

Finanziert von der Europäischen Union
NextGenerationEU

September 2025

Datentreuhänder als Schlüssel zum Datenteilen

Ansätze, Herausforderungen und Empfehlungen für die Umsetzung

September 2025

Datentreuhänder als Schlüssel zum Datenteilen

Ansätze, Herausforderungen und Empfehlungen für die Umsetzung

Technopolis Group: Stephan Kreutzer, Prof. Dr. Thomas Heimer, Fiona Bauer, Lea Rabe
Fraunhofer ISI: Prof. Dr. Knut Blind, Dr. Nicholas Martin
Law & Innovation: Prof. Dr. Max von Grafenstein
GRI GmbH, RWTH Aachen: Dr. Rita Streblow, Junsong Du, Joel Schölzel

Die Studie wurde im Auftrag des Bundesministeriums für Forschung, Technologie und Raumfahrt durchgeführt. Sie wird aus dem europäischen Wiederaufbaufonds „NextGenerationEU“ im Rahmen der Aufbau- und Resilienzfazilität refinanziert.

RWTH Aachen University
E.ON Energieforschungszentrum
Lehrstuhl für Gebäude- und Raumklimatechnik
Mathieustr. 10
D-52074 Aachen

Verfügbar über das Institutionelle Repositorium der RWTH Aachen University
DOI: https://doi.org/10.18154/RWTH-2025-07886

Inhaltsverzeichnis

Abbildungen

Abkürzungsverzeichnis

Abkürzung	Definition
API	Application Programming Interface
BStatG	Bundesstatistikgesetz
B2B	Business-to-Business
B2C	Business-to-Consumer
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation Électrotechnique
C2B	Consumer-to-Business
DSGVO	Datenschutz-Grundverordnung
DGA	Data Governance Act
DMA	Digital Markets Act
DNG	Datennutzungsgesetz
DSA	Digital Services Act
DSGVO	Datenschutz-Grundverordnung
EHDS	European Health Data Space
ETSI	European Telecommunications Standards Institute
FDZ	Forschungsdatenzentren
FHIR	Fast Healthcare Interoperability Resources
GWB	Europäischer Gesundheitsdatenraum (engl. 'European Health Data Space')
IDSA	International Data Spaces Association
KI	Künstliche Intelligenz
NIS	Netz- und Informationssysteme
PIMS	Personal Information Management Systems
SOLID	Social Linked Data
TTDSG	Telekommunikation-Telemedien-Datenschutzgesetz
UWG	Gesetz gegen den unlauteren Wettbewerb

Glossar

Begriff	Definition
Data Broker	Data Broker (auf Deutsch: Datenmakler) sind Unternehmen oder Einzelpersonen, die personenbezogene Daten sammeln, analysieren, zusammenführen und verkaufen oder anderweitig weitergeben – meist ohne direkten Kontakt zu den betroffenen Personen. Während sich andere Typen von Datenintermediären meist auf das reine Teilen von Rohdaten beschränken, bieten Data Broker zusätzlich auf den Daten aufbauende Analyseergebnisse als Dienstleistung an.
Datengebende (engl. 'data providers')	Datengebende sind solche natürlichen oder juristischen Personen, die die technisch-organisatorische Kontrolle über den Zugang zu den Daten innehaben und gewähren. Der Begriff hebt die aktive Rolle beim Datenteilen hervor. Datengebende können zugleich Drittbetroffene sein, wenn sie zwar die Kontrolle über den Zugang zu den Daten innehaben, sich die Daten jedoch (auch) auf sie selbst beziehen. Die Begriffe Datenhalter bzw. -inhaber werden häufig synonym verwendet, legen aber (im Unterschied zum Begriff Datengebende), den Fokus eher auf das statische Halten von Daten als auf das dynamische Teilen.
Datenintermediär (engl. 'data intermediary')	In der allgemeinen Diskussion ist der Begriff des Datenintermediärs ein Sammelbegriff für verschiedene Modelle oder Instrumente, die alle darauf abzielen, den Datenaustausch zwischen (mindestens zwei) Akteuren zu vereinfachen, durchzuführen oder zu begleiten. Unter die Leistungen eines Datenintermediärs fallen z. B. das Gewähren eines sicheren Datenaustauschs oder das Bekanntmachen verfügbarer Daten (Deutsche Industrie- und Handelskammer, o. J.). Der Begriff des Datentreuhänders ist eine Sonderform bzw. eine Unterkategorie von Datenintermediären.
Datenmodell	Ein Datenmodell ist die formale Abbildung der Informationsobjekte der betrachteten Diskurswelt mittels ihrer Attribute und Beziehungen. Ziel ist die eindeutige Definition und Spezifikation der in einem Informationssystem zu verwaltenden Objekte, ihrer für die Informationszwecke erforderlichen Attribute und der Zusammenhänge zwischen verschiedenen Informationsobjekten (Gabler Wirtschaftslexikon, o. J.).
Datennutzende (engl. 'data users')	Datennutzende sind natürliche oder juristische Personen, die durch eine rechtmäßige Übertragung oder Freigabe Zugriff auf bestimmte Daten erhalten und diese für eigene Zwecke analysieren, verarbeiten oder weiterverwenden.
Datenökosystem	Ein Datenökosystem wird im Folgenden als ein Umfeld begriffen, in dem verschiedene Akteure, z. B. Datengebende, Datennutzende, Datentreuhänder, zusammenkommen, um Daten zu produzieren, anzubieten, zu finden und zu „konsumieren" (d. h. weiterzuverwenden, zu verarbeiten, anzureichern, zu archivieren, zu publizieren, Entscheidungen darauf zu fällen etc.) (Putnings, 2021).
Datenraum	Dezentralisiertes Datenökosystem, das auf gemeinsam vereinbarten Technologien, Werten, Standards oder Schnittstellen basiert und einen effektiven und vertrauenswürdigen Austausch von Daten zwischen den Teilnehmenden ermöglicht. Ziel ist die Schaffung mehrseitiger Märkte, die Steigerung bzw. Verbesserung der Datenverfügbarkeit und bessere Datenzugriffsmöglichkeiten der Teilnehmenden. Bausteine eines Datenraums umfassen Bedingungen und Mechanismen in Verbindung mit Datenangeboten, so für die Preisgestaltung und Vertragsprozesse sowie die Veröffentlichung und das Auffinden von Datenangeboten (Otto et al., 2022). Innerhalb des Ökosystems werden verschiedene Rollen definiert, die sich in die drei Gruppen (i) Governance, (ii) Teilnehmende und (iii) unterstützende Dienstleistungen einteilen lassen. In einem Datenraum, wie oben definiert, übernimmt die Governance-Ebene (bei Gaia-X auch unter der Bezeichnung des Föderators) Funktionen wie z. B. das Identitätsmanagement, Zertifizierung und die Orchestrierung des Datenraums im Allgemeinen (Otto et al., 2022; Kraemer et al., 2023). Ein solcher Föderator erinnert somit stark an das breit angesetzte Begriffsverständnis eines Datentreuhänders. Datenräume können offen oder geschlossen sein (in verschiedenen Abstufungen), der Zugang kann diskriminierend oder nichtdiskriminierend erfolgen.
Datensouveränität	Datensouveränität bezieht sich auf das Konzept, wonach natürliche Personen das Recht und die Kontrolle über ihre eigenen Daten haben sollten. Insbesondere sollte eine natürliche

Begriff	Definition
	Person selbst entscheiden, wie die Daten, die ihr gehören oder zu ihrer Identifizierung verwendet werden können, erhoben, gespeichert, verarbeitet und geteilt werden. Die DSGVO enthält keine eindeutige Definition der Datensouveränität, aber die entsprechende Vorgabe wird bereits vorgesehen. Es wird in Art. 5 DSGVO klar darauf hingewiesen, dass zum Schutz der Rechte und Freiheiten der betroffenen Person die Verarbeitung, Erhebung und Speicherung der personenbezogenen Daten kontrolliert werden müssen.
Datentreuhänder (engl. 'data trustee')	Neutraler Intermediär, der einen vertrauensvollen und fairen Ausgleich der Interessen der beteiligten Akteure – Datengebende sowie Datennutzende – ermöglicht, gegebenenfalls neue Vertrauensbeziehungen anbahnt, den technischen und organisatorischen Zugang zu qualitativ hochwertigen Daten unter Wahrung des Datenschutzes sowie Interoperabilität garantiert (BMBF, 2021).
Datentreuhand-modell (engl. 'data trust model')	Spezifische technische, rechtliche und organisatorische bzw. geschäftliche Ausformung eines Datentreuhänders.
Datenvermittlungs-dienst	Im Sinne von Art. 2 Nr. 11 DGA ist ein Datenvermittlungsdienst (engl.: data intermediary service) ein Dienst zur Herstellung einer Geschäftsbeziehung zwischen einer unbestimmten Anzahl von Datengebenden und Datennutzenden zur Ermöglichung gemeinsamer Datennutzung. Je nachdem, welche Funktionen sie erfüllen, können manche Datentreuhandmodelle rechtlich als Datenvermittlungsdienste gelten, andere wiederum nicht. Eine Diskussion der rechtlichen Perspektive auf die Rolle des DGA bei der rechtlichen Absicherung von Datentreuhandmodellen findet sich in Kapitel 2.3.
(Anwen-dungs)-Domäne	Bezeichnet ein spezifisches Fach- oder Branchengebiet, z. B. Mobilität, Energie, Klima.
Drittbetroffene	Drittbetroffene sind natürliche oder juristische Personen, auf die sich Daten beziehen, ohne dass sie die technisch-organisatorische Kontrolle über den Zugriff auf diese Daten und die Verwendung haben. Das ist häufig der Fall bei personenbezogenen Daten, die einerseits von Datengebenden technisch verwaltet werden (z. B. Mobilitätsunternehmen), sich dabei aber auf Dritte beziehen (z. B. die Nutzenden des Mobilitätsangebots).
Föderiertes Lernen	Im Kontext Künstlicher Intelligenz bezieht sich der Begriff auf ein maschinelles Lernverfahren, bei dem KI-Modelle trainiert werden, ohne dass die zugrunde liegenden Daten zentralisiert werden müssen. Stattdessen verbleiben die Daten lokal auf den Endgeräten oder bei den Datenhaltern, und nur die Modellparameter oder Modellaktualisierungen werden mit einem zentralen Server ausgetauscht. Ziel ist es, die Privatsphäre der Daten zu schützen und gleichzeitig ein leistungsfähiges Modell zu entwickeln (Kairouz, 2021).
Neutralität unter dem DGA	Neutralitätsverpflichtung für Datenvermittlungsdienste (siehe Art. 12 lit. a DGA, d. h. klare und strukturelle Trennung von Datenvermittlung und -nutzung gemäß Erwägungsgrund Nr. 32). Der Datenvermittlungsdienst muss zur Vorbeugung von Interessenkonflikten von einer unabhängigen juristischen Person erbracht werden, d. h. rechtlich unabhängig sein. Wirtschaftliche Unabhängigkeit wird dagegen nicht verlangt. Der Anbieter des Datenvermittlungsdiensts darf jedoch seine Leistung nicht von der Nutzung anderer eigener Dienste abhängig machen, vergleiche Art. 12 lit. b DGA und Erwägungsgrund 33 – Kopplungsverbot (Hennemann/von Ditfurth, 2022). Demgegenüber verlangt § 26 Abs. 1 Nr. 2 TTDSG für den Bereich der Einwilligungsagenten („Anerkannte Dienste zur Einwilligungsverwaltung"), dass der Einwilligungsagent „kein wirtschaftliches Eigeninteresse an der Erteilung der Einwilligung und an den verwalteten Daten haben (darf) und unabhängig von Unternehmen (… / sein muss), die ein solches Interesse haben können". Ob damit ein wirtschaftliches Eigeninteresse noch möglich ist, ist zweifelhaft.
Personal Information Management Systems (PIMS)	Softwarelösungen, die es Einzelpersonen ermöglichen, ihre persönlichen Daten sicher zu verwalten und sie nach eigenem Ermessen mit anderen zu teilen. Anbieter von Online-Diensten und Werbetreibende müssen mit PIMS interagieren, wenn sie diese Daten verarbeiten wollen. Bei PIMS handelt es sich um Geschäftsmodelle, die im Auftrag von Verbraucherinnen und Verbrauchern gegenüber Dritten agieren (Schneider, 2022).

Begriff	Definition
	PIMS wird im Rahmen der Begleitforschung als möglicher technischer Baustein eines Datentreuhänders verstanden, aber nicht als ein Datentreuhändermodell.
Semantik	Semantik beschreibt die Bedeutung von Daten und deren Beziehungen zueinander. Sie geht über die reine Struktur (Syntax) hinaus und befasst sich mit der inhaltlichen Interpretation von Daten. Durch semantische Anreicherung werden Daten maschinenlesbar und -interpretierbar, was die automatisierte Verarbeitung und Integration heterogener Datenquellen und kontextbezogene Analysen ermöglicht.
Sichere Datenverarbeitungsumgebung	Ein technisch-organisatorischer Verarbeitungsrahmen, in dem nicht nur der Zugriff auf Daten, sondern auch deren Nutzung (in unterschiedlichem Ausmaß) kontrolliert werden kann. Er bildet einen wichtigen Mechanismus, um den Kontrollverlust der Datengebenden über ihre Daten zu verhindern und damit das Wert-Risiko-Dilemma zu überwinden.
Sektor	Bezeichnet die Einteilung nach gesellschaftlichen oder organisatorischen Bereichen, etwa Wirtschaft, Wissenschaft, Zivilgesellschaft, Politik und Verwaltung.
Wert-Risiko-Dilemma	Eine Situation, in der Daten deshalb nicht geteilt werden, weil zum Zeitpunkt der Datenweitergabe die Datenteilenden den Mehrwert der Datennutzung als geringer als die (Compliance-)Risiken und Kosten ansehen; die Situation wird als Dilemma wahrgenommen, weil sich der Mehrwert der Daten oft erst aus der konkreten Datennutzung ergibt, sich die Risiken und Kosten aber bereits zuvor mit Weitergabe der Daten an den Datennutzenden realisieren (v. Grafenstein, 2022).

Executive Summary (Deutsch)

Die vorliegende Studie präsentiert die **Ergebnisse einer dreijährigen Begleitforschung** zu den vom Bundesministerium für Forschung, Technik und Raumfahrt (BMFTR) geförderten „Projekten zur Entwicklung und praktischen Erprobung von Datentreuhandmodellen in den Bereichen Forschung und Wirtschaft". Datentreuhänder sind in diesem Zusammenhang als intermediäre Strukturen zu verstehen, die den technisch-organisatorischen Austausch von Daten zwischen Datengebenden und -nutzenden bewerkstelligen.

Im Rahmen der Begleitforschung erfolgte zunächst eine **Bestandsaufnahme** der geförderten Pilotprojekte und anderer Anwendungsbeispiele sowie der wissenschaftlichen Literatur zur möglichen Rolle von Datentreuhändern in Datenökosystemen. Darauf aufbauend identifizierte und systematisierte die Begleitforschung **zentrale Herausforderungen** und **erste Lösungsansätze** für den Aufbau und Betrieb von Datentreuhändern. Die Analyse der eigens erhobenen Daten sowie die konzeptionellen Arbeiten der Begleitforschung orientierten sich dabei an vier **Querschnittsthemen**, die in ihrer Wechselwirkung untersucht wurden: 1. **Technische Infrastruktur, 2. Rechtliche Rahmenbedingungen, 3. Geschäfts- und Betriebsmodellentwicklung sowie 4. Akzeptanz, Standardisierung, Zertifizierung und Skalierung**. Die Befunde der Begleitforschung sowie die daraus abgeleiteten **Handlungsempfehlungen** richten sich nicht nur an bestehende und künftige Betreiber von Datentreuhändern, sondern auch an politische Entscheidungsträger und Akteure aus Wissenschaft und Wirtschaft sowie Zivilgesellschaft, die am Aufbau einer funktionsfähigen Datenökonomie beteiligt sind. Daneben richtet sich die Studie an alle Interessierten an der Schnittstelle von Forschung, Innovation und Digitalisierung.

Ausgangshypothese der Begleitforschung war, dass Daten aufgrund eines ungünstigen Wert-Risiko-Verhältnisses nur begrenzt innerhalb und zwischen Sektoren (Wissenschaft, Wirtschaft) geteilt werden, auch wenn das vermehrte Teilen von Daten aus gesamtgesellschaftlicher und insbesondere innovationspolitischer Sicht wünschenswert wäre. Demnach schrecken potenzielle Datengebende oftmals davor zurück, ihre Daten zu teilen, da sie einen Kontrollverlust bezüglich der weiteren Verwendung dieser Daten fürchten. Außerdem halten vermeintliche und tatsächliche Compliance-Risiken Datengebende und Datennutzende gleichermaßen in vielen Fällen vom Datenteilen ab. Gleichzeitig ist der mögliche Wert, der sich sowohl für Datengebende als auch -nutzende aus dem Datenteilen ergeben kann, oftmals schwer zu bemessen. Diesen Umstand fasst die Begleitforschung unter dem Begriff **Wert-Risiko-Dilemma** zusammen.

Als neutrale Instanzen haben **Datentreuhänder** das Potenzial, einen fairen Interessensausgleich zwischen Datengebenden und -nutzenden zu ermöglichen, gegebenenfalls neue Vertrauensbeziehungen anzubahnen und den technisch-organisatorischen Zugang zu qualitativ hochwertigen Daten unter Wahrung des Datenschutzes sowie der Interoperabilität zu garantieren. Diese **These** lässt sich anhand der konzeptionellen Überlegungen theoretisch und in Anbetracht der empirischen Befunde praktisch **validieren**. Theoretisch lässt sich herleiten, dass **Datentreuhänder den Wert des Datenteilens positiv beeinflussen** und das damit einhergehende **Risiko des Kontrollverlusts über die geteilten Daten** für die Datengebenden sowie Compliance-Risiken für Datengebende und -nutzende **senken** können. Voraussetzung dafür ist, dass Datentreuhänder Vertrauen zwischen Datengebenden und -nutzenden schaffen und sich selbst als vertrauenswürdige Akteure platzieren, dass sie rechtliche Unsicherheiten reduzieren und Mehrwerte für Datengebende und -nutzende ermöglichen.

Die empirischen Auswertungen der Begleitforschung führen zu folgenden **Kernbefunden**: Die BMFTR-geförderten Pilotprojekte konnten insbesondere technische und rechtliche Anforderungen an den Aufbau von Datentreuhändern in verschiedenen Domänen identifizieren und entsprechende Lösungsansätze erproben. Gleichzeitig bestätigen die in den Pilotprojekten aufgeworfenen Fragen und weiteren Befunde der Begleitforschung, dass bestimmte technische, rechtliche und wirtschaftliche Herausforderungen einem breiten Einsatz

von Datentreuhändern derzeit noch entgegenstehen. Lösungsansätze für einige dieser Herausforderungen konnten von der Begleitforschung, wie im Folgenden dargestellt, empirisch identifiziert und konzeptionell weiterentwickelt werden.

Zunächst ist festzustellen, dass Datenteilen vor allem dann für Datengebende und -nutzende interessant ist, wenn konkrete und wertvolle Anwendungsfälle für die so geteilten Daten klar erkennbar sind. Für den Erfolg von Datentreuhändern ist es daher aus Sicht der Begleitforschung essenziell, dass diese die relevanten Datenbestände, Branche(n), Technologien, Märkte, Geschäftsmodelle und Kulturen der Akteure im Datenökosystem sehr gut kennen. Außerdem sollten sie ein gewisses Standing bei den relevanten Akteuren haben, um **akzeptiert** zu werden. Dies wiederum hat Implikationen für die zu wählende Geschäftsstrategie und mögliche Skalierung des jeweils gewählten Datentreuhandmodells.

Aus rechtlicher Sicht ist durch die Betreiber von Datentreuhändern zunächst zu klären, wer über den Zugriff auf und die Verwendung von zu teilenden Daten bestimmt und welche Compliance-Risiken sich hieraus für Datengebende und -nutzende ergeben. Aus rechtlicher Sicht ist eine wesentliche Funktion von Datentreuhandmodellen, die Compliance-Risiken der Datenteilenden sowie die mit der Kontrolle dieser Risiken üblicherweise verbundenen Kosten zu reduzieren. Vor diesem Hintergrund entwickelte die Begleitforschung eine Typologie von Datentreuhandmodellen, welche Fallgruppen nach der Intensität der Compliance-Risiken und dem erforderten Umfang an Kontrollmechanismen klassifiziert. Je nach Risiko können die Daten entweder der Allgemeinheit als offene Daten bereitgestellt, nur bestimmten vertrauenswürdigen Datennutzenden zugänglich gemacht oder gar nicht als Rohdaten, sondern ausschließlich in Form von darauf aufbauenden Analyseergebnissen zwischen Datengebenden und -nutzenden geteilt werden. Einem Datentreuhänder kommt dann die Funktion zu, die entsprechenden rechtlichen, technischen und organisatorischen Infrastrukturen zur Verfügung zu stellen. Ein wichtiger Begriff, der diese Infrastrukturen beschreibt, sind die sogenannten sicheren Datenverarbeitungsumgebungen.

Ein zentraler Befund der Begleitforschung ist es, dass der aktuelle auf das Teilen von Daten zugeschnittene deutsche wie europäische **Rechtsrahmen** (insbesondere der Data Governance Act bzw. DGA) zwar wichtige Schritte in Richtung vertrauensfördernder Infrastrukturen macht. Um vor allem die Rechtssicherheit für Datengebende und -nutzende sowie Datentreuhänder in der Praxis ui erhöhen, müsste der Rechtsrahmen allerdings noch stringenter und konsistenter auf dieses Ziel ausgerichtet werden. Denn die Rechtssicherheit zeigt sich in den Pilotprojekten sichtbar als ein Hemmnis für den Aufbau von Datentreuhändern und Datenökosystemen. Die von der Begleitforschung auf empirischer Basis konzeptionell aufgestellten Fallgruppen können dabei helfen, das je nach Intensität der jeweils vorliegenden Risiken und möglichen Interessenskonflikte zwischen Datengebenden und -nutzenden am besten geeignete Datentreuhandmodell zu identifizieren.

Aus den rechtlichen Anforderungen für Datentreuhandmodelle lassen sich **technische Bausteine** für deren Umsetzung ableiten. Diese Bausteine bilden das fundamentale Gerüst, um den vertrauensvollen Austausch und die Nutzung von Daten zu ermöglichen. Auch wenn die konkrete Ausgestaltung je nach Anwendungsfeld variieren kann, müssen Datentreuhänder dabei jedoch immer bestimmte Anforderungen in Bezug auf Interoperabilität, Datensicherheit und Datenminimierung erfüllen, um sich am Markt etablieren zu können. Interoperabilität bezieht sich hierbei auf Schnittstellen und Datenmodelle für eine reibungslose Datenübertragung. Unter dem Gesichtspunkt der Datensicherheit müssen geeignete Maßnahmen für die Authentifizierung, Autorisierung, Protokollierung, Datenverschlüsselung und Zertifizierung ergriffen werden. Datenminimierung bezieht sich darauf, dass nur jene Informationen offengelegt werden, die für den jeweiligen Anwendungsfall unabdingbar sind. Die Begleitforschung präsentiert einen Baukasten, der je nach Anwendungsfall geeignete Bausteine zur Erfüllung dieser zentralen Anforderungen enthält.

Daneben spielen technische, rechtliche und organisatorische **Standards** bei der erfolgreichen Etablierung von Datentreuhändern eine Rolle. Es zeigt sich, dass Vertrauen nicht allein durch

die Wahl geeigneter technischer Bausteine entsteht, sondern meist nur im Zusammenhang mit transparenten Prozessen, Zertifizierungen, glaubwürdigen Betreibern und partizipativen Governance-Strukturen. Insgesamt steht die Entwicklung von Standards sowohl für Daten(teilen) als auch für Datentreuhänder noch am Anfang. Die Begleitforschung konnte in den untersuchten Pilotprojekten verschiedene Ansätze zur Standardisierung des Datenaustauschs identifizieren, insbesondere im Bereich Medizin- und Gesundheitsforschung sowie in der Forstwirtschaft. Auf Standards können wiederum **Zertifizierungen** aufgesetzt werden, die Governance, Finanzierung, Datenzugangsregeln, Datensicherheit, Ethik und Nachhaltigkeit sowie Qualität der durch einen Datentreuhänder geteilten Daten ausweisen. Entsprechende Maßnahmen werden von den Pilotprojekten für wünschenswert gehalten, finden sich jedoch bislang noch nicht in der Praxis. Die aktuell unzureichende Verfügbarkeit allgemein akzeptierter Standards für Daten, Datenteilen und Datentreuhänder stellt eine Hürde sowohl für die weitere Entwicklung der einzelnen Datentreuhänder als auch für eine stärkere Interoperabilität zwischen verschiedenen Datentreuhändern dar. Als vergleichsweise wichtige Entwickler standardisierter Komponenten haben z. B. **Gaia-X** und die **International Data Spaces Association** aber auch andere Datenrauminitiativen und -technologien wie **SOLID** (Social Linked Data) mittelfristig das Potenzial, die Entwicklung zu stärkerer Interoperabilität zu unterstützen.

Auch die Entwicklung tragfähiger **Geschäftsmodelle** für den langfristigen Betrieb von Datentreuhändern gestaltet sich in der Pilotprojekt-Praxis herausfordernd. Es bestehen Unsicherheiten bei der Bepreisung von Daten, der langfristig tragfähigen Finanzierung von Datentreuhändern sowie bei der Wahl eines geeigneten Betriebsmodells für diese. Grundsätzlich sind die wenigsten Betreiber eines Datentreuhänders rein monetär motiviert – vielmehr hoffen diese meist, neue datenbasierte Anwendungsfälle zu ermöglichen, die wiederum ihnen und anderen Akteuren im Datenökosystem zugutekommen. Dennoch müssen die Kosten für den Betrieb eines Datentreuhänders zumindest gedeckt werden. Dies kann sowohl mittels for-profit- als auch über non-profit-Modelle organisiert werden. Je nach Anwendungsdomäne wird von den Pilotprojekten eine öffentliche Trägerschaft bevorzugt, etwa in der Domäne der Medizinforschung, oder aber privatwirtschaftliche Träger, wie etwa in der Energiebranche oder der Wohnungswirtschaft. Bei der Finanzierung des Datentreuhänders werden von den Pilotprojekten tendenziell Abonnementmodelle gegenüber transaktionsbasierten pay-per-use-Ansätzen bevorzugt.

Eine europaweite sowie domänenübergreifende **Skalierung** von Datentreuhandmodellen ist derzeit noch kaum absehbar, wird jedoch von an Datentreuhändern beteiligten Akteuren für wünschenswert erachtet. Skalierung wird dabei von diesen eher als Zusammenschluss föderierter, aber eigenständiger Datentreuhänder verstanden, denn als Expansion einzelner Datentreuhänder in neue geografische oder sektorale Märkte. Die technische Interoperabilität von Datentreuhändern – etwa durch die Standardisierung von technischen Bausteinen – ist somit eine zentrale Voraussetzung, um Skalierung zu ermöglichen.

Insgesamt bestätigen die Befunde die Eingangshypothese der Begleitforschung, wonach Datentreuhänder ein mögliches Instrument zur positiven Beeinflussung des Wert-Risiko-Dilemmas beim Datenteilen darstellen. Dabei wird sich aller Voraussicht nach nicht das eine, domänen- und sektorübergreifend zu bevorzugende Datentreuhandmodell durchsetzen. Vielmehr ist davon auszugehen, dass sich ein modularer Werkzeugkasten aus rechtlichen, technischen und organisatorischen Bausteinen etablieren wird. Hierzu leistet die Begleitforschung mit ihrer Systematisierung von Fallgruppen des Datenteilens und entsprechend zu wählenden Funktionen eines Datentreuhänders einen Beitrag.

Aus den Befunden lassen sich erste **Handlungsempfehlungen** für Datentreuhandbetreiber, politische Entscheidungsträger, Vollzugsbehörden und die öffentliche Verwaltung, sowie für Wissenschaft und Wirtschaft ableiten. Diese Empfehlungen liegt die Erkenntnis der Begleitforschung zu Grunde, dass neben der geeigneten Wahl von Lösungen durch die Betreiber die rechtlichen, technischen und ökonomischen Rahmenbedingungen maßgeblich

die Erfolgsaussichten von Datentreuhändern beeinflussen. Das gemeinsame Ziel aller Akteure sollte dabei die Überwindung des eingangs aufgeworfenen Wert-Risiko-Dilemmas sein.

Datentreuhandbetreiber sollten vor allem klar definieren, welchen Mehrwert und welche Funktionen sie für Datengebende und -nutzende bieten. Je nachdem, wie die Antwort auf diese Frage ausfällt, lassen sich unterschiedliche technische und rechtliche Bausteine und ein geeignetes Geschäftsmodell inklusive Trägerschaft und Finanzierungsansatz wählen. Sinnvoll wäre es außerdem, auf einheitliche technische Komponenten zu setzen, um eine spätere Skalierung des Datentreuhänders zu ermöglichen. Um Vertrauen im Ökosystem aufzubauen, sollten Datentreuhandbetreiber außerdem eine geeignete Rechtsform wählen (die sich je nach Anwendungsfeld unterscheiden mag) und strategische Partnerschaften mit relevanten Akteuren aufbauen. Um das Datenökosystem in Gang zu bringen, sind neben den Datentreuhändern selbst aber auch Datengebende und -nutzende aufgefordert, entsprechende Dienste zu nutzen und sich an entsprechenden Referenzprojekten zu beteiligen.

Der Gesetzgeber hat Hebel, um die Rechtssicherheit fürs Datenteilen wie auch für den Betrieb von Datentreuhändern zu erhöhen. Insbesondere auf europäischer Ebene sollte erörtert werden, den DGA dahingehend umzugestalten, dass Datentreuhänder alle Funktionen übernehmen können, die nötig sind, um zur Auflösung des Wert-Risiko-Dilemmas im jeweiligen Ökosystem beizutragen. Daneben sollte die **Politik** Standardisierung und Zertifizierung von Datentreuhändern und Komponenten intensiver anstoßen bzw. unterstützen. Die öffentliche Hand kann auch eine Vorreiterrolle einnehmen, etwa, in dem sie selbst Daten der Verwaltung mittels Datentreuhändern teilt oder indem sie Anwendungsfälle für Datentreuhänder in einem Repository systematisiert sammelt. Das BMFTR hat die Erprobung und Skalierung von Datentreuhändern bereits mittels vierer Förderrichtlinien unterstützt. Weitere Anschubfinanzierung von Datentreuhändern durch öffentliche Einrichtungen kann gerechtfertigt sein, sollte aber daran geknüpft sein, dass hierbei auf Standardkomponenten zurückgegriffen wird und die organisierte Zivilgesellschaft sowie Interessengruppen im jeweiligen Datenökosystem noch stärker einbezogen werden.

Die **Wissenschaft** generiert einen beträchtlichen Teil der Daten, die für die Lösung gesamtgesellschaftlicher Probleme von Relevanz sind. Sie findet sich daher oft in der Rolle der Datengebendeno wn wieder, aber auch in der Rolle der Datennutzenden, wenn sie Forschung auf Grundlage von Daten Dritter betreibt. Akteure der Wissenschaft sind daher aufgerufen, sich unter anderem an der Standardisierung von Datenformaten zu beteiligen und interdisziplinär den Beitrag von Datentreuhändern zur Überwindung des Wert-Risiko-Dilemmas weiter zu beforschen. Auch sollte die Wissenschaft durch die Nutzung von Datentreuhändern zu deren Etablierung beitragen.

Neben der Wissenschaft spielt die **Wirtschaft** eine zentrale Rolle beim Aufbau einer florierenden Datenökonomie. Unternehmen sind wichtige Akteure als Kunden von Datentreuhändern. Unternehmen und Verbände sollten sich aus Sicht der Begleitforschung daher stärker an der Entwicklung von entsprechenden Standards beteiligen, als Referenzkunden für Datentreuhänder engagieren und bereit sein, interne Daten über sichere Datenverarbeitungsumgebungen mit Dritten zu teilen.

Die Befunde der Begleitforschung zeigen auf, dass einem breiten Einsatz von Datentreuhändern in der Praxis derzeit noch **rechtliche, technische und organisatorische Herausforderungen** entgegenstehen. Die Begleitforschung zeigt hier **Lösungsansätze** auf, die empirisch über die Pilotprojekte identifiziert und konzeptionell-analytisch weiterentwickelt wurden. Gleichzeitig besteht aber aus Sicht der Begleitforschung auch **weiterer Forschungsbedarf**, insbesondere hinsichtlich vertrauensbildender Maßnahmen für Datentreuhänder und das Datenteilen, technischer Aspekte zur Erhöhung von Datenintegrität und -nutzbarkeit sowie der Interoperabilität, der Wechselwirkungen zwischen Rechtsformen und Geschäftsmodellen sowie der Wahl eines geeigneten Betreibers und der Bepreisung von geteilten Daten. Die identifizierten Herausforderungen beim Aufbau funktionierender

Datentreuhänder sind aus Sicht der Begleitforschung zu meistern, und die Lösungsansätze können erfolgreich zum Einsatz gebracht werden, wenn Betreiber, Politik, Wissenschaft und Wirtschaft hier eng zusammenarbeiten. Unter dieser Voraussetzung können Datentreuhänder einen wertvollen **Beitrag zum Aufbau von Datenökosystemen** leisten, mit entsprechenden positiven Wirkungen auf Innovation und Wertschöpfung in Deutschland und in Europa.

Executive Summary (English)

The present study presents the **final results of three years of accompanying research** on a funding line supporting projects for the development and practical testing of data trust models in the fields of research and business put out by the German Federal Ministry of Research, Technology and Space (BMFTR). In this context, data trustees refer to intermediary structures that ensure the technical-organisational exchange of data between data providers and data users.

As part of the accompanying study, an **inventory** of the funded pilot projects and other use cases as well as the scientific literature on the possible role of data trustees in the development of data ecosystems was carried out first. The accompanying study then identified and systematised **key challenges** and **initial solutions** for the establishment and operation of data trustees. The analysis of the empirically collected data and the conceptual work of the accompanying study focused on four **cross-cutting topics: 1. technical infrastructure, 2. legal framework conditions, 3. business and operating model development and 4. acceptance, standardisation, certification and scaling**. Overall, the technical, legal and economic aspects of setting up data trustees were analysed in their interaction. The findings of the accompanying study and the recommendations for action derived from them are aimed at existing and future operators of data trustees but also at political decision-makers and stakeholders from science, business and civil society who are involved in the development of a functioning data economy. The study is also aimed at an interested audience at the intersection of research, innovation and digitalisation.

The **fundamental hypothesis of the accompanying study** was that, from the perspective of society as a whole and innovation policy in particular, data is shared within and between sectors (science, business) only to a limited extent due to an unfavourable **value/risk ratio**. This is of concern given that increased data sharing would be desirable from the perspective of society as a whole and from the perspective of innovation policy. Accordingly, potential data providers are reluctant to share their data, as they fear a loss of control over its further use. In addition, perceived and actual compliance risks discourage data providers and users alike from the sharing of data. At the same time, the potential value that can result from data sharing for both data providers and data users is difficult to measure. This is summarised by the accompanying research under the term **value/risk dilemma**.

As neutral bodies, **data trustees** can facilitate a fair balance of interests between data providers and data users, initiate new relationships of trust where necessary and guarantee technical and organisational access to high-quality data while ensuring data protection and interoperability. This **assumption** can be validated both by the conceptual considerations and the empirical findings outlined in this study. From a theoretical point of view, data trustees can **positively influence the value of data sharing by reducing the associated risk of loss of control over the shared data for data providers and compliance risks for data providers and users.** As a precondition for this, they have to create trust, reduce legal uncertainties and create added value for data providers and users. To this end, data trustees must both pave the way for new **relationships between data providers and data users** and further develop existing ones in such a way that they enable value-based data sharing aimed at a fair balance of interests.

The empirical analyses of the accompanying study lead to some **key findings**. The pilot projects funded by the BMFTR identified technical and legal requirements to be met when setting up data trustees and were able to test out different solutions. At the same time, the questions raised by the pilot projects, as well as additional findings of the accompanying research, confirm that there is a range of technical, regulatory and economic challenges that currently prevent broad deployment of data trusteed. The accompanying research could be empirically identified and conceptually further developed potential solutions to some of these problems, as outlined below.

Firstly, it should be noted that data sharing is only then sufficiently interesting for data providers and users if specific and valuable use cases for the data shared in this way are clearly recognisable. From the perspective of the accompanying study, it is thus essential that data trustees are very familiar with the relevant databases, sector(s), technologies, markets, business models and even the cultures of the stakeholder organisations. They also need a certain standing with the relevant stakeholders in order to be **accepted**. This in turn has implications for the business strategy to be chosen and the possible scaling of the data trust model selected.

Looking at regulatory framework conditions, data trustee operators must first clarify who determines access to and use of the data to be shared and what compliance risks this entails for data providers and users. To this end, the accompanying study developed a typology of data trust models that categorises case groups according to the intensity of the compliance risks and the required scope of control mechanisms. In cases where, in addition to open data, raw data or even analytical results based on the data are to be shared between data providers and users, a data trustee has needs to perform specific functions according to the model. For instance, as soon as raw data or analysis results are shared, it is usually the task of the data trustee to create a secure data processing environment.

A key finding of the accompanying research is that, in practice, the current German and European **legal framework** (in particular the Data Governance Act / DGA) creates only limited legal certainty for data providers and users as well as data trustees. This is proving to be an obstacle to the establishment of data trustees and data ecosystems. The case groups conceptualised by the accompanying study on an empirical basis can help to identify the most suitable data trustee model depending on the intensity of the respective risks and possible conflicts of interest between data providers and data users.

Technical building blocks for their implementation can be derived from the legal requirements for data trust models. These building blocks form the fundamental framework for enabling the trustworthy exchange and use of data. Even if the specific design can vary depending on the field of application, data trustees must fulfil requirements in terms of interoperability, data security and data minimisation. Interoperability refers to interfaces and data models for smooth data transfer. In terms of data security, suitable measures must be taken for authentication, authorisation, recording or logging, data encryption and certification. Data minimisation refers to the fact that only the information that is essential for the respective use case is disclosed. The accompanying study presents a modular system that contains suitable building blocks to fulfil these central requirements, depending on the use case.

Apart from the legal and technical design of a data trust model, technical, legal and organisational **standards** play a role in the successful establishment of data trustees. This shows that trust is not created solely through the selection of suitable technical building blocks, but only in connection with transparent processes, certifications, credible operators and participatory governance structures. Overall, the development of standards for both data and data trustees is still in its infancy. The accompanying study was able to identify various approaches in the pilot projects analysed, particularly in the fields of medical and health research and forestry. Standards can in turn be used as a basis for **certifications** that recognise the governance, financing, data access rules, data security, ethics and sustainability as well as quality of the data shared via a data trustee. Corresponding measures are considered desirable by the pilot projects but have not yet been implemented in practice. The current insufficient availability of generally accepted standards represents a hurdle not only for the further development of individual data trustees, but also for greater interoperability between different data trustees. As comparatively important developers of standardised components, **Gaia-X** and the **International Data Spaces Association**, but also other data space initiatives and technologies such as **SOLID** (Social Linked Data), have the potential to support the development of greater interoperability in the medium term, as do other data space initiatives.

The development of viable **business models** for the long-term operation of data trustees is also proving challenging in practice. There are uncertainties regarding the pricing of data,

sustainable long-term financing of data trustees and the choice of a suitable operator for them. In principle, very few operators of a data trustee are motivated purely by monetary considerations - rather, they hope to enable new, data-based use cases that will in turn benefit them and other players in the data ecosystem. Nevertheless, the costs of operation must at least be covered. This can be organised using both for profit and not-for-profit models. Depending on the application domain, the pilot projects sometimes favour public sponsorship, for example in the domain of medical research, whereas private-sector sponsors are also conceivable in the energy or housing industry, for example. In terms of pricing, the pilot projects tend to favour subscription models over transaction-based pay-per-use approaches.

A Europe-wide and cross-domain **scaling** of data trustee models is currently hardly foreseeable. At the same time, such an approach is considered desirable by stakeholders involved in data trustees. Scaling is understood more as a merger of federated but independent data trustees than as the expansion of individual data trustees into new geographical or sectoral markets. The technical interoperability of data trustees – for example through the standardisation of technical components – is therefore a key prerequisite for enabling scaling.

Overall, the findings confirm the initial hypothesis of the accompanying study, according to which data trustees are a possible instrument for positively influencing the value/risk dilemma in data sharing. In all likelihood, no single data trustee model favoured across all domains and sectors will prevail. Instead, it can be assumed that a modular toolbox of legal, technical and organisational components will become established. The accompanying study contributes to this by systematically categorising case groups of data sharing and functionalities of data trusteed to be selected according to these case groups.

Recommendations for action for data trustee operators, policymakers, science and business can be derived from the findings. These recommendations are based on the accompanying study's insight that the right choice of solutions by data trustee operators does not determine their success alone, but that legal, technical and economic framework conditions need to be considered just as much. The common goal of all interested parties should therefore be to overcome the initially presented value/risk dilemma.

Above all, **data trustee operators** should clearly define the added value and functions they offer for data providers and users. Depending on the answer to this question, different technical and legal components and a suitable business model, including sponsorship and financing approach, can be selected. It is also important to rely on standardised technical components to enable scaling later on. To build trust in their data trustee in the ecosystem, data trustee operators should also choose a suitable legal form (which may differ depending on the field of application) and establish strategic partnerships with relevant stakeholders. In order to get the data ecosystem up and running, data providers and users are also called upon to utilise corresponding services and participate in corresponding reference projects in addition to the data trustees themselves.

Lawmakers can increase legal certainty for data sharing as well as for the operation of data trustees. At the European level in particular, lawmakers should consider reworking the DGA in such a way that data trustees can assume all the functions necessary to help resolve the value/risk dilemma in the respective ecosystem. In addition, **policymakers** should initiate and support the standardisation and certification of data trustees and components even more. The public sector can also take on a pioneering role and share administrative data itself via data trustees. It can also systematically collect use cases for data trustees in a repository. The BMFTR has already supported the testing and scaling of data trustees in four funding guidelines to date. Further seed funding for data trustees may be justified but should be linked to the increased use of standard components and involvement of various stakeholder groups in the respective ecosystem.

Science generates a considerable proportion of the data that is relevant for solving problems affecting society as a whole. It therefore often finds itself in the role of a data provider, but also

in the role of a data user when it conducts research based on third-party data. The science community is therefore called upon to participate in standardisation efforts – e.g., in the area of data formats – and to conduct further interdisciplinary research into the contribution of data trustees to overcoming the value-risk dilemma. The science community should also contribute to the establishment of data trustees by making active use of them.

In addition to science, the **economy** plays a central role in the development of a flourishing data economy. Companies are key players as customers of data trustees. In the view of the accompanying study, companies and associations should therefore participate in the development of standards, act as reference customers for data trustees and be prepared to share internal data with third parties via secure data processing environments.

The accompanying study shows that there are currently still practical **legal, technical and organisational challenges to** the widespread use of data trustees. The accompanying study identifies **possible solutions** here. At the same time, however, there is also **a need for further research** from the perspective of the accompanying study, particularly with regard to confidence-building measures for data trustees and data sharing, technical aspects for increasing data integrity and usability as well as interoperability, the interactions between legal forms and business models as well as the choice of a suitable operator and the pricing of shared data. In the view of the authors of the accompanying study, the identified challenges can be overcome, and the solutions can be successfully implemented if politics, science and business work closely together. Under these conditions, data trustees can fully realise their potential and make a valuable **contribution to the development of data ecosystems**, with corresponding positive effects on innovation and value creation in Germany and Europe.

1 Kontext und Einordnung

Die Industrienationen durchlaufen seit einigen Jahren einen Wandlungsprozess. Wurden in der Vergangenheit Wertschöpfungen primär mit hardware-basierten Produkten geschaffen, so zeichnet sich die jüngere Zeit durch einen Wechsel hin zu datenbasierten Geschäftsmodellen aus. Innovationen zielen entsprechend immer mehr auf die Generierung und Nutzung von Daten ab. **Daten** gelten somit als **wesentlicher Treiber für Wertschöpfung**. Sie bilden die Grundlage für Forschung, Innovation und die Lösung gesellschaftlicher Herausforderungen. Zwar werden immer mehr Daten generiert, oft jedoch sind sie für potenzielle Nutzende nicht zugänglich. Im Gegenteil existieren heute **große Datenbestände** in den „**Silos**" verschiedenster Organisationen – Firmen, Forschungseinrichtungen, Behörden oder auch auf den Endgeräten von Privatpersonen –, ohne dass mögliche Datennutzende **außerhalb** (und manchmal sogar innerhalb) dieser Organisationen leicht auf sie **Zugriff** bekommen könnten. Sehr oft ist es für Außenstehende sogar äußerst schwierig herauszufinden, welche Datenbestände überhaupt wo existieren. Erhebliche wirtschaftliche, wissenschaftliche und gesellschaftliche **Potenziale von Datennutzung bleiben somit unausgeschöpft**. Diesen ‚Datenschatz' gilt es zu heben.

Einem stärkeren Teilen von Daten zwischen Akteuren (sowohl Privatpersonen als auch Organisationen) stehen derzeit noch erhebliche technische, rechtliche, wirtschaftliche und persönliche Hürden und Risiken entgegen. **Datentreuhänder** bieten eine Möglichkeit, diese Hürden zu überwinden und stärkeres Datenteilen zu forcieren (für eine Definition von Datentreuhändern, s. Glossar). Als **neutrale**, auf den Interessensausgleich zwischen beteiligten Akteuren bedachte **Intermediäre** im Datenökosystem stellen sie die technischen und rechtlich-organisatorischen Strukturen bereit, über die Daten unter Wahrung der Rechte der Beteiligten geteilt werden können.

Wie Datentreuhänder am besten aufgebaut und betrieben werden können, ist dabei noch offen. Europaweit befinden sich verschiedene Ansätze und Modelle im Aufbau. Um die Entwicklung von Datentreuhändern auch in Deutschland voranzutreiben, hat das **Bundesministerium für Bildung und Forschung (BMBF**; fortan **BMFTR**) von 2021 bis 2025 zwanzig **Projekte zur Entwicklung und praktischen Erprobung von Datentreuhandmodellen** in Forschung und Wirtschaft gefördert. Die BMFTR-Pilotprojekte konzipierten, entwickelten und erprobten Datentreuhandmodelle, also spezifische Ausgestaltungen eines Datentreuhänders, unter realen Praxisbedingungen in verschiedenen Domänen von Gesundheit über Forstwirtschaft bis hin zu Windenergie. An den Projekten waren verschiedene Akteure aus Wissenschaft und Wirtschaft beteiligt – insgesamt gab es zwei Einzelprojekte und 18 Verbundprojekte. Die Projekte wurden im Regelfall mit bis zu 800.000 Euro gefördert (BMBF 2021).[1]

Begleitet wurde die Umsetzung der geförderten Pilotprojekte durch eine Begleitforschung. Diese wurde von einem Konsortium aus Technopolis Deutschland GmbH, Fraunhofer ISI, der Universität der Künste Berlin und der RWTH Aachen von 2022 bis 2025 umgesetzt. Der besondere **Fokus** hierbei lag auf der systematischen Untersuchung zentraler Herausforderungen und möglicher, über einzelne BMFTR-Pilotprojekte hinaus praktikabler Lösungsansätze in den vier **Querschnittsthemen Akzeptanz, rechtliche Rahmenbedingungen, Geschäftsmodellentwicklung, technische Infrastruktur sowie Standardisierung und Zertifizierung**. Die vorliegende Studie stellt den Abschlussbericht dieser Begleitforschung dar. Eine Evaluierung der einzelnen Pilotprojekte oder der Förderrichtlinie gehörte hingegen nicht zum Aufgabenbereich der Begleitforschung.

Die Begleitforschung schloss drei Datenerhebungs- und auswertungsrunden ein:

[1] Eine Übersicht der Pilotprojekte findet sich in Anhang C sowie unter https://www.bildung-forschung.digital/digitale-zukunft/de/wissenschaft_und_forschung/datentreuhandmodelle/datentreuhandmodelle_pilotvorhaben/datentreuhandmodelle_pilotvorhaben_node.html (zuletzt abgerufen am 25. August 2025).

- In der ersten Runde lag der Fokus auf einer **Bestandsaufnahme** zum Thema, die primär auf einer schlagwortbasierten Suche und **Auswertung wissenschaftlicher Literatur** zu den vier eingangs genannten Querschnittsthemen (siehe Bibliografie in Anhang A) sowie einer Untersuchung von **Anwendungsbeispielen von datentreuhandähnlichen Modellen aus dem In- und Ausland** (siehe Anhang D) basierte. Hierauf aufbauend wurden eigene **konzeptionelle Überlegungen** der Begleitforschung zur Definition und Funktionalität von Datentreuhändern ausgearbeitet. Zu den Ergebnissen dieses ersten Arbeitsschritts veröffentlichte die Begleitforschung einen ersten Zwischenbericht (Technopolis Group et al., 2024a).
- In der zweiten Runde untersuchte die Begleitforschung **Umsetzungshemmnisse** bei der Etablierung von Datentreuhändern. Hierfür wurden **empirische Erhebungen unter den Pilotprojekten** (Online-Befragung sowie leitfadengestützte Interviews) sowie unter **externen Expertinnen und Experten** (leitfadengestützte Interviews) durchgeführt. Die Erhebungen orientierten sich dabei an den vier Querschnittsthemen und deckten sowohl spezifische Aspekte einzelner Pilotprojekte als auch allgemeine Herausforderungen beim Aufbau von Datentreuhändern ab. Außerdem wurden Zwischenberichte der Pilotprojekte ausgewertet. Auf den Ergebnissen aufbauend folgten sodann wieder konzeptionelle und analytische Arbeiten der Begleitforschung, insbesondere zur Klassifizierung unterschiedlicher Fallgruppen von Datentreuhandmodellen sowie möglicher technischer und rechtlicher Bausteine für Letztere. Zu den Zwischenergebnissen aus diesem Arbeitsschritt veröffentlichte die Begleitforschung einen zweiten Zwischenbericht (Technopolis Group et al., 2024b).
- In der dritten Runde befasste sich die Begleitforschung schwerpunktmäßig mit **Lösungsansätzen und** erarbeitete **Handlungsempfehlungen** für die erfolgreiche Etablierung von Datentreuhändern. Auch hierfür wurden Vertreterinnen und Vertreter der Pilotprojekte sowie externe Expertinnen und Experten befragt. Außerdem wurde die Literaturauswertung um neu hinzugekommene Publikationen erweitert. Die Ergebnisse dieses dritten Arbeitsschritts flossen in die vorliegende Studie ein.

Die Zwischenergebnisse wurden in jeder der drei Runden im Rahmen von Vernetzungsveranstaltungen vor Ort sowie virtuell in **Fachgruppenworkshops** mit Vertreterinnen und Vertretern der Pilotprojekte diskutiert und anschließend weiter ausgearbeitet. Die Vielzahl an Datenerhebungen im Rahmen der Begleitforschung ermöglichte eine umfassende Einbindung aller Pilotprojekte. Die empirischen Befunde aus den Pilotprojekten halfen der Begleitforschung dabei, ihre eigenen konzeptionellen Überlegungen entlang der vier Querschnittsthemen zu validieren und nachzuschärfen, und lieferten ein Stimmungsbild bezüglich der Machbarkeit verschiedener Bausteine und Funktionalitäten von Datentreuhändern. Die so gewonnenen Erkenntnisse fließen insbesondere direkt in Kapitel 3 der Studie ein.

Fachlich wurde die Begleitforschung durch einen **Projektbeirat** unterstützt, der sich aus Expertinnen und Experten aus Wissenschaft und Praxis zusammensetzte (siehe Anhang E).

Die **Studie** ist folgendermaßen **gegliedert**:

- **Kapitel 1** ordnet die Studie in den Kontext der Begleitforschung ein und beschreibt ihr methodisches Vorgehen.
- **Kapitel 2** stellt die zentralen Erkenntnisse vor. Hierfür wird zunächst die Ausgangslage beschrieben und die zentrale Arbeitshypothese der Begleitforschung hergeleitet. Anschließend werden die Herausforderungen bei der Etablierung von Datentreuhandmodellen entlang der verschiedenen Querschnittsthemen vorgestellt. Zu jedem Thema finden sich Schlussfolgerungen und eine Beurteilung zum Handlungsbedarf in Boxen zum Schluss des jeweiligen Unterkapitels.
- **Kapitel 3** präsentiert die aus den Schlussfolgerungen abgeleiteten Handlungsempfehlungen an Betreiber von Datentreuhandmodellen sowie an Politik, Wissenschaft und Wirtschaft.

- **Kapitel 4** skizziert, in welchen Bereichen nach Auffassung der Begleitforschung weiterer Forschungsbedarf besteht.

Die Befunde der Begleitforschung sowie der daraus abgeleiteten Handlungsempfehlungen richten sich an Betreiber von Datentreuhändern und an diejenigen, die es werden wollen. Außerdem sind die Ergebnisse für politische Entscheidungsträger und Akteure aus Wissenschaft und Wirtschaft sowie Zivilgesellschaft interessant, die am Aufbau einer funktionsfähigen Datenökonomie beteiligt sind. Daneben richtet sich die Studie an das interessierte Fachpublikum in den Bereichen Forschung, Innovation sowie Digitalwirtschaft.

2 Zentrale Erkenntnisse der Begleitforschung

2.1 Ausgangslage: Rolle von Datentreuhändern als Förderer von Akzeptanz für das Datenteilen

Das Wichtigste zur Ausgangslage in Kürze:

- Trotz nachgewiesener Vorteile ist die **Bereitschaft zum Datenteilen aktuell gering**. Zwar zeigt sich in der Wissenschaft eine größere Offenheit als in der Wirtschaft, dennoch bleibt das Teilen von Daten deutlich hinter den bestehenden Potenzialen zurück.
- Ein wesentlicher Grund dafür liegt im sogenannten **Wert-Risiko-Dilemma**: Für viele Akteure ist der konkrete Mehrwert des Datenteilens unklar, während gleichzeitig mit erheblichen Risiken und Kosten gerechnet wird. Diese Unsicherheit hemmt die Bereitschaft, Daten verfügbar zu machen oder zu nutzen.
- **Datentreuhänder** *könnten* hier eine Schlüsselrolle einnehmen, indem sie als Katalysator für verantwortungsvolles, wertbasiertes, auf fairen Interessenausgleich abzielendes Datenteilen wirken und auf diese Weise **zum Aufbau leistungsfähiger und vertrauenswürdiger Datenökosysteme beitragen.**
- Bisher haben sich entsprechende Modelle allerdings kaum über den Pilotstatus hinaus etabliert. **Zentrale Herausforderungen** bestehen unter anderem darin, sowohl Datengebende als auch Datennutzende für eine Teilnahme zu gewinnen, rechtliche Unsicherheiten zu klären, technische Grundlagen und gemeinsame Standards zu schaffen, tragfähige Betriebs- und Geschäftsmodelle zu entwickeln und letztlich die Skalierung der Datentreuhandansätze sicherzustellen. Eine vertiefte Auseinandersetzung mit diesen Herausforderungen folgt in den nächsten Unterkapiteln.

Das Teilen von Daten ist wertvoll für Forschung, Innovation und Wertschöpfung und hilft bei der Lösung gesellschaftlicher Herausforderungen wie der Entwicklung nachhaltiger Mobilitätskonzepte, der Erforschung komplexer Klimamodelle oder der Bekämpfung seltener Krankheiten. Zwischen Organisationen und/oder Individuen geteilte Daten gelten daher als bedeutende Ressource des 21. Jahrhunderts. Das aus Sicht der Datengebenden selbstbestimmte Teilen bildet außerdem eine nach europäischen Regeln rechtssichere **Grundlage für** das Training von Algorithmen des maschinellen Lernens und neuronaler **Künstlicher Intelligenz** (KI). Dieser Aspekt gewann im Verlauf der Begleitforschung vor allem durch das Aufkommen der großen KI-Basismodelle wie GPT-4 besondere Bedeutung, da diese aktuell mit Daten trainiert werden, deren Eigentümerinnen und Eigentümer dieser Nutzung nicht oder nicht explizit zugestimmt haben. Sichtbar wird bei den aktuellen Entwicklungen neben den verfügbaren Finanz- und Computer-Ressourcen der Wert von großen, einheitlich zugänglichen Datenbeständen. So sind es typischerweise die großen Tech-Konzerne oder mit diesen verpartnerte Unternehmen, die große Basismodelle entwickeln und anbieten. Nur sie haben die notwendigen Datenbestände. Da in Europa derartige Unternehmen und somit zentral gehostete Datenbestände nicht in vergleichbarem Umfang vorliegen, kommt dem **Aufbau großer, föderierter Datenökosysteme für das sichere Teilen von Daten** unterschiedlichster Herkunft eine zukünftig stark steigende Bedeutung zu. Schafft es Europa nicht, Datenökosysteme vor allem für KI-Zwecke aufzubauen, droht der Technologieabstand zu und die technologische Abhängigkeit von den hier führenden Nationen und Unternehmen weiter zuzunehmen.

In diesem Zusammenhang ist außerdem wichtig zu betonen, dass **Daten durch das Teilen** *innerhalb* eines Sektors (Wirtschaft, Wissenschaft, Verwaltung) **einen zusätzlichen Wert erlangen**, der sich durch eine sektorübergreifende gemeinsame Datenverknüpfung und Datennutzung, also etwa zwischen Wirtschaft und Wissenschaft, noch weiter steigern kann. Auch vor dem Hintergrund der (Wieder-)herstellung von Datensouveränität, Transparenz und damit allgemeiner auch digitaler Souveränität (Kreutzer et al., 2022) ist die Förderung eines

strukturierten Datenteilens im deutschen sowie europäischen Kontext eine dringliche politische Aufgabe.

Anders als bei großen datengetriebenen Plattformen wie Google, Meta oder Amazon sind **Daten in Deutschland und Europa oftmals fragmentiert vorhanden**, sowohl innerhalb der Wirtschaft (insbesondere im Fall mittelständischer Unternehmen) als auch in der Wissenschaft, und nicht zuletzt in der Verwaltung. Sie verbleiben somit oftmals in ihren Silos. Daher stellt sich die Frage, welche Faktoren Datenteilen eher begünstigen oder erschweren.

Laut Umfragen sind Menschen grundsätzlich bereit, auch aus ihrer Sicht sensible Daten (z. B. Gesundheitsdaten) für „gute Zwecke" wie Forschung oder Dekarbonisierung **zu teilen** (Köngeter et al., 2022; Mohr & Cloos, 2022; Meijer & Potjer, 2018; ODI, 2019, Acharya & Mekker, 2022). Die wichtigsten Hemmnisse, die Privatpersonen vom Datenteilen abhalten, sind dabei Datenschutzbedenken und Sorgen vor Missbräuchen sowie Aufwand (Blankertz, 2020; Köngeter et al., 2022; Acharya & Mekker, 2022; Meijer & Potjer, 2018; Choi et al., 2022). Je größer der nötige zeitliche, kognitive oder materielle Aufwand und je komplexer der Prozess, desto weniger teilen Menschen ihre Daten. Auch bei Forschungseinrichtungen besteht grundsätzlich die Bereitschaft, Daten zu teilen, wobei Datenschutzbedenken oftmals eine praktische Hürde darstellen.

Bei Unternehmen hingegen ist die Bereitschaft, Daten zu teilen, deutlich geringer ausgeprägt (Fraunhofer ISST, 2022; Röhl et al., 2021; RfII, 2021). Firmen sehen vom Datenteilen ab, weil sie sich bislang meist wenig direkten Nutzen davon versprechen (bzw. weil Geschäftsmodelle fehlen, die Datenteilen belohnen würden) und sie zudem Risiken sehen. Zu diesen zählen Datensicherheit, Abfluss von Geschäftsgeheimnissen, Compliance-Verletzungen aufgrund unklarer Rechtslagen sowie die Gefahr von Reputationsschäden (RfII, 2020; CfDEI, 2021; Brown et al., 2022; FPF, 2017; Blankertz, 2020; Blankertz & Specht-Riemenschneider, 2021). Weitere Hürden sind Aufwand, fehlende Ressourcen und technische Infrastruktur sowie fehlende Data Literacy/Data Skills (RfII, 2020; ODI, 2019; CfDEI, 2021).

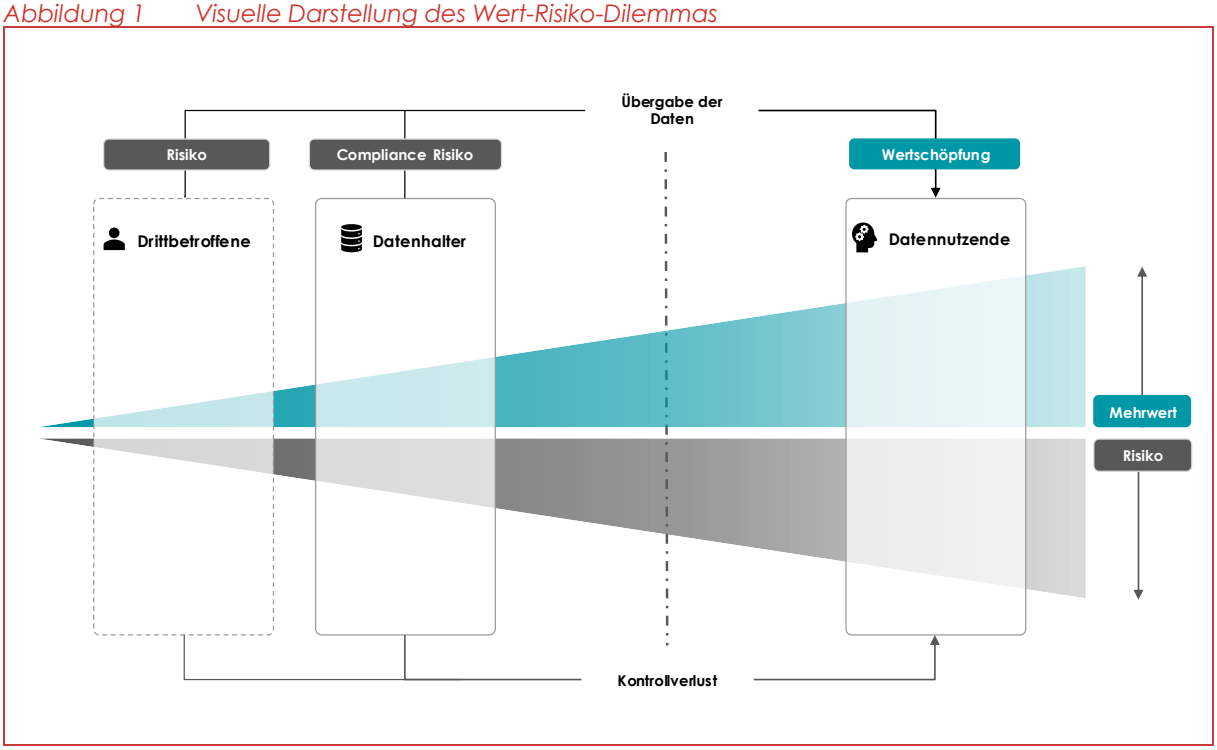
Umgekehrt teilen Unternehmen Daten primär dann, wenn sie darin klare Vorteile erkennen und glauben, Risiken und Aufwand kontrollieren zu können. Vorteile können geldlich sein (Datenverkauf oder Datenzugang gegen Gebühr), reziproker Datenzugang, oder Auslagerung von Forschung und Entwicklung, etwa an die Wissenschaft (FPF, 2017; CfDEI, 2021; ADRF, 2018; ODI, 2019). In der Praxis findet Datenteilen bisher meist nur nach sehr umfangreichem und aufwendigem, oft persönlichem Vertrauensaufbau und Aushandlungsprozessen statt (FPF, 2017; ADRF, 2018).

Auch für die **Datennutzenden** können geteilte Daten Risiken bergen. Da die Daten per Definition von Dritten erstellt wurden, können unklare Datenqualität, Verzerrungen, inkorrekte Metadaten und kleine, aber potenziell folgenschwere Fehler wie falsche Einträge oder inkonsistente Einheiten schwieriger zu erkennen sein (Gal & Rubinfeld, 2019). Zudem stellt sich immer die Frage, ob das spätere (betriebswirtschaftliche) Ergebnis in einem positiven Verhältnis zum Aufwand für die Datenakquisition stehen wird. Kritisch sind daher Vertrauen in die Qualität und die Aufbereitung der Daten einschließlich Metadaten und Datenherkunft sowie die Bedienbarkeit der technischen Infrastruktur und Interfaces.

Die Arbeitshypothese der Begleitforschung ist daher, dass Daten aus gesamtgesellschaftlicher und insbesondere innovationspolitischer Sicht aufgrund eines unklaren Kosten-Nutzen-Verhältnisses nur unzureichend innerhalb und zwischen Anwendungssektoren (Wissenschaft, Wirtschaft) geteilt werden. Konkret besteht ein Dilemma kollektiven Handelns darin, dass der *Wert* zu teilender Daten für die Datennutzenden oftmals vor dem eigentlichen Teilen nur schwer zu bemessen ist, sodass potenzielle Datennutzende zögerlich sind, die Aufwände der Datengebenden für das Teilen ihrer Daten zu kompensieren. Gleichzeitig entstehen sowohl für Datengebende als auch Datennutzende Risiken und Kosten im Zusammenhang mit dem Datenteilen. Datengebende verlieren mit der Übergabe der Daten an die Datennutzenden üblicherweise die Kontrolle über die damit verbundenen Risiken (Compliance,

Betriebsgeheimnisse etc.). Selbst wenn es den Datengebenden und -nutzenden gelingt, Wertschöpfung und Risiken gerecht zu verteilen, sind die dafür aufgewendeten Kosten teilweise prohibitiv groß, sodass ihnen das Teilen der Daten nicht lohnenswert erscheint. Je mehr Akteure am Datenteilen beteiligt sind und je mehr Daten (auch unterschiedlicher Art) dabei geteilt werden, desto höher kann dabei zwar der potenzielle Nutzen ausfallen, jedoch steigen auch die konkreten Kosten aufgrund höherer Komplexität. Dies alles führt dazu, dass Daten oftmals in ihren Silos bleiben. Abbildung 1 veranschaulicht dieses **Wert-Risiko-Dilemma**: Mit der Übergabe der Daten verlieren die Datengebenden (hier sowohl Drittbetroffene als auch Datenhalter) die Kontrolle über die Daten, wobei die (potenzielle) Wertschöpfung steigt (türkiser Farbbereich), gleichzeitig aber auch die Risiken (Compliance, Betriebsgeheimnisse etc.) zunehmen (grauer Farbbereich), was sich wiederum negativ auf die Kosten-Nutzen-Kalkulation von Datengebenden auswirkt. Der Umstand, dass sowohl Wert als auch Risiko beim Datenteilen diffus sind, ist durch die von links nach rechts zunehmende Transparenz der Farbbereiche symbolisch dargestellt. Hierbei wird auf Seite der Datengebenden zwischen den Datenhaltern (z. B. Pharmaunternehmen) und Drittbetroffenen (z. B. Patientinnen und Patienten) unterschieden.

Abbildung 1 Visuelle Darstellung des Wert-Risiko-Dilemmas

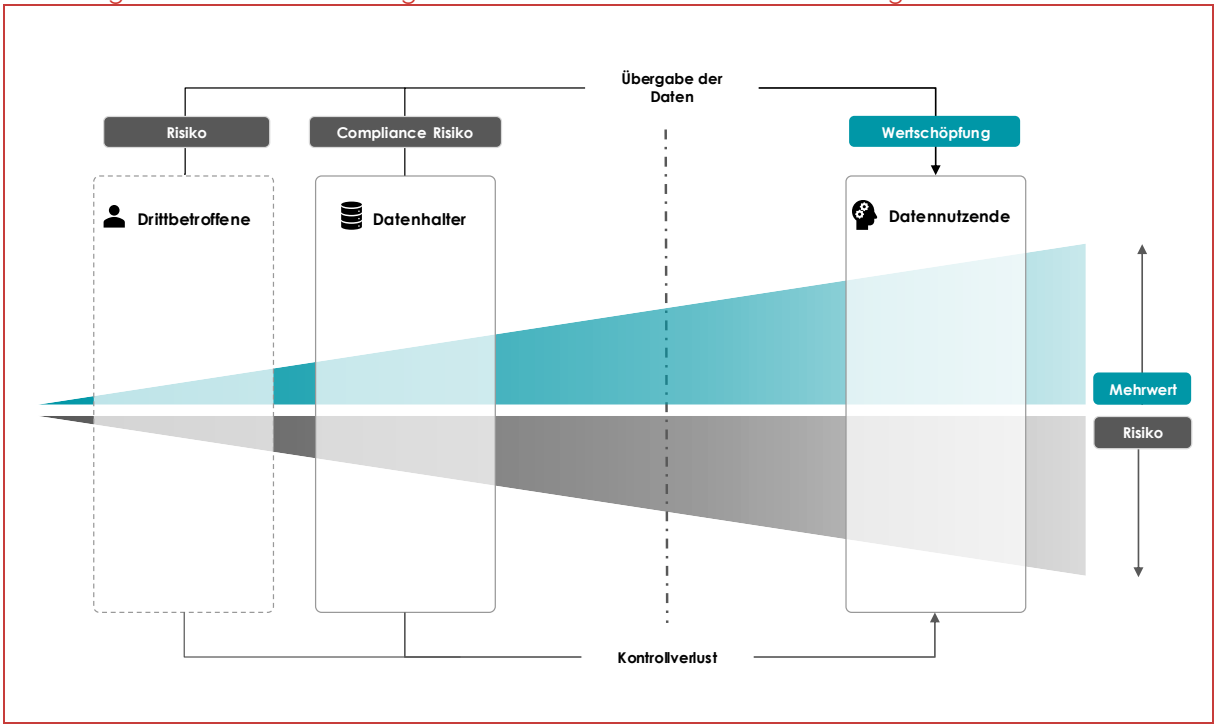


Quelle: Eigene Darstellung (aufbauend auf v. Grafenstein, 2022).

Das Wert-Risiko-Dilemma müsste also dahingehend aufgelöst werden, dass der Wert des Datenteilens die damit verbundenen Kosten und Risiken überwiegt. Hierfür gibt es zwei Hebel: Entweder wird der Wert durch bestimmte Maßnahmen erhöht und/oder konkretisiert oder aber die Kosten sowie Risiken werden gesenkt. Auch eine Kombination beider Ansätze ist möglich. Datentreuhänder sind *ein mögliches* Instrument unter mehreren zur positiven Beeinflussung dieses Wert-Risiko-Verhältnisses (andere Ansätze finden sich bei Data Brokern oder auch Datenräumen, s. Glossar). Um als Lösungsbaustein für leistungsfähige Datenökosysteme fungieren zu können, müssen Datentreuhänder daher Hürden fürs Datenteilen abbauen und Mehrwerte für Datengebende und -nutzende schaffen. Gelingt ihnen dies, haben sie das Potenzial, als **Katalysator für verantwortungsvolle datengetriebene Lösungen für gesamtgesellschaftliche Probleme** zu fungieren. Hierfür müssen die Datentreuhänder

vertrauensvolle Beziehungen zwischen Datengebenden und -nutzenden schaffen, die ein wertbasiertes, auf fairen Interessensausgleich abzielendes Datenteilen ermöglichen. Der mögliche Effekt eines Datentreuhänders auf das Wert-Risiko-Dilemma ist in Abbildung 2 veranschaulicht: Wenn ein Datentreuhänder als zusätzlicher Akteur beim Datenteilen zwischen Datengebende und -nutzende tritt, kann er die Risiken und Kosten für Datengebende so weit verringern und gleichzeitig den Wert der Daten so weit steigern, dass die Wertschöpfung die Risiken und Kosten übersteigt. Dementsprechend ist in dieser Abbildung der türkise Farbbereich („Mehrwert") größer dargestellt als der graue („Risiko"). Idealerweise hilft der Datentreuhänder auch dabei, Wert und Risiken klarer zu bestimmen. Dies ist durch die flächige Darstellung der Farbbereiche veranschaulicht (im Gegensatz zu den transparenter werdenden Farbbereichen in Abbildung 1).

Abbildung 2 Visuelle Darstellung eines Datentreuhänders zur Überwindung des Wert-Risiko-Dilemmas



Quelle: Eigene Darstellung (aufbauend auf v. Grafenstein, 2022).

Um das aufgezeigte Spannungsfeld zwischen Risiko und Wertschöpfung aufzulösen, rückt die Rolle des Datentreuhänders in den Fokus der weiteren Diskussion. Im Folgenden wird deshalb zunächst beleuchtet, welche konkreten Anforderungen mit der Rolle des Datentreuhänders verbunden sind, welche Aufgaben er dabei übernimmt und welche Hürden noch bestehen, das dargestellte Wert-Risiko-Dilemma tatsächlich aufzulösen.

Begriffsverständnis Datentreuhänder

Der Begriff beschreibt die betreibende Stelle von Datentreuhandmodellen. Datentreuhandmodelle wiederum bezeichnen die spezifische technische, rechtliche und organisatorische bzw. geschäftliche Ausgestaltung eines Datentreuhänders.

Die Begleitforschung verwendet folgende Arbeitsdefinition in Anlehnung an die erste Förderrichtlinie des BMFTR zur Erprobung von Datentreuhandmodellen: *Neutraler Intermediär, der einen vertrauensvollen und fairen Ausgleich der Interessen der beteiligten Akteure – Datengebende sowie Datennutzende – ermöglicht, gegebenenfalls neue Vertrauensbeziehungen anbahnt, den technischen und organisatorischen Zugang zu*

qualitativ hochwertigen Daten unter Wahrung des Datenschutzes sowie Interoperabilität garantiert (BMBF, 2021).

Neben dem Begriff Datentreuhänder wird in der Literatur auch von Datenräumen, Datenintermediären und Datenvermittlungsdiensten gesprochen. Es existiert keine allgemein anerkannte Abgrenzung zwischen diesen Begriffen. Gleichwohl stellt der Begriff Datenraum eher auf die technische Infrastruktur als auf die rechtlich-organisatorische und geschäftliche Struktur ab und bezieht sich auf dezentral organisiertes Datenteilen. Datenintermediäre agieren dabei in einem Datenraum bzw. gestalten diesen mit.

Von Datentreuhändern abzugrenzen sind außerdem Datenvermittlungsdienste im Sinne des DGA (einige Datentreuhandmodelle könnten rechtlich unter diesen Begriff fallen, andere nicht, siehe Kapitel 2.3.2).

Der Begriff der Datenintermediäre könnte wiederum eine alternative Übersetzung der englischsprachigen Definition des „data intermediary" im Sinne des DGA darstellen. Soweit diese Studie auf die Definition des DGA referenziert, verwendet sie den offiziellen deutschen Rechtsbegriff des Datenvermittlungsdienstes.

In der Literatur lassen sich folgende **zentrale Anforderungen *an* bzw. Funktionen *von* Datentreuhändern** identifizieren: Zunächst das Herstellen von Transparenz und Vertrauen unter den Datengebenden und -nutzenden, sodass es zu einer fairen, aus Sicht aller Beteiligten lohnenden Verteilung der Wertschöpfung, Risiken und Kosten kommt. Ein Datentreuhänder erreicht dies, indem er die dafür benötigten Mittel auf möglichst kostengünstige Weise zur Verfügung stellt. Die vom Datentreuhänder zur Verfügung gestellten Mittel können sich dabei auf **organisatorische, technische oder die Rechtssicherheit betreffende Aspekte** konzentrieren oder auch alle drei Aspekte integrieren. Damit einher geht die Erwartung an den Datentreuhänder als neutrale, den Datengebenden und -nutzenden zwischengeschaltete Instanz, die vormals nicht in Kontakt zueinanderstehenden Akteure zwecks des Datenteilens zusammenzubringen oder aber bestehende Beziehungen (geschäftlicher oder forschungsbasierter Natur) zwischen Akteuren um eine Komponente des Datenteilens zu erweitern.

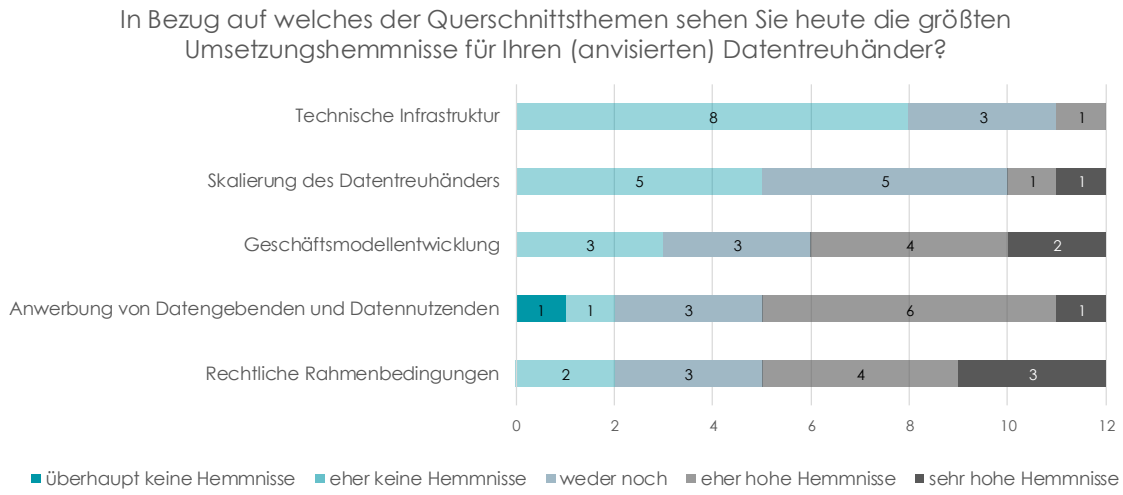
Datentreuhandmodelle lassen sich danach unterscheiden, welche und wie viele **Funktionen** sie für die Datengebenden und -nutzenden bei der Überwindung ihres Wert-Risiko-Dilemmas übernehmen. So kann sich ein Datentreuhänder auf die **technisch-organisatorischen Aspekte** beschränken, z. B. um eine Beziehung zwischen Datengebenden und -nutzenden herzustellen, wobei der eigentliche Datenfluss direkt zwischen diesen beiden Akteuren ohne Zwischenschaltung des Datentreuhänders erfolgt („peer-to-peer"). Der Datentreuhänder kann aber auch die technisch-organisatorische Verfügbarmachung übernehmen, ohne die Daten selbst zu bearbeiten. Dies umfasst etwa die Verwaltung und Durchsetzung von Zugangsrechten, ein durchgängiges Einwilligungsmanagement und die Protokollierung. Daneben kann der Datentreuhänder die Qualität der zu teilenden Daten sicherstellen oder sogar erhöhen, und zwar nicht nur in technischer Hinsicht, sondern auch indem er gewährleistet, dass sie gemäß den rechtlichen Vorgaben auch verarbeitet werden dürfen. Schließlich können Datentreuhänder auch **rechtliche Aspekte** adressieren und die erheblichen Rechtsunsicherheiten für Datengebende und -nutzende beim Datenteilen reduzieren.

Mehrwertdienste, die der Datentreuhänder darüber hinaus anbieten kann, umfassen unter anderem die Pseudonymisierung oder Anonymisierung, Datenbereinigung und die Aufbereitung der Metadaten. Besonders wertvoll, aber auch herausfordernd kann die Übernahme der Datenharmonisierung und deren semantische Beschreibung sein: Da Datenstandards oft fehlen, sind Daten meist entweder nicht oder bestenfalls mit heterogenen Semantiken beschrieben. Diese Beschreibungen zu harmonisieren, ist wiederum Voraussetzung dafür, Daten konsistent auffindbar und nutzbar zu machen. Gleichzeitig ist der Aufwand dafür derzeit in vielen Fällen noch hoch und stellt somit eine zentrale Hürde bei der Nutzung heterogener Daten dar. Hier können Datentreuhänder gezielt unterstützen, wenn sie

einheitliche semantische Beschreibungen sowie entsprechende Mapping-Verfahren anbieten. Auf der Datenharmonisierung aufbauend können Datentreuhänder sodann Daten aus verschiedenen Datenquellen innerhalb eines Datenökosystems verknüpfen, um neue, höherwertige Kombinationen von Daten weiterzugeben und Analysedienste anzubieten. Schließlich kann der Datentreuhänder auch als Orchestrator eines Ökosystems und „Use Case Builder" auftreten, der potenzielle Datengebende und -nutzende aktiv zusammenbringt und mit ihnen konkrete Use Cases erarbeitet.

Wie oben dargelegt, haben Datentreuhänder also *theoretisch* das Potenzial, Datenteilen zu fördern. *Praktisch* kommt die Begleitforschung allerdings zum Ergebnis, dass funktionierende, dauerhaft etablierte Datentreuhänder in Deutschland zumindest bislang kaum aktiv sind. **Der Aufbau entsprechender Modelle gestaltet sich schleppend.** Dies zeigt auch eine aktuelle internationale Analyse der Landschaft von Datentreuhändern in der Praxis (Lipovetskaja et al., 2024). Die Autorinnen und Autoren konstatieren, dass der zunehmenden Bedeutung von Datentreuhändern bislang nur eine geringe Zahl etablierter Geschäftsmodelle gegenübersteht. Auch die bislang begrenzte Überführung der in den Pilotprojekten entwickelten Datentreuhänder in den dauerhaften Betrieb verdeutlicht, dass es sich bei der Geschäftsmodellentwicklung um einen nur langsam voranschreitenden Entwicklungsprozess handelt. Die Begleitforschung hat hierfür mehrere zentrale **Herausforderungen** ausgemacht, die einer erfolgreichen Etablierung von Datentreuhändern im Wege stehen (siehe Abbildung 3 für eine Übersicht entsprechender Ergebnisse aus der Befragung der Pilotprojekte).

Abbildung 3 Wahrnehmung von Umsetzungshemmnissen in den Pilotprojekten



Quelle: Online-Befragung unter den Pilotprojekten der ersten Förderrichtlinie im Herbst 2024 (n = 12).

Die grundlegendste Herausforderung ist es dabei, **Datengebende und –nutzende anzuwerben**, sie also dafür zu gewinnen, Daten zu teilen und geteilte Daten zu verwenden, und dies über einen Datentreuhänder zu tun.

Die nächsten Herausforderungen sind die erheblichen Rechtsunsicherheiten bzw. das erwartete Compliance-Risiko. Hier ist insbesondere unklar, auf welche (systematisierte) Weise ein Datentreuhänder die Datengebenden und -nutzenden bei der technischen und organisatorischen Umsetzung der **rechtlichen Anforderungen sowie Klärung der Compliance-Fragen** optimalerweise unterstützen sollte. In technisch-organisatorischer sowie betriebswirtschaftlicher Hinsicht erschweren ungenügende Datenstandardisierung, fehlende technische Schnittstellen sowie mangelnde Standards für plattformübergreifende

Nutzungskontrolle und Autorisierung den **technischen Aufbau** von Datentreuhändern und steigern den Aufwand / die Kosten) für Datengebende und -nutzende.

Außerdem gibt es kaum überzeugende Ansätze zur langfristigen **Finanzierung von Datentreuhändern**, was wiederum zumindest teilweise in der Schwierigkeit begründet liegt, Daten einen verbindlichen Preis zu geben.

Diese und weitere Herausforderungen sowie Lösungsansätze werden daher in den **folgenden Unterkapiteln** näher diskutiert. Dabei werden zunächst Herausforderungen beim **Anwerben von Datengebenden und -nutzenden** problematisiert. Es folgt die Thematisierung **rechtlicher Rahmenbedingungen**, aus denen sich die **technischen Anforderungen und Bausteine** ableiten lassen. Daraus wiederum entwickelt die Begleitforschung eine **Toolbox**, die bei der Ausgestaltung von Datentreuhandmodellen helfen kann. Ausgangspunkt ist hierbei immer die Frage, welche potenziellen Interessenkonflikte zwischen Datengebenden und -nutzenden in einem bestimmten Anwendungsbereich bestehen (könnten) und welche Bausteine eines Datentreuhänders diese am effizientesten und effektivsten auflösen können. Sodann wird die Rolle von technischen und organisatorischen **Standards** diskutiert. Diese sind nicht zuletzt mit Blick auf eine Senkung der Kosten bei der Implementierung wichtig. Als weitere zentrale Komponente für den erfolgreichen Aufbau von Datentreuhändern werden verschiedene Aspekte bei der Wahl eines **Betriebs- bzw. Geschäftsmodells** erörtert. Zu guter Letzt liefert das Kapitel eine Einschätzung zu **Skalierungspotenzialen** verschiedener Datentreuhandmodelle – sowohl geografisch als auch domänenübergreifend.

2.2 Anwerben von Datengebenden und -nutzenden

Das Wichtigste zu Anreizen für Datengebende und -nutzende in Kürze:

- Um Akteure fürs Datenteilen zu gewinnen, müssen Datentreuhänder ihnen einen **Mehrwert bieten**, der die ihnen entstehenden Kosten und Risiken übersteigt. Der bloße Datenzugang reicht dabei meist nicht aus. Von Interesse sind vielmehr **konkrete und wertvolle Use Cases**, die mit den geteilten Daten realisiert werden können. Eine mögliche Strategie ist, dass der Datentreuhänder selbst als Use-Case-Entwickler oder Koordinator des Datenökosystems auftritt und potenziellen Datengebenden und -nutzenden damit den praktischen Nutzen einer Teilnahme am Datenteilen sichtbar macht.
- Für Firmen und andere Institutionen wird der mit dem Datenteilen verbundene Wert meist **materiell** sein (z. B. gesteigerte Umsätze oder niedrigere Kosten durch Produkte und Prozesse, die mittels der Daten entwickelt oder verbessert werden können; Zahlungen für bereitgestellte Daten etc.). Für Privatpersonen kann der Wert auch ein **immaterieller** (ethischer) sein, etwa über eine altruistische Datenspende.

2.2.1 Materielle Anreize

Wie in den folgenden Kapiteln genauer analysiert, können Recht, Technik sowie Standards und Zertifizierungen dazu beitragen, Kosten und Risiken möglichst gering zu halten. Geringe Risiken und niedrige Kosten bieten jedoch noch keinen Grund, um Datentreuhänder zu nutzen und Daten zu teilen bzw. diese Daten zu nutzen. Dafür braucht es ein positives Wertversprechen. **Ein einfaches Bereitstellen von Daten reicht hierfür oft nicht aus**. Ein wesentlicher Punkt, der sich in den Gesprächen mit externen Expertinnen und Experten und den Pilotprojekten herauskristallisierte, ist, dass für viele Akteure **Datenzugang an sich oft nur von begrenztem oder sogar gar keinem Interesse ist**. Ein Experte betonte im Interview daher, dass Datentreuhänder sich nicht primär als Institutionen zur Förderung des Datenteilens sehen sollten, sondern vielmehr als Treiber für die Entwicklung konkreter datenbasierter Technologien (z. B. KI oder Digitale Zwillinge in einer bestimmten Industrie), also mit einem klaren technologischen Ziel, das über den bloßen Datenzugang hinausgeht.

Von Interesse sind also vor allem die Use Cases, die sich mit den Daten entwickeln lassen. Diese augenscheinlich triviale Spitzfindigkeit hat wichtige Implikationen für die Anwerbung von Datengebenden und -nutzenden und die Anreizsetzung des Datenteilens/-nutzens. **Wertige Use Cases zu identifizieren und praktisch umzusetzen ist oft nicht einfach**, sondern stellt eine Innovationsleistung dar. Diese ist selbst risikobehaftet (der erhoffte Gewinn könnte nicht eintreten), oft (noch) tangential zum bestehenden Kerngeschäft der Akteure und erfordert regelmäßig erheblichen Aufwand. Wenn der Datentreuhänder sich primär auf das einfache Bereitstellen von Daten konzentriert, liegt das geschäftliche Risiko und die Kosten für die Identifizierung und Umsetzung von Use Cases größtenteils bei den Datengebenden und -nutzenden. Außerhalb bestimmter atypischer Branchen – insbesondere Pharmazeutik und Medizin – scheint die Bereitschaft von Datengebenden und -nutzenden, dieses Innovationsrisiko einzugehen, jedoch oft verhalten.[2] Entsprechend schwierig gestaltet es sich, sie für den Datentreuhänder anzuwerben.

Eine Lösung für diese Problematik ist, dass der Datentreuhänder selbst als **Use-Case-Entwickler, Matchmaker und Orchestrator des Datenökosystems** auftritt – als (vertrauenswürdige und neutrale) Instanz, die Akteure, welche ansonsten eher nicht zusammenkämen, als Datengebende und -nutzende zusammenbringt, neue Informationsflüsse zwischen ihnen herstellt und mit ihnen Use Cases identifiziert und aufarbeitet. Dazu muss der Datentreuhänder die relevanten Datenbestände, Branche(n), Technologien, Märkte, Geschäftsmodelle und sogar Kulturen der Akteure sehr gut kennen. Zudem muss er ausreichend Standing in den jeweiligen Fach- und Branchencommunitys haben, um Akteure zusammenbringen zu können. Das hat auch Implikationen für die Skalierungsmöglichkeiten und Geschäftsstrategie eines Datentreuhänders. Da es schwierig sein dürfte, die nötige Expertise und das Standing, um als Ökosystem-Orchestrator auftreten zu können, für viele Branchen und Communitys gleichzeitig aufzubauen, dürften Datentreuhänder sich hier eher gezielt auf bestimmte Branchen oder sogar Sub-Branchen (z. B. Versicherungswesen für bestimmte Industrieanlagen) oder spezifische Technologien spezialisieren (z. B. KI-Entwicklung in der Autoindustrie).

Aus gewinnbringenden Use Cases lässt sich ein Mehrwert erwirtschaften, der zwischen Datengebenden und -nutzenden (sowie gegebenenfalls dem Datentreuhänder) aufgeteilt werden kann. Hierfür sind verschiedene praktische Ausgestaltungen denkbar. Eine **Gewinnbeteiligung** garantiert den Datengebenden einen langfristigen Anteil am erwirtschafteten Wert, erhöht allerdings auch ihr Risiko (der Erfolg könnte ausbleiben). Ex-ante-**Zahlungen für Daten** bieten größere Sicherheit, allerdings auch niedrigere Gewinnaussichten. Sie verschieben das unternehmerische Risiko zu den Datennutzenden, die nun für die Daten aufkommen müssen, und das ohne schon zu wissen, ob der Use Case erfolgreich sein wird. Mischformen dieser beiden Instrumente sind ebenfalls denkbar. Dabei stellt die korrekte Bepreisung von Daten jedoch oft kein triviales Problem dar (siehe weiter Kapitel 2.6.3).

Neben Zahlungen können Datentreuhänder den Datengebenden wie -nutzenden auch **nicht-monetäre instrumentelle Vorteile** bieten, z. B. Analyseergebnisse oder Zugang zu neuen Diensten. Welches dieser verschiedenen Anreizsysteme für einen Datentreuhänder und die avisierten Datengebenden und -nutzenden jeweils das Passende ist, dürfte von Fall zu Fall variieren. In der Praxis scheinen Datentreuhänder heute mit all diesen Anreizsystemen zu experimentieren.

2.2.2 *Nicht-materielle Anreize: Datenaltruismus*

Datenaltruismus ist vor allem dann relevant, wenn **Privatpersonen** als Datengebende auftreten. Am besten scheint Datenaltruismus aktuell im Medizinbereich zu funktionieren (Bereitstellung

[2] Der medizinische Bereich scheint insofern andersartig zu sein, als dass sich die einschlägigen Datentreuhänder in der Regel um die Nutzung von Patientendaten für die medizinische Forschung und Entwicklung drehen – einer von allen Branchenakteuren sehr gut verstandenen Familie von Use Cases, bei denen auch die Standardisierung von Daten relativ weit fortgeschritten ist. Wie wertig ein Datensatz und ein Use Case ist, lässt sich somit erheblich einfacher, schneller und mit weniger Aufwand beurteilen als in vielen anderen Branchen.

von Patientendaten für die Forschung). Der gesellschaftliche Nutzen ist hier besonders leicht verständlich und der moralische Imperativ vielleicht besonders stark. Zudem werden diese Daten meist im Kontext von bereits stattfindender medizinischer Behandlung erhoben (d. h. der zusätzliche Aufwand für die Datenspendenden ist gering) und die Erhebung wird meist von Personen durchgeführt oder begleitet, die allgemein hohes Vertrauen genießen (Ärztinnen und Ärzte, Pflegepersonal). Auch bietet das Gesundheitssystem mit Krankenhäusern, Praxen und Versicherungen einen relativ leicht aktivierbaren Kanal, um Privatpersonen zu kontaktieren und um Datenspenden zu bitten. Außerhalb der Domäne **Gesundheit** sind diese Faktoren bisher selten im gleichen Umfang präsent.

2.2.3 Schlussfolgerungen und Handlungsbedarf

Um Datengebende und -nutzende anzuwerben, müssen Datentreuhänder ihnen einen Wert bieten, der die entstehenden Kosten und Risiken übersteigt. Für Firmen und andere Institutionen wird dieser **Wert** meist **materiell** sein (z. B. gesteigerte Umsätze oder niedrigere Kosten durch Produkte und Prozesse, die mittels der Daten entwickelt oder verbessert werden konnten; Zahlungen für bereitgestellte Daten etc.). Für Privatpersonen kann der Wert auch ein **immaterieller** (moralischer) sein, etwa über eine altruistische Datenspende. Neben einem glaubwürdigen Wertversprechen, das in diesem Unterkapitel weiter ausgeführt wird, ist auch **Vertrauen** bei allen beteiligten Akteuren eine kritische Vorbedingung. Standards und Zertifizierungen sowie die nachvollziehbare Lösung technischer und rechtlicher Risiken sowie die Wahl des Betriebsmodells sind kritische Hebel, um Vertrauen aufzubauen, und werden in den folgenden Kapiteln weiter diskutiert, beginnend mit den rechtlichen Rahmenbedingungen.

2.3 Rechtliche Rahmenbedingungen für den Betrieb von Datentreuhändern

Das Wichtigste zu rechtlichen Rahmenbedingungen in Kürze:

- Im europäischen Recht existiert kein allgemeines **Eigentumsrecht an Daten**. Stattdessen schützt eine Vielzahl an Gesetzen unterschiedliche Interessen in spezifischen Kontexten – etwa durch **Schutzgesetze** (z. B. Datenschutz, Geschäftsgeheimnisse, IT-Sicherheit) oder durch **Teilhaberechte** (z. B. EU Data Act, EHDS, DNG), die Datenzugriffs- und Verwendungsrechte regeln.
- Datentreuhänder bewegen sich in einem komplexen rechtlichen Umfeld, in dem sie sowohl die **Compliance-Risiken** der Datengebenden und -nutzenden minimieren als auch ihre eigenen kontrollieren müssen. Der **DGA** stellt Anforderungen an die Neutralität von Datentreuhändern und hat damit eine wichtige Funktion bei der Bildung des erforderlichen **Vertrauens** für das Teilen von Daten, klärt aber viele Compliance-Fragen nicht ausreichend.
- Da die hohen Compliance-Risiken ein wesentlicher Hinderungsgrund dafür sind, Daten zu teilen, stellt sich die Frage, in welchen Konstellationen Datentreuhänder bereit sind, Compliance-Verantwortung zu übernehmen. Die Begleitforschung untersucht daher verschiedene mögliche **Datentreuhandmodelle**, die sich hinsichtlich der Risikointensität, des Datenzugriffs und der Compliance-Verantwortung unterscheiden. Für diesen Zweck lassen sich drei übergeordneten Fallgruppen unterscheiden:
  - Fallgruppe 1 (**Offene Daten**): Daten ohne Schutzinteressen werden öffentlich bereitgestellt, mit oder ohne weitere Bedingungen.
  - Fallgruppe 2 (**Geteilte Rohdaten**): Rohdaten werden nur bestimmten Nutzergruppen zugänglich gemacht, mit unterschiedlicher Tiefe der Zugriffskontrolle. Die untersuchten Pilotprojekte lassen sich am häufigsten einem Modell dieser Fallgruppe zuordnen, in dem der Datentreuhänder nur die Vertrauenswürdigkeit der Datennutzenden, nicht aber die tatsächliche Nutzung kontrolliert.
  - Fallgruppe 3 (**Geteilte Analyseergebnisse**): Nur aggregierte oder analysierte Ergebnisse werden weitergegeben. Diese dritte Fallgruppe hat das höchste Skalierungspotenzial.
- „**Sichere Verarbeitungsumgebungen**“ im Sinne des DGA sind nur solche Modelle, die nicht nur den Zugriff, sondern auch die Nutzung der Daten kontrollieren. Diese Modelle bieten das größte Potenzial zur Risikominimierung und Skalierung.
- Die vorgestellten Fallgruppen dienen als **Toolbox**, um je nach Risikointensität das passende Modell zu wählen, mit dem Ziel, das Wert-Risiko-Dilemma durch Übernahme der Compliance-Verantwortung, technische Kontrolle und organisatorische Maßnahmen so weit aufzulösen, dass das Datenteilen für alle Beteiligten lohnenswert erscheint.

Das vorliegende rechtliche Unterkapitel wird zunächst die Frage klären, wem die Daten eigentlich gehören, wer also über den Zugriff auf und die Verwendung der Daten bestimmen darf. Hierauf aufbauend wird die Rolle von Schutzgesetzen thematisiert, die beim Teilen von Daten beachtet werden müssen. Schließlich werden die verschiedenen Datentreuhandmodelle dargestellt, an die das nachfolgende technische Unterkapitel 2.4 mit seinen technisch-organisatorischen Bausteinen anknüpft.

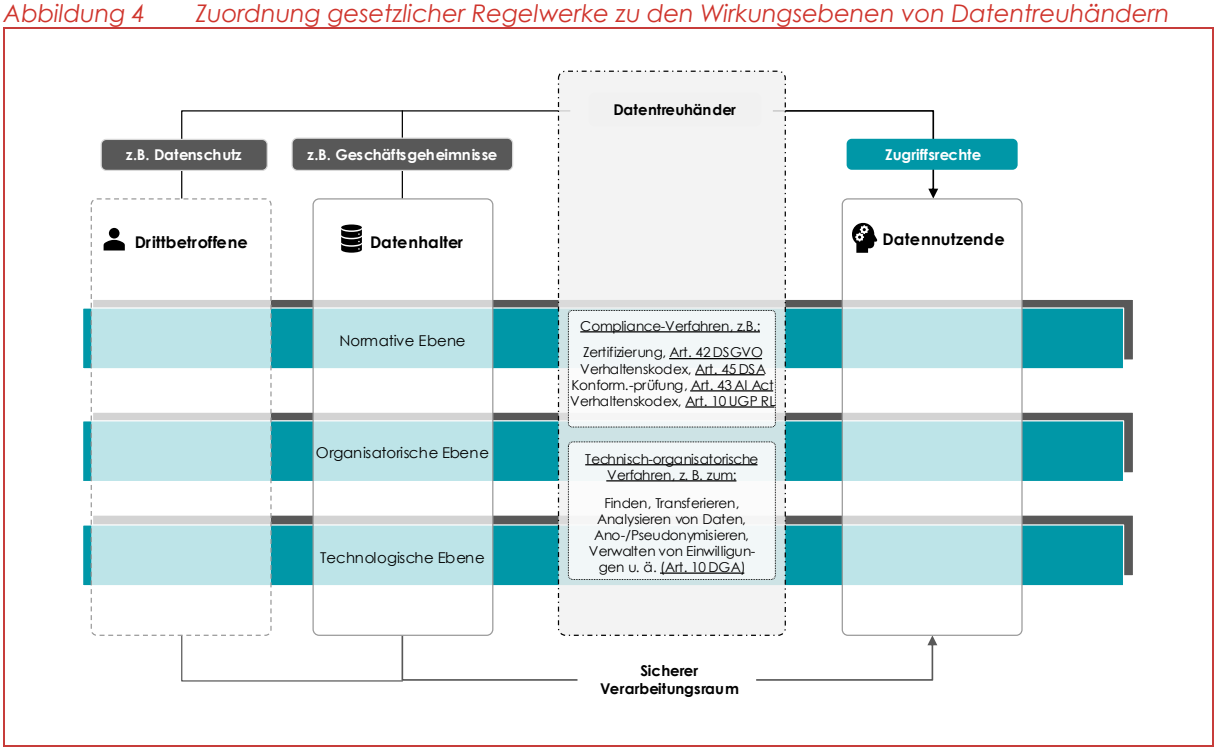
2.3.1 Klären der Data-Ownership-Frage

Ein **Eigentumsrecht an Daten**, das einer einzelnen Person ein exklusives und absolut geltendes Verfügungsrecht an Daten zuweist, gibt es im europäischen Recht nicht (zum Folgenden mit weiteren Nachweisen zum Diskussionsstand Kruse & v. Grafenstein 2025). Das Recht verfolgt vielmehr einen relativen, interessenspezifischen Ansatz, wonach es im Rahmen verschiedener Gesetze an bestimmten Daten, in bestimmten Kontexten für bestimmte Personengruppen

bestimmte Interessen schützt. Grundsätzlich lassen sich diese Gesetze danach unterscheiden, ob sie Interessengruppen vor Risiken der Verwendung von Daten schützen oder ob sie für Personen eine Teilhabe an der Wertschöpfung von Daten sicherstellen. Im Fokus der Aufmerksamkeit standen in den letzten Jahren die erstgenannten, also Schutzgesetze wie das Datenschutzrecht, das Betroffene vor den Risiken der Verarbeitung von Daten für ihre Grundrechte schützt. Aber auch der Schutz von Geschäftsgeheimnissen, von IT-Security-Risiken (siehe etwa die NIS-Richtlinien), des Wettbewerbs (z. B. i. R. d. UWG, GWB oder DMA), der Schutz vor Plattformrisiken (DSA) sowie der Schutz vor den Risiken des Einsatzes Künstlicher Intelligenz (KI-Verordnung) fallen darunter.

In jüngerer Zeit traten demgegenüber vermehrt auch **Gesetze** in den Fokus, die bestimmten Interessengruppen ein **Teilhaberecht an der Wertschöpfung von Daten** garantieren, meist in der Form von Datenzugriffs- und Verwendungsrechten. Hierzu gehören etwa der EU Data Act, die jüngst veröffentlichte EU-Verordnung über den europäischen Gesundheitsdatenraum (EHDS), nationale Gesetze wie das Datennutzungsgesetz (DNG), Personenbeförderungsgesetz (§ 3a PBefG) und das noch im Entwurfsstadium befindliche Mobilitätsdatengesetz (MDG). Neben diesen Gesetzen, die zwingende, aber bestimmten Bedingungen unterworfene Datenteilungspflichten bzw. Datenzugriffsrechte vorsehen, gibt es auch noch solche, die das Teilen von Daten erleichtern bzw. entsprechende Anreize setzen sollen. Dazu gehört der DGA, insbesondere mit seinen Regelungen zu Datenvermittlungsdiensten. Abbildung 4 zeigt, auf welchen Wirkungsebenen von Datentreuhändern die jeweiligen Gesetze ansetzen: Wie in Kapitel 2.1 ausgeführt, können Datentreuhänder auf der normativen, der organisatorischen und der technologischen Ebene beim Datenteilen unterstützen. Auf der normativ-organisatorischen Ebene wirken insbesondere Gesetze, die sicherstellen, dass Daten rechtskonform verarbeitet werden. Auf der organisatorisch-technologischen Ebene greifen wiederum Regelungen zur praktischen Umsetzung der normativen Vorgaben.

Abbildung 4 Zuordnung gesetzlicher Regelwerke zu den Wirkungsebenen von Datentreuhändern



Quelle: Eigene Darstellung (aufbauend auf v. Grafenstein, 2022).

Wichtig ist diese Unterscheidung in zweierlei Hinsicht: Erstens macht sie klar, dass sich diese Gesetze nicht widersprechen, sondern nebeneinander bestehen bzw. ineinandergreifen,

sofern sie parallel auf ein und dieselbe Datenverarbeitung anwendbar sind. Zweitens zeigt die zweite Kategorie an „Datenteilungsgesetzen", dass der Gesetzgeber die Möglichkeit Dritter, Daten ebenfalls nutzen zu dürfen, nicht dem freien Spiel des Marktes überlässt. Beide Aspekte lassen sich an einem Beispiel veranschaulichen:

Möchte ein Unternehmen A auf Daten eines Dienstanbieters B zugreifen, die dieser im Zusammenhang mit der Nutzung seines Dienstes erhoben hat, müssen beide zum einen sicherstellen, dass eine Weitergabe und Nutzung der Daten nicht das Datenschutzrecht der Endnutzenden dieses Dienstes sowie Geschäftsgeheimnisse eines Partnerunternehmens C verletzt. Eine andere Frage ist, vorausgesetzt, die Daten können unter Einhaltung des Datenschutzes und Wahrung der Geschäftsgeheimnisse grundsätzlich geteilt werden, ob Dienstanbieter B darüber frei entscheiden darf oder ob Unternehmen A einen Datenzugriffsanspruch hat. Im ersten Fall muss Unternehmen A versuchen, mit einer Gegenleistung Dienstanbieter B zu überzeugen, die Daten mit ihm zu teilen (z. B. mit einer Geldleistung, einem Datentausch, einem Mehrwertdienst etc.). Dabei steht Unternehmen A häufig vor der Herausforderung, eine Gegenleistung anbieten zu müssen, obwohl es selbst noch keinen konkreten Mehrwert aus der Nutzung der Daten gezogen hat. Aber selbst wenn Unternehmen A eine überzeugende Gegenleistung machen könnte, hängt es letztlich von der freien Entscheidung des Dienstanbieters B ab, ob er die Daten teilt oder nicht. Ein Datenzugriffsanspruch löst dieses Problem des alleinigen Entscheidungsrechts des A, das sich letztlich aus dessen technischer Kontrolle des Datenzugriffs speist, indem es B einen rechtlich abgesicherten Anspruch gibt (siehe v. Grafenstein, 2023).

Hinter Datenzugriffs- und Nutzungsrechten stehen somit ein ökonomischer, organisatorischer und normativer Gedanke: Aus ökonomischer Perspektive steigt der Wert der Daten mit der Vielzahl ihrer Verwendungsmöglichkeiten. Daher ist es sinnvoll, nicht nur derjenigen Person die Möglichkeit der Wertschöpfung zu überlassen, die die technische Kontrolle über den Zugang zu den Daten ausübt, sondern möglichst jeder Person, die einen Mehrwert aus den Daten schöpfen kann. Dem exklusiven Verwertungsinteresse des Datenhalters wird bei Datenzugriffs- und Nutzungsrechten in der Regel über den Schutz von Geschäftsgeheimnissen entsprochen, siehe etwa den Data Act. In organisatorischer Hinsicht wird die Komplexität des Austauschverhältnisses deutlich reduziert, wenn die Datennutzenden den Datenhalter nicht an der Wertschöpfung teilhaben lassen müssen (siehe zu den Schwierigkeiten bereits zuvor beim Wert-Risiko-Dilemma). Schließich klären Datenzugriffs- und Nutzungsrechte die normative Frage, wieso nur diejenigen, die den technischen Zugang zu den Daten kontrollieren, den Wert aus den Daten schöpfen können sollen. Diese Frage stellt sich vor allem in solchen Konstellationen, in denen weitere Personen oder Institutionen an der Generierung der Daten mitgewirkt haben (zum Ganzen bereits Bria et al., 2023).

Ein weiterer wichtiger Aspekt, der durch die Unterscheidung zwischen Schutzgesetzen und Datenzugriffsrechten klar wird, ist, dass das Wert-Risiko-Dilemma nicht nur in Situationen des freiwilligen Datenteilens auftritt, sondern auch beim **gesetzlich verpflichtenden Datenteilen.** Der Unterschied, der sich dabei ergibt, ist der Wechsel der Perspektive: Beim freiwilligen Teilen der Daten kommt es primär auf die Perspektive der Datengebenden an, ob die ihnen von den Datennutzenden versprochene Teilhabe an deren Wertschöpfung die Risiken und Kosten so weit überwiegen, dass die Datengebenden das Teilen ihrer Daten lohnend finden. Bei **gesetzlichen Datenzugriffsrechten** ist es umgekehrt. Hier geht es primär um die Perspektive der potenziellen Datennutzenden und die Frage, ob der mit dem Datenteilen verbundene erwartete Mehrwert die Compliance-Risiken und wirtschaftlichen Kosten überwiegt, sodass es nun den Datennutzenden lohnend erscheint, ihr Datenzugriffsrecht (wenn nötig mit Hilfe der zuständigen Behörden und Gerichte) gegenüber den Datenhaltenden durchzusetzen. Auch in diesen Situationen können Datentreuhänder eine wesentliche Rolle bei der Überwindung der Interessenkonflikte an den Daten spielen (Bria et al., 2023; Kerber & Gill, 2024).

2.3.2 *Datentreuhandmodelle kategorisiert nach Intensität der Compliance-Risiken*

Eng verknüpft mit der Frage, wie Datentreuhänder die Compliance-Risiken der Datengebenden minimieren, ist die Frage, wer in diesem Dreiecksverhältnis zwischen Datengebenden, Datennutzenden und Datentreuhändern rechtlich die Verantwortung für die Einhaltung der **Compliance-Anforderungen** übernimmt. Denn letztlich geht es darum, wer für einen Verstoß gegen die einschlägigen Schutzgesetze geradestehen muss. Dabei sehen sich Datentreuhänder bei der Klärung der Compliance-Verantwortlichkeiten einer doppelten Herausforderung gegenüber: Von Datentreuhändern wird nicht nur erwartet, dass sie die Compliance-Risiken der Datengebenden minimieren, sondern sie müssen auch ihre eigenen Compliance-Risiken kontrollieren. Diese Doppelaufgabe wird für sie zusätzlich dadurch erschwert, dass der Gesetzgeber an sie weitere Anforderungen stellt. Zu nennen ist hier allen voran der DGA, der sogenannte Datenvermittlungsdienste reguliert (insbesondere Art. 12 DGA).

Was regelt der DGA in Bezug auf Datentreuhänder?

In seinem dritten Kapitel regelt der DGA sogenannte Datenvermittlungsdienste (Art. 10 ff.). Diesen schreibt Erwägungsgrund 27 DGA eine Schlüsselrolle in der Datenwirtschaft zu, weil sie die „gemeinsame Datennutzung" zwischen Unternehmen unterstützen und „im Zusammenhang mit den im Unionsrecht oder im nationalen Recht festgelegten Verpflichtungen" erleichtern sollen.

Art. 2 Nr. 11 DGA definiert Datenvermittlungsdienste sowohl positiv als auch negativ. Hervorgehoben sollen insofern die folgenden Kriterien werden: Zum einen geht es positiv um die

- Bereitstellung technischer, rechtlicher oder sonstiger Mittel,
- um Geschäftsbeziehungen zwischen einer unbestimmten Anzahl von betroffenen Personen (im Sinne des Datenschutzes) oder Dateninhabern einerseits und Datennutzern andererseits herzustellen,
- um die gemeinsame Datennutzung zu ermöglichen.

Ein Nebensatz stellt klar (siehe neben Art. 2 Nr. 11 ebenso Art. 10 lit. b DGA), dass die Definition des Datenvermittlungsdienstes auch die Bereitstellung von Mitteln für Zwecke der Ausübung der Rechte betroffener Personen in Bezug auf ihre personenbezogenen Daten erfasst (also z. B. zum Einholen oder Abgeben von Einwilligungen oder zur Durchsetzung von Datenauskunftsansprüchen). Unter den Negativkriterien soll hier Art. 2 Nr. 11 lit. a DGA hervorgehoben werden. Danach fallen solche Dienste nicht unter den Begriff des Datenvermittlungsdienstes, in deren Rahmen

- Daten von Dateninhabern eingeholt und aggregiert, angereichert oder umgewandelt werden,
- um deren Wert erheblich zu steigern,
- und Lizenzen für die Nutzung der resultierenden Daten an die Datennutzer vergeben werden,
- ohne eine Geschäftsbeziehung zwischen Dateninhabern und Datennutzern herzustellen.

Damit dürften viele sogenannte Data Broker nicht in den gesetzlichen Anwendungsbereich fallen, da bei diesen genau die Analyse von zu teilenden Daten im Vordergrund steht, und sie somit nicht den Anforderungen aus Art. 10 ff. DGA entsprechen. Gleichzeitig bieten sie durch die angebotenen Mehrwertdienste ein besonders hohes Wertschöpfungspotenzial (siehe Kapitel 2.6.3).

Um die Neutralität von Datenvermittlungsdiensten und damit das Vertrauen in sie sicherzustellen, müssen sich die Anbieter dieser Dienste bei der zuständigen Behörde anmelden, die die Einhaltung einer Reihe von Anforderungen überwacht. Zu diesen

Anforderungen gehört insbesondere die Vorgabe, dass Datenvermittlungsdienste die Daten für keine anderen Zwecke nutzen dürfen, als sie den Datennutzenden zur Verfügung zu stellen. Außerdem müssen sie über eine gesonderte juristische Person bereitgestellt werden (lit. a). Die Anmeldung als Datenvermittlungsdienst nach dem DGA kann potenziell als staatlich abgesicherter Vertrauensanker für Datengebende und -nutzende fungieren, indem sie signalisiert, dass der Dienst alle Interessen neutral vertritt und in einen Ausgleich bringt. Inwiefern sich dieses Instrument in der Praxis tatsächlich bewährt, bleibt jedoch abzuwarten. Bislang haben sich europaweit 24 Dienste registrieren lassen, wobei zu berücksichtigen ist, dass eine Pflicht zur Registrierung erst ab September 2025 greift. [3]

Wie oben bereits gezeigt, ist der Begriff der Datenvermittlungsdienste einerseits sehr weit definiert. Auch das ist zu begrüßen, da so auch technische oder sonstige Mittel darunter fallen, die den Austausch oder die gemeinsame Nutzung von Daten ermöglichen (Art. 2 Nr. 11 und Art. 10 lit. b). Entsprechende Funktionen bietet Apple mittlerweile an (siehe Safari)[4]. Google wiederum hatte eine solche Funktion bereits angekündigt, dann jedoch wieder fallen gelassen (siehe Chrome)[5]. Die wettbewerbsrechtlichen Verfahren gegen Apple und Google zeigen, dass eine staatlich abgesicherte Pflicht zur neutralen (und nicht eigennützigen) Erbringung solcher Mittel bzw. Dienste wichtig ist. Das gilt für alle anderen Personal Information Management Services (wie Dienste zur Verwaltung von Einwilligungen gemäß § 26 TDDDG).

Andererseits adressiert der DGA andere Bereiche nur am Rande oder lässt sie explizit außen vor. Auffallend ist zunächst, dass der DGA zwar explizit bezweckt, mit den Datenvermittlungsdiensten das Vertrauen in das Teilen von Daten zu steigern, dabei aber die Rechtsunsicherheiten nicht ausreichend konkret adressiert. Beim Schutz von Geschäftsgeheimnissen stellt sich das Problem weniger, da der Ausgleich nur zwischen den Datengebenden und -nutzenden geregelt wird. Hier kann der Datentreuhänder also zivilrechtlich vermitteln. Sobald es aber um die Verletzung öffentlich-rechtlicher Vorgaben geht, die zumindest auch durch öffentliche Behörden durchgesetzt werden, wie im Datenschutz- oder Wettbewerbsrecht, kann ein Datentreuhänder weit weniger zur Rechtssicherheit beitragen (siehe im Detail bereits Technopolis Group et al., 2024b). Um die Rechtsunsicherheit beim Datenteilen auch bei solchen Regelungen zu reduzieren, wäre es etwa naheliegend gewesen, Verfahren zum Nachweis der Einhaltung der diversen rechtlichen Anforderungen vorzusehen oder zumindest mit Verfahren aus solchen Gesetzen abzustimmen (siehe etwa Art. 40 ff. DSGVO in Bezug auf Verhaltensrichtlinien und Zertifizierungsprogramme, Art. 45 DSA sowie Art. 10 UGP-RL in Bezug auf entsprechende Verhaltenskodizes oder Art. 43 AI Act in Bezug auf Konformitätsprüfungen).

Vor diesem Hintergrund sollen die verschiedenen **Kategorien für Datentreuhandmodelle aus rechtlicher Perspektive** dargestellt werden, die auf Grundlage der empirischen Befunde aus der Begleitforschung entwickelt wurden. Das folgende Schaubild (Abbildung 5) teilt die verschiedenen beobachteten bzw. aufgrund der empirischen Befunde analytisch entwickelten Modelle von links nach rechts danach ein, wie klein oder groß die (Compliance-)Risiken sind, die der Datentreuhänder kontrollieren soll, und wie umfassend die von ihm zur Verfügung gestellten Kontrollmechanismen entsprechend sein müssen. Danach enthält die von der Begleitforschung erarbeitete Kategorisierung drei Grundtypen (**Fallgruppen**), die sich weiter ausdifferenzieren lassen. Dabei lässt sich jeweils die rechtliche Rolle des

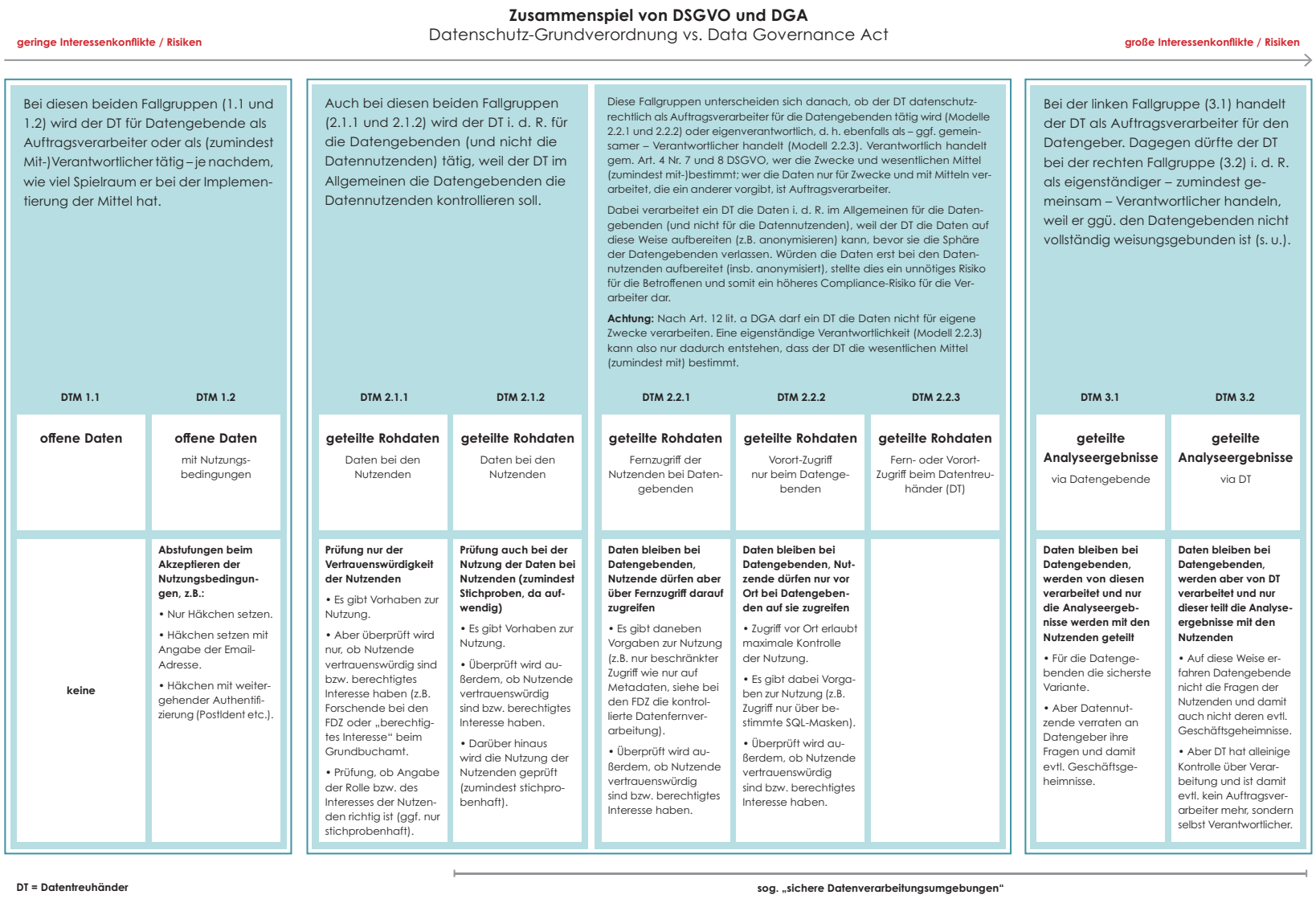
[3] EU register of data intermediation services: https://digital-strategy.ec.europa.eu/en/policies/data-intermediary-services (zuletzt abgerufen am 7. August 2025).

[4] Siehe das Blocken von Pop-up-Fenstern, wie etwa sog. Cookie-Banner, was das Verweigern von angefragten Einwilligungen erleichtert, unter https://support.apple.com/de-de/102524 (zuletzt abgerufen am 5. Juni 2025).

[5] Zunächst angekündigt mit Blogpost vom 22. Juli 2024 unter https://privacysandbox.com/news/privacy-sandbox-update/ und dann wieder zurückgenommen mit einem Blogpost vom 22. April 2025 unter https://privacysandbox.com/news/privacy-sandbox-next-steps/ (beide zuletzt abgerufen am 5. Juni 2025).

Datentreuhänders bzw. der Compliance klären, die dieser im Verhältnis zu den Datengebenden und -nutzenden ein- bzw. übernehmen sollte.

Abbildung 5 Szenarien für die Umsetzung des Datenteilens durch verschiedene Datentreuhandmodelle



Quelle: Eigene Darstellung.

Zentral ist u. a. die Frage, auf welche Weise ein Datentreuhänder die **Anforderungen des Datenschutzrechts** an das Teilen von Daten erfüllt bzw. erfüllen sollte, um die Interessenkonflikte zumindest in dieser Hinsicht erfolgreich aufzulösen. Hier gibt es zwei grundsätzliche Wege: Die Datengebenden und -nutzenden holen dafür entweder die Einwilligung der Betroffenen ein. Im privaten Sektor führt an der Einwilligung (oder dem Vertragsmodell) in der Regel dann kein Weg vorbei, wenn mit den Informationen einzelne Personen evaluiert werden sollen (z. B. um Dienste bzw. Leistungen an ihre individuellen Bedürfnisse, Interessen oder Fähigkeiten anzupassen). Anders gelagert ist der Fall, wenn statistische Informationen über Personengesamtheiten gewonnen werden, ohne dass dies negative Auswirkungen auf Personen hätte. In diesen Situationen spielen sichere Verarbeitungsumgebungen eine herausgehobene Rolle, weil sie das Risiko minimieren, dass Datennutzende doch einen direkten Bezug zwischen den verarbeiteten Informationen und einer einzelnen Person herstellen können (siehe hierzu im Detail Rupp & v. Grafenstein, 2024). Klargestellt sei hier, dass die Einholung der Einwilligung der Betroffenen keine uneingeschränkte Erlaubnis zur Verarbeitung personenbezogener Daten darstellt. Nicht nur müssen auch hier objektiv-strukturelle Schutzmaßnahmen wie etwa zur Datenminimierung und Vertraulichkeit eingehalten werden, sondern auch die weiteren Betroffenenrechte wie Datenzugang, -korrektur und -löschung. Auch insofern spielen Datentreuhänder also eine sehr wichtige Rolle, indem sie die geeigneten technisch-organisatorischen Maßnahmen zur Verfügung stellen.

Die in Abbildung 5 dargestellten Datentreuhandmodelle dienen aber nicht nur dazu, Datenschutzrecht einzuhalten. Im Kern geht es darum, in zunehmendem Ausmaß zu kontrollieren, unter welchen Bedingungen Datennutzende die Daten verwenden. Damit helfen die verschiedenen Datentreuhandmodelle genauso, den Schutz von Geschäftsgeheimnissen, der IT-Sicherheit oder des Wettbewerbs entsprechend den jeweiligen Schutzbedürfnissen einzuhalten. Immer wieder explizit wird auch auf den **DGA** Bezug genommen. Im Folgenden werden die in der oberen Abbildung aufgeführten Fallgruppen im Detail beschrieben und verglichen.

2.3.3 Fallgruppe 1 (Offene Daten)

Bei der ersten Klasse der oben dargestellten Datentreuhandmodelle sind die (Compliance-)Risiken am niedrigsten. Das bedeutet, dass diese Daten in der Regel nicht geschützt sind, also sie u. a. keinen Personenbezug im Sinne der DSGVO aufweisen und auch keine Geschäftsgeheimnisse beinhalten. Da hier keine Schutzinteressen Dritter verletzt sind, können die Daten der Allgemeinheit offen zur Verfügung gestellt werden. In dieser Klasse gibt es zwei Unterarten an Datentreuhandmodellen:

Nur das erste Modell ganz links in der obigen Abbildung (Datentreuhandmodell 1.1) erfüllt streng genommen die Anforderungen eines echten **Open-Data-Modells.** Denn nur hier stehen die Daten der Allgemeinheit bedingungslos zur Verfügung (siehe etwa die Open-Data-Definition bei Open Knowledge Foundation, o. J.). Im zweiten Modell von links (Datentreuhandmodell 1.2) stehen die Daten zwar der Allgemeinheit zur Verfügung, werden aber mit Bedingungen versehen. Die Bindung an solche Bedingungen ist allerdings schwach, weil ihre Einhaltung zumindest aktuell kaum eingeklagt oder anderweitig technisch eingefordert wird. Praktisch bauen diese Bedingungen also darauf, dass die Datennutzenden sie freiwillig einhalten. Dabei sind unterschiedliche Anforderungen vorstellbar, unter denen Datennutzende ihr Einverständnis mit den Nutzungsbedingungen erklären müssen: vom Setzen eines Häkchens innerhalb der Download-Maske bis hin zur Authentifizierung im Wege eines PostIdent-Verfahrens. Die unterschiedlichen Anforderungen für das Einverständnis dürften dabei hauptsächlich psychologische Wirkung auf die Datennutzenden haben.

Bei beiden Fallgruppen wird der Datentreuhänder in der Regel für die Datengebenden als Auftragsverarbeiter, manchmal aber auch als (zumindest Mit-)Verantwortlicher tätig – je nachdem, wie viel Spielraum er bei der Implementierung der Mittel hat. Aus datenschutzrechtlicher Compliance-Sicht ist es zunächst vorzugswürdig, wenn der

Datentreuhänder nur als Auftragsverarbeiter und nicht als (gemeinsam) Verantwortlicher in Erscheinung tritt, da Letzteres unter anderem eine eigene Rechtsgrundlage erfordert.

Die Einschaltung eines Datentreuhänders kann hier in Form eines rein technischen Betreibers einer Open-Data-Plattform vorkommen. Wenn die Daten vor Veröffentlichung noch bereinigt oder gar anonymisiert werden müssen, kann es verlässlicher und vor allem kostengünstiger sein, für die Erledigung dieser komplexeren Aufgaben einen darauf spezialisierten Datentreuhänder einzusetzen. Je komplexer diese Aufgabe ist und je mehr sie die Kontrollfähigkeit des Datengebenden übersteigt, desto eher sollte der Datentreuhänder zumindest im Innenverhältnis auch die Compliance-Verantwortung übernehmen.

Prinzipiell kann ein solcher Dienst auch ein **Datenvermittlungsdienst** gemäß Art. 2 Nr. 11 und Art. 10 DGA sein. Fraglich ist jedoch in der ersten Unterfallgruppe, ob ein solcher Datentreuhänder seine Dienste anbietet, um Geschäftsbeziehungen zwischen den Datengebenden und Datennutzenden herzustellen. Eher denkbar ist dies bei der zweiten Unterfallgruppe, weil hier der Datentreuhänder zumindest Nutzungsbedingungen an die Datennutzenden im Namen der Datengebenden weitergibt. Werden die Daten bedingungslos der Allgemeinheit zur Verfügung gestellt, ist ein solches Rechtsgeschäft fragwürdiger.

2.3.4 Fallgruppe 2 (Geteilte Rohdaten)

In der zweiten Fallgruppe der „geteilten Rohdaten" werden die Daten nicht der Öffentlichkeit zur Verfügung gestellt, sondern nur bestimmten Nutzergruppen. Dabei geht es nicht darum, andere Nutzergruppen willkürlich von der Datennutzung auszuschließen. Vielmehr folgt die Prüfung der Nutzergruppen bei diesen Datentreuhandmodellen zwei Sachgründen: Zum einen definieren diese Datentreuhandmodelle bestimmte Datennutzergruppen auf Basis einer typisierten Interessenabwägung. Dabei werden Nutzergruppen bestimmt, denen ein gegenüber der Allgemeinheit größeres Interesse an der Nutzung der jeweiligen Daten zugeschrieben wird. Gleichzeitig kann im Wege dieser Modelle zunehmend sichergestellt werden, dass die Datennutzenden die Nutzungsbedingungen einhalten. Hier ergeben sich zudem die Unterschiede zwischen den Unterarten dieser zweiten Klasse an Datentreuhandmodellen, die im Folgenden beschrieben werden.

<u>Datennutzung in der Verantwortungssphäre der Datennutzenden (Unterfallgruppe 2.1)</u>

Ein erster Unterschied lässt sich danach vornehmen, ob die Daten die Verantwortungssphäre der Datengebenden verlassen und an die Datennutzenden übermittelt werden („Daten bei Datennutzenden", Unterfallgruppe 2.1) oder ob die Datennutzenden nur innerhalb der Verantwortungssphäre der Datengebenden auf die Daten zugreifen dürfen („Daten bei Datengebenden", Unterfallgruppe 2.2). Verlassen die Daten die Verantwortungssphäre des Datengebenden, hat es für die Datennutzenden den Vorteil, dass diese die Daten in ihren eigenen Einrichtungen mit ihren eigenen technisch-organisatorischen Möglichkeiten verarbeiten können und damit freier in ihrer Verwendung sind. Vor allem für die Datengebenden hat dies jedoch den Nachteil, dass sie dann nicht so umfassend kontrollieren können, wie die Datennutzenden die Daten konkret verwenden, sprich, ob sich diese an die Nutzungsbedingungen halten.

Eine weitere Unterscheidung lässt sich entsprechend der **Tiefe der Verwendungskontrolle** vornehmen. Beim Datentreuhandmodell mit der niedrigsten Kontrolldichte (Datentreuhandmodell 2.1.1) prüft der Datentreuhänder gar nicht, wie die Datennutzenden die Daten bei sich konkret verwenden. Geprüft wird nur, ob die Datennutzenden zum Kreis der begünstigten Datennutzungsgruppe gehören. Im Übrigen nimmt das Datentreuhandmodell an, dass die Datengebenden kraft der (überprüften) Rolle der Datennutzenden darauf vertrauen, dass die Datennutzenden die Nutzungsbedingungen auch einhalten. Aufgrund der niedrigen Prüftiefe handelt es sich innerhalb dieser zweiten Fallgruppe um das

Datentreuhandmodell mit dem geringsten Aufwand. Auffällig ist, dass die meisten Pilotprojekte dieses Datentreuhandmodell für sich gewählt haben.

Zumindest mit zwei Pilotprojekten wurde jedoch auch diskutiert, ob es angesichts der Missbrauchsrisiken angemessener wäre, nicht nur die Vertrauenswürdigkeit der Datennutzenden, sondern auch die konkrete Verwendung der Daten bei und durch die Datennutzenden zu kontrollieren (Datentreuhandmodell 2.1.2). Bei einem dieser Projekte, das den Austausch von Cyber-Security-Vorfällen zwischen Unternehmen organisiert, ist der Projekterfolg maßgeblich davon abhängig, dass diese Informationen nicht in die Hände von Hackern fallen. Möchte man das Risiko ausschließen, dass sich Hacker in das Unternehmen der begünstigten Datennutzergruppe einschleusen, würde eine bloße Überprüfung der Datennutzenden nicht ausreichen. Vielmehr müsste darüber hinaus auf Applikationsebene nachvollzogen werden, welche konkreten Personen aus welchen Abteilungen mit welchen Anwendungen auf die Daten zugreifen. Ähnliches wurde mit einem weiteren Pilotprojekt diskutiert, wo ähnlich hohe Schutzinteressen Dritter, nämlich das Bankgeheimnis und die Vertraulichkeit von Steuerberatern, betroffen sind.

Eine solche Kontrolldichte auf Applikationsebene hat allerdings den Nachteil, dass sie die Implementierung des Zero-Trust-Prinzips im technisch-organisatorischen System der Datennutzenden erfordert. Da dabei jeder Zugriff individuell autorisiert und kontrolliert werden muss, entsteht ein nicht unerheblicher Aufwand beim Erstellen der „white-listed" Applikationen, Personen und Abteilungen. Auch sollte dieses Datentreuhandmodell nicht darüber hinwegtäuschen, dass selbst hier eine Applikation noch missbräuchlich angewendet werden kann oder die sensiblen Informationen zumindest über den Bildschirm durch reines Lesen oder per Videoaufnahme ausgelesen werden und auf einen anderen Datenspeicher übertragen werden können. Immerhin ließe sich dieses Risiko mit organisatorischen Mitteln weiter reduzieren, etwa indem die befugten Mitarbeitenden entsprechende Nutzungsvereinbarungen unterschreiben und deren Einhaltung durch das Unternehmen selbst oder durch externe Audits zumindest stichprobenhaft überprüft wird. Letztlich erfordert auch der Einsatz solcher organisatorischen Mittel aber ein gewisses Vertrauen, dass die entsprechenden Mitarbeitenden die Bedingungen entweder aus Rechtschaffenheit oder Angst vor Aufdeckung einhalten.

Auch hier ist es zumindest datenschutzrechtlich vorzugswürdig, wenn der Datentreuhänder im Auftrag der Datengebenden handelt, also weitgehend weisungsgebunden ist. Der Europäische Gerichtshof (EuGH) interpretiert die gemeinsame Festlegung der technischen oder (!) organisatorischen Mittel gemäß Art. 26 i. V. m. Art. 4 Nr. 7 DSGVO in seinen jüngsten Urteilen allerdings sehr weit. Danach kann eine gemeinsame Verantwortlichkeit einer Person selbst dann vorliegen, wenn sie gar keinen technischen Zugang zu den Daten hat, sondern nur den Zugang organisiert (EuGH, 2018, Rz. 69 ff.; EuGH, 2024, Rz. 59 ff.). Damit könnte auch ein Datentreuhänder als ein mit den Datengebenden gemeinsam Verantwortlicher angesehen werden, selbst wenn er nur die Voraussetzungen der Datennutzenden für den Zugang bzw. die Nutzung kontrolliert. So ist umso eher an eine (eventuell gemeinsame) Verantwortlichkeit des Datentreuhänders zu denken, je komplexer dieser Prüfvorgang wird und je stärker dieser die tatsächlichen Kontrollmöglichkeiten der Datengebenden übersteigt. In solchen Fällen sollte der Datentreuhänder zumindest im Innenverhältnis auch die Compliance-Verantwortung übernehmen.

In jedem Fall sollte der Datentreuhänder in der Regel im Auftrag der Datengebenden und nicht der Datennutzenden tätig werden. Dies ergibt sich bereits daraus, dass der Datentreuhänder die Datennutzenden kontrollieren soll. Dieses Ziel würde unterlaufen, wenn der Datentreuhänder im Auftrag der Datennutzenden tätig würde.

Der offene Wortlaut von Art. 2 Nr. 11 und Art. 10 DGA legt es nahe, dass auch die in diesem Abschnitt besprochenen Datentreuhandmodelle 2.1.1 und 2.1.2 ein Datenvermittlungsdienst im Sinne des DGA sein können. Zumindest dürfte das Datentreuhandmodell auf die Herstellung von Geschäftsbeziehungen zwischen Datengebenden und Datennutzenden gerichtet sein.

Bei genauerer Betrachtung der einzelnen Vorschriften scheint der Gesetzgeber allerdings mehr das klassische Durchleitungsmodell vor Augen gehabt zu haben. Dieser Ausdruck meint, dass ein Datentreuhänder die Daten von den Datenhaltenden technisch bei sich einsammelt und dann an die Datennutzenden ausgibt. Ob Datentreuhänder in dieser zweiten Klasse die Daten wirklich immer selbst bei sich vorhalten, ist zumindest dann zweifelhaft, wenn der Datentreuhänder lediglich den Zugang und die Nutzung der Daten anhand normativer Vorgaben kontrolliert. Ob der Gesetzgeber diese Fälle wirklich ausschließen wollte oder diese Fälle lediglich übersehen hat, kann an dieser Stelle nicht abschließend bewertet werden. Sinnvoll wäre es aber, sämtliche Dienste zu erfassen und zu fördern, die das Datenteilen rechtlich, technisch oder organisatorisch unterstützen.

Datennutzung in der Verantwortungssphäre des Datengebenden (Unterfallgruppe 2.2)

Werden die Daten als so sensibel eingestuft, dass das Risiko nicht hinnehmbar erscheint, dass Datennutzende sie z. B. über einen Bildschirm auslesen können, empfehlen sich Datentreuhandmodelle, in denen die Datennutzung ausschließlich in der Verantwortungssphäre der Datengebenden erfolgt. Das gibt den Datengebenden weitestgehende Kontrollmöglichkeit. Selbst ob Datennutzende die Informationen über den Bildschirm auslesen und sich auf einem Zettel notieren, könnten Datengebende auf diese Weise kontrollieren (z. B., indem sie eine Videokamera oder eine überwachende Person in dem Raum postieren).

Auch wenn dieser Fall bei keinem der Pilotprojekte beobachtet wurde, kommt es in der Praxis vor. Prominentes Beispiel sind die Forschungsdatenzentren (FDZ). Hier gibt es einen sogenannten On-Site-Zugang für Daten (vergleiche Datentreuhandmodell 2.2.2), die nur „formal anonymisiert" sind, bei denen also nur die direkten Identifier entfernt wurden (was einer bloßen Pseudonymisierung gleichkommt). Weil der reine On-Site-Zugang für Forschende relativ aufwändig ist (man denke an die Anfahrt), bieten die FDZ mittlerweile auch einen Remote-Zugang an (vergleiche Datentreuhandmodell 2.2.1). Die Datennutzung findet dabei ebenfalls in der technischen Infrastruktur der FDZ statt; ein Download der Daten ist ausgeschlossen.[6] Datennutzende können aber von ihrer Heimatinstitution aus zugreifen. Letztlich ist der Remote-Zugang ein Kompromiss zwischen dem bloßen On-Site-Zugang bei den Datengebenden und dem vorbeschriebenen Datentreuhandmodell, in dem die Daten zwar an die Datennutzenden übergeben, dort von den Datengebenden nun aber ihrerseits remote bzw. mittelbar kontrolliert werden. Die Übergänge zwischen den verschiedenen Unterklassen können in der Praxis je nach Ausgestaltung fließend sein.

Wichtig ist klarzustellen, dass die FDZ datenschutzrechtlich nicht als Auftragsverarbeiter der ursprünglichen Datengebenden, sondern als eigenständig Verantwortliche handeln (vergleiche Datentreuhandmodell 2.2.3). Die Übermittlung der Daten von den ursprünglichen Datengebenden an die FDZ, die Anonymisierung der Daten und Verfügbarmachung beruhen somit auf einer eigenen Rechtsgrundlage (§ 16 Abs. 6 BStatG). Dagegen zeigt die hier vorgestellte Kategorisierung beide Zugriffswege zunächst als Datentreuhandmodell, bei denen der Zugriff bei den ursprünglichen Datengebenden erfolgt (vergleiche Datentreuhandmodelle 2.2.1 und 2.2.2). Handelt ein Datentreuhänder hier als reiner Auftragsverarbeiter, hat dies den Vorteil, dass die Übermittlung keiner eigenen Rechtsgrundlage bedarf; mit zunehmender Komplexität der Tätigkeit des Datentreuhänders sollte aber an eine Übernahme der Compliance-Verantwortung zumindest im Innenverhältnis zwischen Datentreuhänder und Datengebenden gedacht werden.

Prüft der Datentreuhänder nicht nur den Zugang und die Nutzung entsprechend normativer Vorgaben, sondern stellt auch die technische Infrastruktur für die Datenverarbeitung bereit

[6] Siehe zu den verschiedenen Zugangswegen und Anonymisierungsformen auf der Website der Forschungsdatenzentren unter https://www.forschungsdatenzentrum.de/de/zugang und https://www.forschungsdatenzentrum.de/de/anonymitaet (beide zuletzt abgerufen am 5. Juni 2025).

(siehe das zuvor benannte Durchleitungsmodell), dürfte außerdem ein Datenvermittlungsdienst gemäß Art. 2 Nr. 11 und Art. 10 DGA vorliegen. Erst recht gilt dies, wenn der Datentreuhänder Datensätze von verschiedenen Datengebenden einsammelt, aufbereitet und Datennutzenden zur Verfügung stellt. In diesem Fall ist der Datentreuhänder unstreitig gemeinsam mit den Datengebenden handelnder Verantwortlicher im Sinne der DSGVO, wenn es sich um personenbezogene Daten handelt (vergleiche Datentreuhandmodell 2.2.3).

2.3.5 Fallgruppe 3 (Geteilte Analyseergebnisse)

Schließlich gibt es Datentreuhandmodelle, in denen die Datennutzenden überhaupt keinen Zugriff auf die Rohdaten erhalten. In diesen Fällen stellen die Datennutzenden lediglich ihre Anfrage, die sie mit dem Datensatz der Datengebenden beantworten möchten. Im Datentreuhandmodell 3.1 generieren die Datengebenden dann die Antworten (gegebenenfalls mit Hilfe eines hierfür beauftragten Datentreuhänders) und übergeben diese den Datennutzenden. Aus Sicht betroffener Dritter ist dies das sicherste Datentreuhandmodell, weil hier das Risiko am niedrigsten ist, dass die Datennutzenden die in den Rohdaten enthaltenen personenbezogenen oder geschäftsgeheimnisrelevanten Informationen erhalten. Enthalten diese Antworten keine personenbezogenen Informationen, bedarf es selbst für die Übergabe dieser Daten an die Datennutzenden keiner Rechtsgrundlage mehr. Da der Datentreuhänder keine Rohdaten übermittelt, ist auch fraglich, ob er als Datenvermittlungsdienst im Sinne des Art. 2 Nr. 4 und Art. 10 DGA anzusehen ist. Andererseits spricht Art. 12 lit. e DGA dafür, da dort eine solche Aufbereitung der Daten zur Erleichterung der Datenübermittlung ausdrücklich vorgesehen ist.

Anders dürfte dies dagegen bei der Variante zu beurteilen sein, in der der Datentreuhänder die Ergebnisse generiert und die Datengebenden bewusst aus dem Analysevorgang herausgehalten werden (Datentreuhandmodell 3.2). Ein solches Modell kommt insbesondere in Fällen in Betracht, in denen die Datennutzenden allein schon ihre Frage als geschäftsgeheimnisrelevant betrachten. Sollten die Datengebenden potenzielle Wettbewerber sein, möchten die Datennutzenden vermeiden, dass die Datengebenden durch die Frage auf die Geschäftsidee schließen können. Hier kommt die „treuhänderische" Funktion des Datentreuhänders besonders stark zum Tragen. Gleichzeitig sind genau dies die Fälle, die aus dem Anwendungsbereich des DGA ausgeschlossen werden. Denn Art. 2 Nr. 11 lit. a DGA schließt wie geschildert solche Dienste aus, „in deren Rahmen Daten von Dateninhabern eingeholt und aggregiert, angereichert oder umgewandelt werden, um deren Wert erheblich zu steigern, und Lizenzen für die Nutzung der resultierenden Daten an die Datennutzer vergeben werden, ohne eine Geschäftsbeziehung zwischen Datengebern und Datennutzern herzustellen". Dieser Fall liegt im letzten hier beschriebenen Datentreuhandmodell 3.2 nach Einschätzung der Begleitforschung wohl vor.

Tatsächlich ist dieser Fall gar nicht so selten, wie er zunächst erscheinen mag. Bei zwei medizindatenschutzrechtlichen Pilotprojekten konnte zwar nicht abschließend geklärt werden, ob sie eher der ersten oder der zweiten Unterfallgruppe der geteilten Analyseergebnisse zuzuordnen sind. Spätestens in Gesprächen mit einem dritten Pilotprojekt stellte sich aber heraus, dass für einen zukünftig geplanten Analysedienst eindeutig das letzte Datentreuhandmodell hilfreich wäre: Bei diesem Pilotprojekt weist der Datentreuhänder in seinem Basisdienst Aufträge verfügbaren Spediteuren zu. Für den zusätzlichen Dienst möchte der Datentreuhänder nun wiederum die Auslastung der Spediteure erfahren, um Aufträge umweltverträglicher auf sie verteilen zu können. Die Spediteure sind aber zurückhaltend, diese Informationen herauszugeben, weil die Auftraggeber anhand dieser Informationen die Preise drücken könnten (etwa weil der Auftraggeber hierdurch erkennt, dass ein wenig ausgelasteter Spediteur wirtschaftlich auf den Auftrag angewiesen ist). Dieses Vertrauensproblem lässt sich dadurch lösen, dass weder Datengebende noch Datennutzende die Daten erhalten, sondern nur der Datentreuhänder die Daten sammelt, aufbereitet und dann anhand der Analyseergebnisse die Speditionsaufträge verteilt.

Nach Einschätzung der Begleitforschung hat **diese dritte Fallgruppe das größte Entwicklungspotenzial**. Denn nicht nur ist sie einem niedrigeren Regulierungsdruck ausgesetzt, da der DGA nicht zur Anwendung kommt. Sie hat auch das größte Skalierungspotenzial. Anders als bei den meisten anderen Modellen konzentriert sich hier der Datentreuhänder auf einen bestimmten Datentyp und ein bestimmtes analytisches Verfahren. Sind die Algorithmen auf dieses einmal eingestellt, inklusive etwaiger Verfahren zum Schutz sensibler Daten, lassen sich diese auf eine Vielzahl vergleichbarer Fälle mit den entsprechenden Skaleneffekten übertragen.

2.3.6 Sichere Verarbeitungsumgebungen und Zertifizierungsverfahren

Schließlich soll kurz auf die Frage eingegangen werden, welche der vorgestellten Datentreuhandmodelle eigentlich unter den Begriff der „sicheren Datenverarbeitungsumgebungen" fallen. Der Begriff findet mittlerweile nicht nur im Gesetz Niederschlag (siehe insbesondere Art. 5 Abs. 3 lit. c und Art. 2 Nr. 20 DGA), sondern wird in der Literatur auch zunehmend als zentraler Lösungsbaustein für das sichere Teilen von Daten diskutiert (z. B. Specht-Riemenschneider, 2024). Aus Sicht der Begleitforschung sollten unter diesen Begriff nur solche Datentreuhandmodelle gefasst werden, die nicht nur den Zugriff auf die Daten, sondern auch die Nutzung der Daten kontrollieren. Demnach gelten nur die Datentreuhandmodelle 2.1.2 bis 3.2 (vergleiche Abbildung 5) als „sichere Verarbeitungsumgebungen". Die Datentreuhandmodelle der ersten Fallgruppe sowie das erste Modell der zweiten Fallgruppe (2.1.1) dagegen kontrollieren nicht die Datennutzung und fallen aus Sicht der Begleitforschung daher nicht unter den Begriff. Als abschließend sollte diese Meinung hier aber nicht verstanden werden. Ziel der dargestellten Datentreuhandmodelle ist es vielmehr, zur Klärung beizutragen, was man unter dem bisher noch unklaren Begriff der sicheren Verarbeitungsumgebungen verstehen kann und sollte.

Außerdem sollen hiermit die **Mechanismen** hervorgehoben werden, die beim Datenteilen die **Rechtsunsicherheit reduzieren**. Wie wichtig solche Mechanismen sind, sollte aus dem Vorstehenden deutlich geworden sein. Ein wesentlicher Hinderungsgrund, Daten zu teilen, sind die aktuell sehr hohen Compliance-Risiken, die das Teilen nicht lohnend erscheinen lassen. Daher wurde in den Ausführungen der verschiedenen Datentreuhandmodelle wiederholt empfohlen, wo der Datentreuhänder kraft besseren Wissens und besserer Kontrolle über diese Risiken auch die Compliance-Verantwortung übernehmen sollte. Auch wo eine solche Übernahme der Compliance-Verantwortung nur im Innenverhältnis zwischen Datengebenden und Datentreuhänder möglich ist – wie etwa im Datenschutzrecht, wo die Datengebenden immer auch selbst im Außenverhältnis haften – kann sie entscheidend für die Weitergabe der Daten sein. Noch wirksamer sind Mechanismen, die das Compliance-Risiko auch im Außenverhältnis reduzieren. Im Datenschutzrecht sind das vor allem solche aus Art. 40 bis 43 DSGVO, also Verhaltensrichtlinien und Zertifizierungsmechanismen. Diese können vor allem bei den folgenden Vorschriften zur Rechtssicherheit beitragen: Art. 24 Abs. 3 (Verantwortlichkeit des Controllers), 25 Abs. 3 (Datenschutz durch Technikgestaltung), 32. Abs. 3 (Sicherheit der Verarbeitung) sowie Art. 83 Abs. 2 lit. j (Geldbußen) DSGVO. Man denke aber auch an die Verhaltensrichtlinien im unlauteren Wettbewerbsrecht oder im Digital Services Act. Da diese Rechtsvorschriften, anders als Verstöße von Geschäftsgeheimnissen, nicht nur von einer Rechtsdurchsetzung des Verletzten abhängen, sondern objektiv von den Behörden durchgesetzt werden, sind solche das Compliance-Risiko reduzierenden Mechanismen wichtig (siehe zu den verschiedenen Compliance-Risiken im Detail bereits Technopolis Group et al., 2024b). Klarzustellen ist an dieser Stelle, welchen Akteuren solche Mechanismen zur Verfügung stehen sollten: An erster Stelle geht es darum, dass die Datengebenden und -nutzenden ihre Compliance-Risiken reduzieren können. Erst an zweiter Stelle geht es um den Datentreuhänder. Das sollte bei der Ausgestaltung dieser Mechanismen unbedingt beachtet werden. Bei den untersuchten Pilotprojekten gab es nur ein Projekt, das überhaupt die Entwicklung eines solchen Mechanismus vorgesehen hat, und auch dort wurde dieses für den Datentreuhänder

und nicht die Datengebenden ausgestaltet. Dies ist ein Punkt, der aktuell in der Praxis durchaus übersehen wird.

2.3.7 Schlussfolgerungen und Handlungsbedarf

Vor diesem Hintergrund zieht die Begleitforschung folgende Schlussfolgerungen und sieht entsprechenden Handlungsbedarf:

- Wesentliche Hindernisse für das Datenteilen sind eine sehr **hohe Rechtsunsicherheit** beim Teilen von Daten und daraus resultierende ungeklärte Compliance-Fragen.
- Die hier entwickelten Fallgruppen können als **Toolbox** dienen, um entsprechend der Intensität der jeweils vorliegenden Interessenkonflikte bzw. Compliance-Risiken das geeignetste Datentreuhandmodell zu identifizieren.
- Der DGA stellt mit seinen Anforderungen in Art. 12 insbesondere zur Neutralität eine wichtige Funktion bei der Bildung des erforderlichen Vertrauens für das Teilen von Daten heraus. Er könnte und sollte allerdings um weitere Regelungen ergänzt werden, die die zahlreichen Compliance-Fragen konkret klären. Hier sollte der Gesetzgeber in einer Überarbeitung des/r Gesetze/s vor allem klären, wie Datentreuhänder die Rechtsunsicherheit in Bezug auf die Einhaltung des Datenschutzrechts, des Schutzes von Geschäftsgeheimnissen, der IT-Sicherheit, des Wettbewerbsrechts etc. deutlich reduzieren können.

Um die rechtlichen Anforderungen beim Datenteilen nicht nur konzeptionell, sondern auch praktisch zu erfüllen, bedarf es geeigneter technischer und organisatorischer Lösungen. Das folgende Unterkapitel widmet sich daher den technischen Bausteinen, die Datentreuhänder einsetzen können, um diese Anforderungen wirksam zu adressieren.

2.4 Technische Anforderungen für den Aufbau von Datentreuhändern

Das Wichtigste zu technischen Anforderungen in Kürze:

- Eine geeignete technische Infrastruktur ist Voraussetzung für die praktische Umsetzung der rechtlichen Anforderungen. Sie muss dabei robust genug sein, um die Sicherheit und Integrität der Daten immer zu gewährleisten, aber auch flexibel genug, um verschiedene Datentreuhandmodelle und domänenspezifische Anforderungen unterstützen zu können.
- Drei **zentrale technische Anforderungen** stehen dabei im Fokus:
  - **Interoperabilität** ist die Voraussetzung für reibungslosen Datenaustausch. Besonders herausfordernd ist die Umsetzung in dezentralen oder hybriden Speicherarchitekturen, wofür Initiativen wie Gaia-X oder Technologien wie SOLID Lösungsansätze bieten könnten. Es besteht allerdings noch hoher Entwicklungs- und Standardisierungsbedarf, bevor Interoperabilität gewährleistet ist.
  - Nach dem Prinzip der **Datenminimierung** sollen nur notwendige Daten geteilt werden. Techniken zur Pseudonymisierung oder Anonymisierung von Daten helfen, Datenschutz zu gewährleisten. In der Praxis betrifft dies vor allem sensible Anwendungsdomänen wie etwa die Medizinforschung.
  - Die dritte zentrale Anforderung ist **Datensicherheit**. Besonders für sensible Daten gewinnen moderne Verschlüsselungstechnologien an Bedeutung, die datenschutzkonforme Analysen ermöglichen, ohne dass Rohdaten offengelegt werden müssen. Auch hier zeigen sich allerdings in der Praxis Herausforderungen hinsichtlich unzureichender Nutzungskontrolle, fehlender plattformübergreifender Standards und der komplexen Umsetzung von Autorisierungsprozessen.
- Technische Lösungen allein schaffen noch kein Vertrauen, sondern müssen **durch rechtliche und organisatorische Maßnahmen ergänzt** werden. Datentreuhänder können hier als Vermittler und Kontrollinstanz agieren, etwa durch technische Prüfungen der Datennutzung oder durch Bereitstellung sicherer Verarbeitungsumgebungen.
- Insbesondere die im vorherigen Unterkapitel eingeführte **Fallgruppe der geteilten Analyseergebnisse bietet großes Potenzial** für Skalierung und Datenschutz, erfordert aber noch erhebliche technische Weiterentwicklungen hinsichtlich praktischer Umsetzung, Performance und Usability.

Die technische Infrastruktur von Datentreuhändern bildet das fundamentale Gerüst, um den vertrauensvollen Austausch und die Nutzung von Daten zu ermöglichen und um den rechtlichen Anforderungen, wie im vorherigen Unterkapitel skizziert, zu genügen. Wie in Kapitel 2.1 dargelegt, muss diese Infrastruktur den Zugang zu qualitativ hochwertigen Daten garantieren und dabei sowohl den Datenschutz wahren als auch Interoperabilität gewährleisten.

2.4.1 Zentrale Anforderungen aus technischer Sicht

Aus technischer Sicht lassen sich zentrale Anforderungen an die technische Infrastruktur definieren. Zunächst bildet **Interoperabilität** die Grundlage für den Aufbau eines sicheren Datentreuhandmodells. Für alle Datentreuhandmodelle ist es entscheidend, geeignete Schnittstellen für die Datenübertragung zu etablieren, die einen reibungslosen Austausch von Daten und Informationen gewährleisten. Neben der technischen Eignung ist die **nutzerfreundliche Ausführung der Schnittstellen**, sodass Datengebende mit möglichst minimalem Aufwand Daten teilen und Datennutzende auf Daten ebenso mit möglichst geringem Aufwand zugreifen können, entscheidend für die Akzeptanz von Datentreuhändern. Dies gilt auch für die Fallgruppe der geteilten Analyseergebnisse, bei dem die Daten als

aufbereitete Erkenntnisse übertragen werden. Damit verbunden ist gleichzeitig die klare Definition von APIs und Datenmodellen, um Interoperabilität zu gewährleisten.

Eine weitere zentrale Anforderung betrifft den Bereich **Datensicherheit**. Die Vertrauenswürdigkeit spielt in allen Modellen eine grundlegende Rolle. In vielen Fällen bedeutet dies, dass die rechtlich formulierten Anforderungen bezüglich der Nutzungsbedingungen der zu teilenden oder zu nutzenden Daten auch technisch umgesetzt werden müssen. Obwohl derartige Anforderungen häufig durch rechtlich-organisatorische Maßnahmen erfüllt werden können, sollten die Nutzungsbedingungen, sofern möglich, auch auf technischer Ebene implementiert werden, um die Vertrauenswürdigkeit solcher Maßnahmen zu erhöhen. Dabei spielt eine ausgewogene Abwägung zwischen dem Wert der Daten und potenziellen Risiken eine zentrale Rolle.

Nicht zuletzt stellt die **Datenminimierung** eine weitere zentrale Anforderung dar. Grundsätzlich sollten nur jene Informationen offengelegt werden, die für den jeweiligen Anwendungsfall unabdingbar sind. Zudem wird in vielen Fällen unter Berücksichtigung datenschutzrechtlicher Vorgaben ausdrücklich gefordert, dass personenbezogene Daten nicht in ihrer unveränderten Originalform an Dritte weitergegeben werden dürfen. Um gleichzeitig den rechtlichen Anforderungen sowie der Nutzbarkeit der Daten gerecht zu werden, muss bei der technischen Umsetzung besonderes Augenmerk auf das Prinzip der Datenminimierung gelegt werden. So kann eine zu hohe Datenminimierung die Daten z. B. im medizinischen Kontext gegebenenfalls unbrauchbar machen.

2.4.2 Erweiterung der Datentreuhandmodelle um technische Bausteine

Im Rahmen der Begleitforschung wurde zur Verknüpfung der zentralen technischen Anforderungen mit den in Kapitel 2.2 eingeführten Datentreuhandmodellen ein **technischer Baukasten** entwickelt. Dieser Baukasten ermöglicht eine fundierte Entscheidung darüber, welche technischen Funktionen für ein spezifisches Datentreuhandmodell implementiert werden müssen und ob dabei auf allgemeine oder domänenspezifische Standards zurückgegriffen werden kann oder individuelle Lösungen entwickelt werden müssen.

Abbildung 6 visualisiert das **Konzept dieses Baukastens** in Form einer Matrix. Die Spalten repräsentieren die verschiedenen eingeführten Datentreuhandmodelle, während die Zeilen die technischen Kategorien darstellen. Der Bereich der Interoperabilität ist unterteilt in Datenbanksysteme, Datenübergabe/Schnittstellen sowie Metadaten und Datenformate. Der Bereich Datensicherheit untergliedert sich weiter in Authentifizierung, Autorisierung, Protokollierungsaspekte, Datenverschlüsselung und Zertifizierung, wobei Letztere die notwendigen Zertifikate für die Implementierung der Sicherheitsfunktionen umfasst. Aus technischer Sicht lassen sich die Modelle wie folgt differenzieren:

Abbildung 6 Erweiterung der Datentreuhandmodelle um technische Bausteine

		Fallgruppe 1: offene Daten		Fallgruppe 2: geteilte Rohdaten bei			Fallgruppe 3: geteilte Analyseergebnisse
		frei	mit Lizenz	Datennutzendem		2.3 + 2.4: Datengebendem/ 2.5: Datentreuhänder	
		DTM 1.1	DTM 1.2	DTM 2.1: Identitäts-kontrolle	DTM 2.2: Nutzungs-kontrolle	DTM 2.3 - 2.5	DTM 3.1 - 3.2
Interope-rabilität	Datenbanksystem	x	x	x	x	x	x
	Datenübergabe/Schnittstelle	x	x	x	x	(x)	x
	Metadaten und Datenformat	(x)	(x)	x	x	(x)	x
Datenmini-mierung	Datenminimierung	(x)	(x)	(x)	(x)	(x)	
Data Trust/ Sicherheit	Authentifizierung		x	x	x	x	x
	Autorisierung			(x)	(x)	x	x
	Protokollierungsaspekte			(x)	(x)	(x)	x
	Datenverschlüsselung	x	x	x	x	x	x
	Zertifizierung	x	x	x	x	x	x

x notwendig
(x) optional

allgemeine Standards
dömanenspezifische Standards
individuell

Quelle: Eigene Darstellung.

Die Matrix kennzeichnet mit einem „x" die für ein spezifisches Datentreuhandmodell essenziellen technischen Bausteine, während optionale Komponenten mit „(x)" markiert sind. Grün hervorgehobene Kategorien verfügen nach empirischer Erhebung der Begleitforschung über verschiedene allgemein standardisierte Konzepte, während blau markierte Bereiche auf domänenspezifische Standards hinweisen. Rot gekennzeichnete Felder signalisieren die Notwendigkeit individueller Entwicklungen. Eine detaillierte Ausarbeitung des Baukastens mit konkreten technischen Konzepten für die einzelnen Kategorien findet sich in Anhang B.

Im Folgenden werden der aktuelle Entwicklungsstand und die Erkenntnisse im Rahmen der Begleitforschung zu den drei zentralen Anforderungen – **Interoperabilität**, **Datenminimierung** und **Datensicherheit** – eingehend erläutert.

2.4.3 Interoperabilität

Die sichere **Speicherung und Verwaltung von Daten** bilden das Fundament jeder technischen Infrastruktur für Datentreuhänder. Die Art der Datenspeicherung beeinflusst maßgeblich sowohl die Architektur als auch die Funktionalität der Systeme. In der Fachliteratur kristallisieren sich **drei zentrale Ansätze** heraus:

Bei der **zentralen Datenspeicherung** werden Daten in einer zentralen Datenbank gesammelt und verwaltet. Datenanbieter laden ihre Daten entweder manuell – etwa über Webportale – oder automatisch – etwa durch Internet-of-Things-Geräte – in diese Datenbanken hoch. Konkrete Anwendungsbeispiele sind die Speicherung statistischer Daten wie Wildtierbeobachtungen oder dynamischer Daten wie Betriebsdaten autonomer Fahrzeuge. Zentrale Speicherarchitekturen bieten erhebliche Vorteile bei der Interoperabilität und Datenverwaltung, da alle Daten in einer standardisierten Struktur vorliegen. Diese Standardisierung erleichtert die Integration und Verarbeitung durch verschiedene Akteure. Allerdings birgt dieser Ansatz erhebliche Risiken im Hinblick auf Datensicherheit und Vertrauen, da ein zentraler Speicherort ein attraktives Ziel für Cyberangriffe darstellt.

Dezentrale Ansätze hingegen belassen die Daten auf den Systemen der Datengebenden und referenzieren die Daten in Katalogen, Portalen oder Marktplätzen. Vielfältig etabliert ist dabei der Zugriff über Web-Schnittstellen in Form von APIs. Diese ermöglichen nicht nur den Datenzugriff, sondern können gleichzeitig Standardisierung fördern. Dezentrale

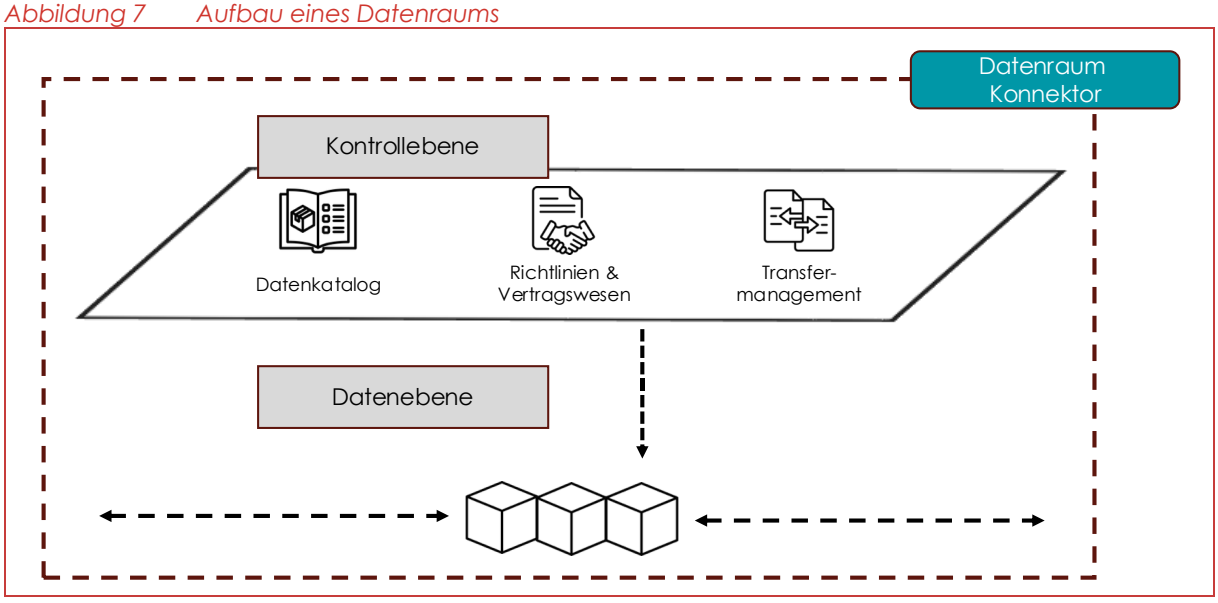
Speicherarchitekturen bieten mehrere Vorteile für Datensicherheit und Vertrauen: Die Datengebenden behalten die Kontrolle über ihre Daten, da der Zugriff kontrolliert werden kann und weil diese Systeme potenziell mehr Resilienz gegenüber Cyberangriffen bieten, da ein Angriff auf einen einzelnen Knoten das Gesamtsystem nicht unbedingt gefährdet. Die Interoperabilität kann jedoch bei dezentraler Speicherung herausfordernder sein.

Eine **hybride Speicherarchitektur** kombiniert zentrale und dezentrale Ansätze, um die Vorteile beider Ansätze zu nutzen. Hybride Speicherarchitekturen ermöglichen es, sensible Daten lokal zu halten, während weniger kritische Daten zentral gespeichert werden können. Dies bietet höhere Flexibilität und kann insbesondere in komplexen Datenökosystemen Vertrauen schaffen.

Für die Interoperabilität bei der Datenübergabe spielen **standardisierte Schnittstellen** eine entscheidende Rolle: Sie ermöglichen den einfachen und effizienten Zugriff auf Daten und reduzieren die Komplexität bei der Integration verschiedener Systeme.

Ein wichtiger technologischer Ansatz zur Umsetzung von Datentreuhändern mit standardisierten Schnittstellen funktioniert über **Datenräume.** Das in Abbildung 7 dargestellte Konzept der **Datenräume** ergänzt die dezentrale Datenhaltung um eine zusätzliche Kontrollebene. Die Kontrollebene beinhaltet softwaretechnische Bausteine zur Umsetzung von Richtlinien und Vertragswesen, das Transfermanagement sowie einen Datenkatalog. Ein standardisierter Datenraum-Konnektor implementiert neben dem eigentlichen Datentransfer Zugriffs-Policies und dient dabei als Vermittler zwischen Datengebenden und -nutzenden. So ermöglicht das Konzept einen kontrollierten und souveränen Datenaustausch zwischen verschiedenen Akteuren, der auf gemeinsamen Standards, Governance-Prinzipien und Vertrauensmechanismen basiert. Im Gegensatz zu zentralisierten Datenplattformen folgen **Datenräume** damit einem föderalen oder hybriden Ansatz, bei dem die Datengebenden die Kontrolle über ihre Daten behalten und selbst bestimmen können, wer unter welchen Bedingungen darauf zugreifen darf.

Abbildung 7 Aufbau eines Datenraums



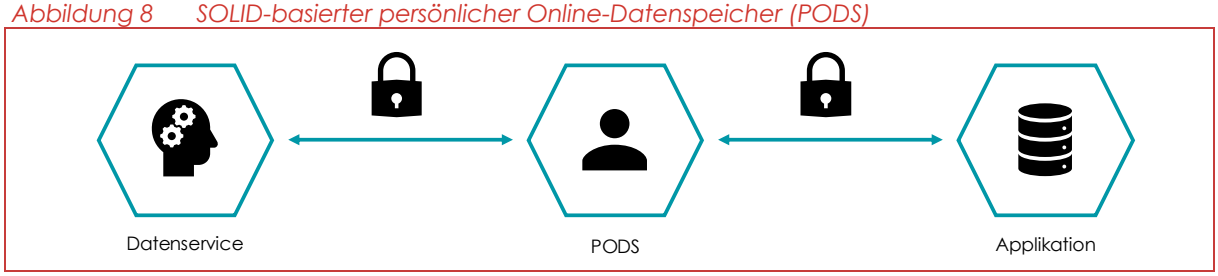
Quelle: Eigene Darstellung.

Europäische Initiativen wie **Gaia-X** haben wesentlich zur Definition von Standards und Referenzarchitekturen für **Datenräume** beigetragen. Gaia-X verfolgt dabei stärker einen „Top-down"-Ansatz, indem es übergreifende Standards, Referenzarchitekturen und Governance-Strukturen etabliert, die dann von verschiedenen Anbietern implementiert werden können.

Dies ermöglicht eine konsistente und interoperable Infrastruktur, die gleichzeitig europäische Werte wie Datensouveränität, Transparenz und Datenschutz respektiert.

Weitere **innovative Lösungsansätze** zur Datensouveränität wurden in verschiedenen Pilotprojekten entwickelt. Ein Projekt nutzte etwa **SOLID-Technologien** (Social Linked Data), um Datenhoheit und standardisierten Datenzugriff zu ermöglichen. Wie in der folgenden Abbildung dargestellt, erlaubt SOLID es Datennutzenden, ihre persönlichen Daten in dezentralen, selbst kontrollierten Datenspeichern (Pods) zu verwalten und selbst zu bestimmen, welche Anwendungen oder Personen auf welche ihrer Daten zugreifen dürfen.

Abbildung 8 SOLID-basierter persönlicher Online-Datenspeicher (PODS)



Quelle: Eigene Darstellung.

Für die Zukunft zeichnet sich eine potenzielle **Konvergenz von Bottom-up-Ansätzen wie SOLID und Top-down-Initiativen wie Gaia-X** ab. Diese Entwicklung könnte zu integrierten Lösungen führen, die sowohl die Datensouveränität der Einzelnen als auch die Interoperabilität auf Systemebene gewährleisten.

Unabhängig von den Austauschmechanismen ist die **Qualität der Daten** eine Grundvoraussetzung für ihre Nutzbarkeit. Datentreuhänder können eine zentrale Rolle bei der Verwaltung von Metadaten übernehmen, indem sie die Konsistenz, Vollständigkeit und Genauigkeit der Daten sicherstellen. Sie können zudem Persistent Identifiers (PIDs) verwenden, um die Eindeutigkeit und Nachvollziehbarkeit von Datensätzen zu gewährleisten (Grossman et al., 2016).

Ein zentraler Aspekt für die Entwicklung von Datentreuhandkonzepten ist die **Vertrauenswürdigkeit** der eingesetzten Technologien. Allerdings weisen Poikola et al. (2023) darauf hin, dass selbst die fortschrittlichste Technologie allein nicht ausreiche, um Vertrauen zu schaffen. Insbesondere spiele die Souveränität der Datengebenden eine Schlüsselrolle: Einerseits müsse ihre Selbstbestimmung beim Umgang mit Daten gewährleistet sein, sodass sie Kontrolle über Nutzung und Nutzungsumfang ihrer Daten behalten. Andererseits sei die technologische Souveränität entscheidend, die es Datengebenden ermöglicht, ihre Systeme weitgehend frei zu wählen und nur an definierten Schnittstellen, etwa Konnektoren, auf vorgegebene Komponenten zurückgreifen zu müssen. Ein gleichwertig wichtiger Faktor sei die User Experience (UX). Um das Vertrauen der Datennutzenden in den Datenaustausch zu gewinnen, müssen daher neben technologischen Lösungen auch rechtliche und serviceorientierte Designansätze berücksichtigt werden.

Basierend auf den Erkenntnissen der Begleitforschung zeigte sich, dass **Interoperabilitätsprobleme den größten Ressourceneinsatz** erfordern. Insbesondere werden dabei Aspekte wie Datenübergabe-Schnittstellen, Metadaten, Datenschemata und Datenmodelle als die Kategorien identifiziert, die besonders aufwändig sind. Dies weist darauf hin, dass trotz vieler domänenspezifischer Standards, die auch in den Pilotprojekten Anwendung fanden – wie etwa Standards des Bundessortenamts für Daten der Pflanzenzüchtung, das ISA-Modell für Experimentdokumente in den Biowissenschaften oder StanForD für die Daten von Forstmaschinen –, der Umsetzungsaufwand für Interoperabilität derzeit noch nicht zu vermeiden ist.

Eine andere **praktische Hürde beim Aufbau interoperabler Schnittstellen** stellen teilweise Maschinenhersteller dar. In (Industrial) Internet-of-Things-Kontexten werden Daten meist über die in Geräten (z. B. Forst- und Landwirtschaftsmaschinen) verbaute Sensorik gesammelt. Um reibungsloses Teilen von Daten zu ermöglichen, müssen diese mit dem Datentreuhänder verbunden sein. Welche Schnittstellen und Standards in den Geräten implementiert werden, obliegt jedoch den Herstellern. Um eine reibungslose Interoperabilität zu ermöglichen, kann es daher sinnvoll sein, Hersteller frühzeitig in den Aufbau von Datentreuhändern einzubinden. Dies wird in manchen der Pilotprojekte bereits angegangen.

2.4.4 Datenminimierung: Datenschutz und Datenverarbeitung

Datenminimierung ist ein zentraler Grundsatz moderner Dateninfrastrukturen, der durch die DSGVO für personenbezogene Daten vorgeschrieben wird. Ziel ist es, die Erhebung, Speicherung und Verarbeitung von Daten auf das notwendige Minimum zu beschränken, um Risiken für die Privatsphäre zu reduzieren.

Ein zentraler Baustein der Datenminimierung ist die **Pseudonymisierung und Anonymisierung** von Daten. Diese Methoden schützen die Identität von Einzelpersonen, indem sie Daten so transformieren, dass Rückschlüsse auf die ursprünglichen Personen erschwert oder unmöglich gemacht werden. Die technische Anonymisierung stellt allerdings eine anhaltende Herausforderung dar, da moderne Technologien wie KI die Gefahr potenzieller Rückschlüsse auf die Identität von Personen erhöhen. Dies unterstreicht die Notwendigkeit strenger technischer und rechtlicher Kontrollmechanismen. KI kann jedoch auch eingesetzt werden, um Daten zu anonymisieren. Hierzu werden neuronale Modelle trainiert, die die zu anonymisierenden Rohdaten zu höherwertigen Aussagen verarbeiten. Nur diese werden dann nach außen gegeben. Die KI-Modelle sind typischerweise als Services etwa in einem Datenraum integriert.

Die **Pseudonymisierung** kann durch zufallsbasierte Nummern oder Hashwerte erreicht werden und ist in der Praxis gut etabliert. **Anonymisierung** gestaltet sich hingegen weitaus komplexer, führt oft zu Datenverlust und es fehlen klare Definitionen, technische Standards oder regulatorische Leitlinien.

Verschiedene technische Lösungen, die eine Anonymisierung gewährleisten bzw. die anonyme Auswertung von Daten ermöglichen können, befinden sich heute in der Entwicklung. Teilweise werden sie auch bereits eingesetzt. Sie werden oft unter dem Oberbegriff **Privacy Enhancing Technologies (PETs)** diskutiert. Dazu gehören Techniken wie Differential Privacy, synthetische Daten, homomorphe Verschlüsselung und Secure Multi-Party Computation. Bei Differential Privacy wird eine gezielte Menge Rauschen in Datensätze eingefügt, sodass deren statistische Aussagekraft beibehalten wird, es aber unmöglich wird, Rückschlüsse auf einzelne Personen im Datensatz zu ziehen oder sie zu identifizieren. Auf Grundlage realer Datensätze lassen sich mit KI synthetische Daten generieren. Ähnlich wie bei Differential Privacy werden die wesentlichen Strukturen und statistischen Verhältnisse, die von Interesse sind, beibehalten, Rückschlüsse auf identifizierbare echte Personen (oder sonstige schutzwürdige Güter) aber unmöglich gemacht. Homomorphe Verschlüsselung und Secure Multi-Party Computation sind kryptographische Verfahren, mit denen Daten verschlüsselt bzw. verteilt ausgewertet werden können, ohne dass die Person oder Stelle, die die Auswertung durchführt, jemals die Daten im Klartext sieht. Als Verschlüsselungsverfahren werden die beiden Ansätze tiefer gehend im nächsten Abschnitt zur weiteren zentralen Anforderung Datensicherheit aufgegriffen.

Personal Information Management Systems (PIMS) sind hingegen Systeme, die Einzelpersonen mehr Kontrolle über ihre persönlichen Daten geben sollen. Mit PIMS können Einzelpersonen ihre persönlichen Daten in sicheren lokalen oder Online-Speichersystemen verwalten und sie nach Belieben weitergeben. So können Datengebende individuell ihre Zustimmung zur Datenverarbeitung erteilen und widerrufen.

In der **praktischen Anwendung** wird Datenminimierung jedoch nicht immer als notwendige technische Anforderung betrachtet. Erfahrungen aus den Pilotprojekten haben gezeigt, dass die Datenminimierung nur etwa 20 % der Anwendungsfälle betrifft. Dies ist darauf zurückzuführen, dass viele Pilotprojekte mit nicht-sensitiven Daten arbeiten. Für sensible Anwendungsfälle bleibt Datenminimierung jedoch essenziell und erfordert verstärkt Forschungsarbeit. Dies zeigte sich bei den Pilotprojekten z. B. im Bereich der Medizin, für Mobilitätsdaten aber auch bei Daten von Endnutzenden im Bereich der IT-Sicherheit.

Projekte mit Anonymisierungsbedarf haben auch Grenzen der technischen Anonymisierung aufgezeigt. Die Erfahrungen aus Pilotprojekten im Verkehrsbereich zeigen, dass die Anonymisierung individuell an den Nutzungszweck angepasst werden muss und eine Kombination aus automatisierten und manuellen Validierungsschritten erfordert. Da derzeit keine Standards zur Anonymisierung von Verkehrsdaten existieren, ist es wichtig, dass vertrauenswürdige Stellen wie Datentreuhänder als Datenverarbeiter fungieren und Compliance-Verantwortung übernehmen.

2.4.5 Datensicherheit

Die **Kontrolle des Datenzugriffs** wird durch zwei technische Bausteine geregelt: **Access Control (AC) und Identity Management (IDM).** Das IDM verwaltet die Identitäten und Berechtigungen der Akteure, während die AC-Komponente den Zugriff auf bestimmte Daten entsprechend den Berechtigungen regelt. Ein innovativer Ansatz ist das Konzept der Self-Sovereign Identity (SSI), das Nutzenden einer Technologie die vollständige Kontrolle über ihre digitalen Identitäten ermöglicht. Im Gegensatz zu konventionellen zentralen IDM-Systemen erlaubt SSI Personen, Organisationen und sogar Maschinen, ihre Identitätsnachweise selbstsouverän zu verwalten. Die Nutzenden (Holder) lassen sich hierfür verschiedene persönliche Attribute – sogenannte Claims – von autorisierten Stellen (Issuers) beglaubigen. Diese Attribute werden als kryptographisch signierte Nachweise (Verifiable Credentials) ausgestellt und können eigenständig verwaltet werden. Dieser Ansatz ergänzt besonders dezentrale und hybride Speicherarchitekturen optimal, da er die Prinzipien der Datensouveränität auf die Identitätsverwaltung überträgt.

Ergänzend dazu spielen **Policy-Enforcement-Komponenten (PEC)** eine wichtige Rolle, um sicherzustellen, dass die Datennutzung nur im vorgesehenen Rahmen erfolgt (Zrenner et al., 2019). Diese Systeme sind besonders relevant bei sensiblen Daten wie Gesundheitsdaten und tragen maßgeblich zur Datensouveränität bei. Das Konzept des „Trust Framework“ (Schinke et al., 2024) betont dabei die Kombination aus maschinen- und menschenlesbaren Verträgen, um sowohl technische als auch rechtliche Anforderungen zu erfüllen. Ergänzend dazu können Mechanismen wie Hash-basierte Integritätsprüfungen (Steinert et al., 2024) eingesetzt werden, um die Authentizität von Daten und zugehörigen Vertrauenslisten sicherzustellen.

Bei der **praktischen Umsetzung** von Datentreuhandmodellen zeigen sich in diesem Bereich mehrere technische Herausforderungen. Besonders problematisch ist die wirksame **Nutzungskontrolle** – häufig endet der Datenschutz bereits auf der Ebene der Identitätskontrolle, während die granulare Kontrolle der tatsächlichen Datenverwendung unzureichend implementiert wird. Standards wie die Open Digital Rights Language (ODRL) könnten theoretisch präzise Nutzungsbedingungen definieren, es fehlen jedoch plattformübergreifende Implementierungen.

In den Pilotprojekten wurde festgestellt, dass die Umsetzung von **Autorisierungs- und Authentifizierungsprozessen** mit besonders vielen Hindernissen verbunden ist. Ein wesentlicher Grund dafür besteht darin, dass plattformübergreifende Standards bislang nicht hinreichend etabliert sind. Dieser Mangel an plattformübergreifenden Standards erschwert die Entwicklung von Datentreuhandmodellen erheblich.

Die **Datenverschlüsselung** stellt ein fundamentales Element in der Sicherheitsarchitektur von Datentreuhändern dar. Besonders für die Fallgruppe der geteilten Analyseergebnisse

gewinnen innovative Verschlüsselungstechnologien wie die homomorphe Verschlüsselung zunehmend an Bedeutung. Diese Technologie ermöglicht es, Berechnungen auf verschlüsselten Daten durchzuführen, ohne diese entschlüsseln zu müssen, wodurch die Datensicherheit und Privatsphäre erheblich gestärkt werden. Traditionelle Verschlüsselungsverfahren basieren auf mathematischen Problemen, die für klassische Computer schwer zu lösen sind, aber mit Quantencomputern und speziellen Algorithmen gebrochen werden könnten. So gibt es einige Standardisierungsaktivitäten im Bereich quantensicherer Kryptografie. Quantensichere Verfahren nutzen alternative mathematische Probleme. Dazu gehören etwa codebasierte, gitterbasierte und multivariate Kryptografie (Post-Quantum-Kryptographie). Die Quantenschlüsselverteilung (QKD) ermöglicht zusätzlich eine abhörsichere Übertragung durch quantenmechanische Prinzipien, bei der jeder Abhörversuch den Quantenzustand messbar verändert.

Die **homomorphe Verschlüsselung** erlaubt es, mathematische Operationen auf verschlüsselten Daten auszuführen, wobei das Ergebnis – nach der Entschlüsselung – identisch ist mit dem Resultat, das bei denselben Operationen auf unverschlüsselten Daten entstehen würde. Dies eröffnet völlig neue Möglichkeiten für datenschutzkonforme Analysen, da sensitive Rohdaten niemals offengelegt werden müssen, während gleichzeitig wertvolle Erkenntnisse gewonnen werden können.

Aktuelle Forschungs- und Entwicklungsansätze zielen darauf ab, die Effizienz homomorpher Verschlüsselungsverfahren zu verbessern und ihre praktische Anwendbarkeit zu erhöhen. Insbesondere in Bereichen wie der medizinischen Forschung, wo hochsensible Patientendaten analysiert werden müssen, oder in der Finanzbranche, wo vertrauliche Finanzdaten verarbeitet werden, zeigt die homomorphe Verschlüsselung großes Potenzial. Für Datentreuhänder, die nach den Modellen der geteilten Analyseergebnisse arbeiten, eröffnet diese Technologie die Möglichkeit, Datenanalysen ohne direkten Zugriff auf die Rohdaten durchzuführen. Die Datengebenden können ihre Daten verschlüsselt bereitstellen, während der Datentreuhänder oder autorisierte Datennutzende Analysealgorithmen auf den verschlüsselten Daten ausführen und nur die resultierenden Erkenntnisse erhalten, ohne jemals Zugang zu den unverschlüsselten Originaldaten zu haben. Dies stärkt das Vertrauen in Datentreuhandmodelle erheblich und kann dazu beitragen, Akzeptanzhürden für das Datenteilen in sensiblen Bereichen zu überwinden.

Eine verwandte kryptographische Technik ist **Secure Multi-Party Computation**. Diese Technik erlaubt es mehreren Parteien, eine gemeinsame Auswertung ihrer Datensätze vorzunehmen, ohne diese Datensätze miteinander oder mit Dritten teilen zu müssen. Ein einfaches Beispiel sind zwei Millionäre, die wissen möchten, wer von ihnen reicher ist, ohne irgendwelche weiteren Informationen über ihr Vermögen offenzulegen. Multi-Party Computation wird heute ebenfalls bereits vereinzelt in der medizinischen Forschung, in der Finanzbranche oder in industriellen Kontexten sowie im öffentlichen Sektor eingesetzt. Wie bei homomorpher Verschlüsselung besteht aber noch erheblicher Entwicklungsbedarf, um Performanz und Usability zu verbessern.

Auch die **Distributed-Ledger-Technologie** kann als ergänzende Komponente in einem umfassenden technischen Baukasten für Datentreuhänder betrachtet werden, die bei der Vertrauensbildung, Transparenz und automatisierten Durchsetzung von Datennutzungsregeln Dienste leisten kann. So kann die Technologie als Kontrollschicht dienen. Während die eigentlichen Daten in konventionellen Systemen gespeichert werden, werden nur Metadaten, Zugriffsrechte und Nutzungsprotokolle mittels Distributed-Ledger-Technologie gespeichert.

2.4.6 Schlussfolgerungen und Handlungsbedarf

Zusammenfassend erfordert der erfolgreiche Aufbau von Datentreuhändern eine ausgewogene Kombination aus technischen Lösungen für Datenschutz und -sicherheit, rechtlichen Rahmenbedingungen und vertrauensbildenden organisatorischen Maßnahmen.

Die Erfahrungen aus den Pilotprojekten unterstreichen, dass technische Lösungen allein nicht ausreichen, um Vertrauen zu schaffen. Wie ein Projekt in der Domäne der Pflanzenzucht betonte, entsteht Vertrauen hauptsächlich auf sozialer Ebene, und **technische Lösungen müssen durch rechtliche und organisatorische Maßnahmen ergänzt werden**. Eine mögliche Kombination besteht darin, dass Datennutzende die Datenverwendung gemäß organisatorischen Verpflichtungen protokollieren und auf Anfrage den Datentreuhändern zur Verfügung stellen, die dann eine technische Prüfung auf Einhaltung der Datennutzungsvereinbarung vornehmen können.

Generell muss die technische Infrastruktur immer flexibel genug sein, um verschiedene Datentreuhandmodelle zu unterstützen und domänenspezifische Anforderungen zu erfüllen, gleichzeitig aber robust genug, um die Sicherheit und Integrität der geteilten Daten zu gewährleisten.

Die noch fehlende **Interoperabilität** zwischen unterschiedlichen Plattformen, praktische Herausforderungen bei interoperablen Schnittstellen als auch weitere individuelle Maßnahmen gerade bei der Anonymisierung schränken die technische Skalierbarkeit noch stark ein. Hier müssen technische Konzepte eng verknüpft mit den rechtlichen Rahmenbedingungen, möglichen Betriebsmodellen und Standardisierungsansätzen noch weiterentwickelt werden. Ein gerade für die Skalierung interessantes Konzept ist insbesondere die Fallgruppe der geteilten Analyseergebnisse, für das ebenfalls noch weiterer Forschungsbedarf in der Umsetzung, Performance und Usability besteht. Im folgenden Unterkapitel wird erörtert, bei welchen technischen und anderen Bausteinen für Datentreuhänder Standardisierungs- und Zertifizierungsbestrebungen zu einer erfolgreichen Etablierung von Datentreuhändern führen könnten.

2.5 Rolle von Standards und Zertifizierung bei der Etablierung von Datentreuhändern

Das Wichtigste zu Standards und Zertifizierung in Kürze:

- Die Entwicklung und Anwendung technischer, rechtlicher und organisatorischer Standards ist zentral für den Aufbau vertrauenswürdiger und interoperabler Datentreuhänder. Während verschiedene europäische Initiativen formale Standards vorantreiben, bleibt deren praktische Etablierung in vielen Domänen noch aus.
- Datentreuhänder können durch die Harmonisierung und Aufbereitung heterogener Daten einen entscheidenden Mehrwert leisten, insbesondere in der Fallgruppe der geteilten Analyseergebnisse. Diese Datenveredelung kann helfen, die Nutzbarkeit von Daten vorübergehend deutlich zu erhöhen, bis geeignete Standards etabliert sind.
- Zertifizierungen können mittelfristig eine wichtige Rolle für Vertrauen und Skalierung spielen, allerdings fehlen aktuell spezifische Zertifikate für Datentreuhänder. Der DGA könnte mit der verpflichtenden Registrierung von Datenvermittlungsdiensten einen ersten vertrauensbildenden Mechanismus bieten.
- Vertrauen entsteht derzeit weniger durch formale Standards, sondern vor allem durch partizipative Aushandlungsprozesse zwischen den beteiligten Akteuren. Initiativen wie z. B. Gaia-X, die IDSA oder SOLID bieten hierfür geeignete Strukturen, werden aber bislang nur begrenzt genutzt.

2.5.1 Rolle von Standards

Neben der rechtlichen und technischen Ausgestaltung spielen technische, rechtliche und organisatorische Standards eine Rolle bei der erfolgreichen Etablierung von Datentreuhändern. Seit Jahren existieren verschiedene Standards, die für Datentreuhänder

relevant sind. Dazu zählen **Standards mit Querschnittscharakter** wie die für Datensicherheit (z. B. ISO 27001) sowie spezialisiertere Standards wie die für Datenrepositorien (ISO 16363), Digitale Archive (DIN 31644) oder Datenherkunft (ISO/IEC AWI 5181). Auch für Biobanken gibt es einen ersten Standard (ISO 20387). Über diese hinaus wurden ab 2024 weitere formale Standardisierungsaktivitäten im Bereich Daten gestartet, die speziell für Datentreuhänder relevant werden. Zum einen wurde im Herbst 2024 von CEN/CENELEC das *Joint Technical Committee 25 on Data Management, Dataspaces, Cloud and Edge* gegründet, das einer entsprechenden Fokusgruppe hervorgegangen ist. Zum anderen hat ETSI im April 2025 ein *Technical Committee Data* ins Leben gerufen. Beide technischen Komitees haben zunächst den Hauptzweck, Standards zu entwickeln, die von einem Standardisation Request der Europäischen Kommission gefordert sind, welcher sich aus Art. 38 Data Act ableitet. Hier gilt es unter anderem das im Jahr 2024 veröffentlichte *CEN Workshop Agreement (CWA) on Trusted data transaction* zu einem harmonisierten europäischen Standard weiterzuentwickeln, der dann für die Implementierung des Data Acts referenziert werden kann. Der Hauptfokus des CWAs liegt darin, Terminologie, Konzepte und Mechanismen im Bereich des Datenaustauschs mit Schwerpunkt auf vertrauenswürdigen Datentransaktionen bereitzustellen. Diese generischen Elemente können bei der Entwicklung von weiteren Standards zur Unterstützung vertrauenswürdiger Datentransaktionen zwischen verschiedenen interessierten Parteien oder Stakeholdern verwendet werden. Daher können die Elemente dieses Basisstandards ein grundlegendes Verständnis bilden, auf dem vertrauenswürdige Datentransaktionen unabhängig von architektonischen Entscheidungen oder technischen Implementierungen basieren können.

Parallel zu diesen von der Europäischen Kommission forcierten formalen Standardisierungsaktivitäten gibt es auch erste, meist **bottom-up getriebene, informelle Aktivitäten zur Etablierung von De-facto-Standards** durch die jeweiligen Fach-Communitys, teilweise unter Mitwirkung von Datentreuhändern selbst. Ein Pilotprojekt hat etwa zur Entwicklung von Standards für die Erfassung von schlafmedizinischen Daten und ihrer Aufnahme in den FHIR-Standard beigetragen. Ein anderes Pilotprojekt hat Standardisierungsbemühungen für die Aufzeichnung von Pflanzenzüchtungsdaten weiter vorangetrieben.

Trotz dieser angelaufenen Aktivitäten ist aktuell noch festzustellen, dass sich in vielen Domänen die **Entwicklung von Datenstandards und vor allem ihre Anwendung noch in den Anfängen** befinden. In Folge sind die formalen Ontologien, Einheiten und Formate, mit denen Daten erfasst werden, mitunter extrem heterogen. Diese Heterogenität wiederum bedeutet, dass der Aufwand, um Daten nutzbar zu machen, schnell sehr hoch wird, wenn keine ausreichenden Datenstandards vorliegen und angewandt werden. Auch prinzipiell attraktive Use Cases rentieren sich unter diesen Umständen oft nicht mehr.

Gleichzeitig scheint die bloße Existenz von Datenstandards noch nicht alle einschlägigen Hindernisse zu lösen, da trotzdem noch besonders viele Ressourcen in die Entwicklung von Datenschemata, Metadaten und Datenmodelle zu investieren sind. Die Probleme werden in Zukunft weniger in der inzwischen angelaufenen Entwicklung der Standards liegen, sondern vor allem in ihrer **breiten Anwendung**. Denn nur wenn Standards auch genutzt werden, reduzieren sie Heterogenität und damit Aufwand. Trotz aller Standards und ihrer Anwendung wird in vielen Domänen eine gewisse Datenheterogenität wohl bestehen bleiben. Grund dafür ist, dass die Anzahl der verschiedenen Datenpunkte, die durch den immer vielfältigeren Einsatz von Sensoren in modernen technischen Systemen erzeugt wird, beständig steigen wird. Insofern Sensoren und ihre Einsatzfelder in einer Marktwirtschaft immer bottom-up entwickelt werden, ist zu erwarten, dass so beständig neue Datenheterogenität entstehen und die Datenstandardisierung regelmäßig hinterherhinken wird.

Die umfassende Weiterentwicklung und Anwendung von Datenstandards bleibt selbstredend Kern jeder Lösung für das sich aus mangelnder Standardisierung ergebende Aufwandsproblem. Hiermit ist jedoch bestenfalls mittelfristig zu rechnen. Eine direktere Lösung

für das Problem Datenheterogenität kann daher sein, dass der Datentreuhänder die Harmonisierung und gegebenenfalls praxisgerechte Aufbereitung und Aggregierung von Daten teilweise selbst übernimmt. Eine derartige Datenveredelung, wie sie in der Fallgruppe der geteilten Analyseergebnisse der eingeführten Datentreuhandmodelle in Kapitel 2.3.2 vorgestellt wurde, kann einen kritischen Mehrwert darstellen, den Datentreuhänder erbringen können und je nach Sektor mitunter müssen, wenn Daten in größerem Umfang geteilt und genutzt werden sollen.

Fehlende Datenstandardisierung stellt ein Problem vor allem für Datennutzende dar, da der zusätzliche Aufwand tendenziell bei ihnen anfällt. **Fehlende technische Schnittstellen**, um Daten in den Datentreuhänder zu speisen oder direkt an Datennutzende weiterzugeben, ist in erster Linie ein Problem für die Datengebenden, weil es ihren Aufwand beim Datenteilen erhöht. Inwiefern Schnittstellen vorhanden sind, scheint sowohl zwischen Domänen als auch Sektoren zu variieren. Hier kann eventuell ein weiterer Standardisation Request der Europäischen Kommission abgeleitet aus Art. 35 Data Act zur *Interoperabilität von Datenverarbeitungsdiensten* Abhilfe schaffen.

In den Pilotprojekten spielen **spezifische Standards** für unterschiedliche Dimensionen eine Rolle. Auf der organisatorischen Ebene bietet die Credential-and-Access-Management(ICAM)-Spezifikation von Gaia-X ein Verifizierungsverfahren aus technischer Sicht, um föderierte Datensysteme aufzubauen. Kontrolltechnisch steht die Open Digital Rights Language (ODRL) zur Beschreibung der Nutzungsbedingungen zur Verfügung sowie das Dataspace Protocol der IDSA, das die Datenkataloge, Metadaten und Nutzungsrichtlinien verbindet, um plattformübergreifenden Datenaustausch zu ermöglichen. Implementierungsspezifisch stehen verschiedene Verschlüsselungsverfahren zur Verfügung, die technisch gut ausgereift und entsprechend verbreitet sind, sodass es hier wenige Unsicherheiten gibt. Im medizinischen Bereich wird mit dem schon genannten FHIR ein etablierter und akzeptierter Standard für den interoperablen Datenaustauch erfolgreich eingesetzt. Weitere domänenspezifische Standards sind STanForD2010 in der Forstwirtschaft und das ISA Abstract Model im Bereich der Biologie, das SOLID-Protocol wird für dezentralisierte Web-basierte Datenservices eingesetzt.

Die **Gaia-X-Initiative** wird in der gesichteten Datentreuhänder-Literatur noch wenig besprochen (aber siehe die Aufsätze in Otto et al., 2022). Indem Gaia-X eine Referenzarchitektur und Dienste bereitstellt, kann sie den Aufbau von Datentreuhändern unterstützen. Gleiches gilt auch für die IDSA. Zudem bieten Gaia-X wie IDSA einen Raum, um die Aushandlungsprozesse, die für den Aufbau von Datentreuhändern essenziell sind, zu forcieren. Als föderierte Struktur kann Gaia-X den Zusammenschluss und die Interoperabilität zwischen verschiedenen sich etablierenden Datentreuhändern ermöglichen. Die Nutzung der Initiative, insbesondere die sektorübergreifende, ist allerdings bislang noch zurückhaltend.

2.5.2 Rolle von Zertifizierungen

Auf Standards können **Zertifizierungen** aufsetzen. Martin & Pasquale (2019) nennen sieben Dimensionen eines Datentreuhänders, die zertifiziert werden sollten: seine Governance, Finanzierung, Datenzugangsregeln, Datensicherheit, Ethik und Nachhaltigkeit sowie Datenqualität. Bislang gibt es jedoch keine Institutionen, die sämtliche dieser Dimensionen zertifizieren, und auch keine speziell auf Datentreuhänder abzielende Zertifizierungen. Mittelfristig dürfte die Zertifizierung eine wichtige Rolle für die Skalierung von Datentreuhändern und ihre Akzeptanz insbesondere auf Seiten von Datennutzenden spielen. Hier sind vor allem der Bedarf von Standards und Gütesiegeln für Daten, ihre Aufbereitung und Kuratierung sowie Metadaten und Provenance zu nennen (RfII, 2020; Stalla-Bourdillon, 2021; Gal & Rubinfeld, 2019). Ist die Qualität von Daten nicht belastbar attestiert oder fehlen Metadaten und Kontextinformationen, können sie oft nur begrenzt genutzt werden. Fehlende Daten-, Metadaten- und Kuratierungsstandards verkomplizieren zudem die Zusammenführung verschiedener Datensets erheblich (Stalla-Bourdillon, 2021; Gal & Rubinfeld, 2019).

Inwiefern Zertifizierungen für die **Akzeptanz von Datentreuhändern seitens der Datengebenden** zum jetzigen Zeitpunkt eine wichtige Rolle spielen können, ist jedoch weniger klar. Datentreuhänder sind eine sehr neue Institution, deren Aufbau regelmäßig komplizierte fallspezifische Fragen aufwirft. Ihr Aufbau braucht daher regelmäßig einen deliberativen Prozess mit sehr umfangreichen Abstimmungen und Verhandlungen unter den beteiligten Akteuren. So werden gemeinsame Verständnisse, Zielsetzungen, Akzeptanz und Vertrauen geschaffen. Da einschlägige Standards und darauf aufbauende Zertifizierungen selbst erst noch erarbeitet und umgesetzt werden müssen, ist nicht davon auszugehen, dass sie kurzfristig und quasi automatisch Akzeptanz schaffen werden. Zum jetzigen Zeitpunkt dürfte eher die **gemeinsame Erarbeitung von Standards und Zertifizierungen durch Akteure** akzeptanzstiftend wirken, wobei der akzeptanz- und vertrauensgenerierende Moment vorerst mehr im Weg zum Standard als in dessen Umsetzung bzw. Zertifizierung selbst liegen dürfte.

Spezifische **Datentreuhänder-Zertifizierungen** werden von den Pilotprojekten sowie externen Expertinnen und Experten für wünschenswert gehalten, existieren aber weiterhin nicht. Grundsätzlich setzen Zertifizierungen die Entwicklung von Standards voraus. Der DGA könnte aber mittelfristig teilweise als Substitut fungieren, insofern Datentreuhänder, die unter die Kategorie des im DGA definierten Datenvermittlungsdienstes fallen, gezwungen sind, sich als solchen bei definierten staatlichen Stellen registrieren zu lassen. Die Anerkennung erfordert den Nachweis, dass die verschiedenen Anforderungen an Datenvermittlungsdienste erbracht werden. Damit kann die Registrierung als anerkannter Datenvermittlungsdienst zumindest mittelfristig als vertrauensstiftende Marke fungieren. Bislang hat sich keines der Pilotprojekte auf Basis von Standards zertifizieren lassen, sondern lediglich an bestehenden Standards orientiert.

2.5.3 Schlussfolgerungen und Handlungsbedarf

Die aktuell **unzureichende Verfügbarkeit allgemein akzeptierter Standards** stellt eine Hürde für die weitere Entwicklung der einzelnen Datentreuhänder, aber auch für eine stärkere Interoperabilität zwischen Datentreuhändern dar. Als vergleichsweise wichtige Entwickler standardisierter Komponenten könnten z. B. **Gaia-X** und die **IDSA** die Entwicklung zu stärkerer Interoperabilität unterstützen, werden aber von den Pilotprojekten nur bedingt wahrgenommen.

Der Aufbau von Datentreuhändern und Ökosystemen, in denen Daten intensiv geteilt werden, sowie die Entwicklung und Etablierung von Standards erfordern relativ viel Zeit, Aufwand und einen intensiven Einbezug der Sektoren- und Domänen-Communitys. Die Entwicklung, breite Etablierung und Anwendung von Datenstandards und Datentreuhänder-Standards ist kritisch für den Aufbau von Datentreuhändern und für die Ermöglichung intensiven Datenteilens. Standards sind aber öffentliche Güter und werden daher von privaten Akteuren im Markt eher in ungenügendem Maße entwickelt und bereitgestellt. Damit sind die aus dem Data Act abgeleiteten Standardisation Requests der Europäischen Kommission positiv zu bewerten, weil sie einen **öffentlich finanzierten Anschub von Standardisierungsaktivitäten** darstellen. Gleichzeitig muss die inhaltliche Ausarbeitung der Standards fest in der Hand der Domänenakteure sein.

Um jedoch nicht nur technische und rechtliche Grundlagen zu schaffen, sondern Datentreuhänder auch langfristig tragfähig zu betreiben, rückt im nächsten Unterkapitel die Frage nach geeigneten Betriebs- und Geschäftsmodellen in den Fokus. Denn ohne wirtschaftlich nachhaltige Strukturen lassen sich Standards und Infrastrukturen kaum dauerhaft etablieren.

2.6 Tragfähige Betriebsmodelle für Datentreuhänder

Das Wichtigste zu Betriebsmodellen in Kürze:
• Ein tragfähiges Betriebsmodell ist eine grundsätzliche Voraussetzung für die langfristige Etablierung von Datentreuhändern. **Unklare Anreize für Betreiber**, **fehlende Finanzierungsperspektiven** und **Rechtsunsicherheit** bremsen derzeit aber viele Initiativen – auch über die BMFTR-geförderten Pilotprojekte hinaus – aus. • **Vertrauen** entsteht nicht allein durch die Wahl einer bestimmten Rechtsform, sondern durch glaubwürdige Neutralität, transparente Governance und die Fähigkeit, langfristige Verlässlichkeit zu garantieren. • Bei der **Finanzierung** präferieren viele der Pilotprojekte Abonnementmodelle gegenüber Alternativen wie transaktionsbasierten Ansätzen, haben aber in der Praxis Schwierigkeiten, diese umzusetzen. Die Bepreisung von Daten bleibt eine zentrale Herausforderung, da etablierte Marktpreise und Bewertungsmechanismen fehlen. • Das größte Potenzial für wirtschaftliche Tragfähigkeit bietet die **Fallgruppe der geteilten Analyseergebnisse**. Hier lassen sich mit geringen Grenzkosten datenbasierte Mehrwertdienste für viele Anwendungsfälle bereitstellen.

Die zögerlichen Entwicklungen bei der Etablierung von Datentreuhändern sind einerseits auf unklare Anreize für deren Betrieb zurückzuführen. Zudem herrscht eine anhaltende Unsicherheit darüber, welche Betriebsmodelle sich langfristig als tragfähig erweisen, sowohl in Bezug auf die Trägerschaft und Organisationsform als auch die langfristige Finanzierung. Dieses Unterkapitel beleuchtet daher verschiedene Möglichkeiten des Betriebs und der Finanzierung von Datentreuhändern.

2.6.1 Anreize für den Betrieb eines Datentreuhänders

Wie bereits angeführt (siehe Kapitel 2.1), steigt der Wert von Daten, wenn sie in Datenräumen mit einer Vielzahl unterschiedlichster Akteure geteilt und für neue Anwendungsfälle nutzbar gemacht werden. Während der gesellschaftliche, wirtschaftliche und politische Nutzen von Datentreuhändern zur Etablierung von Datenräumen zunehmend anerkannt wird, bleibt auf operativer Ebene vielfach offen, **warum eine Organisation den Aufwand und die Verantwortung des Datentreuhandbetriebs auf sich nehmen sollte**. Die empirischen Erhebungen der Begleitforschung zeigen, dass vor allem Organisationen, die selbst bereits Teil eines spezifischen Datenraums oder einer Domäne sind, den Betrieb eines Datentreuhänders forcieren, um hierdurch das Teilen von Daten zu erleichtern. Ziel ist hier also häufig nicht primär eine direkte Monetarisierung einzelner Interaktionen, sondern die Ermöglichung neuer datenbasierter Anwendungsfälle oder Effizienzgewinne, die ihnen selbst und anderen Akteuren im Datenraum zugutekommen. Vielfach besteht der Anreiz hier in der gemeinsamen Nutzung von Daten für Forschungs- oder gemeinwohlorientierte Sozialprojekte (z. B. Förderung der digitalen Souveränität, faire Teilhabe an Datenwertschöpfung). Auf der anderen Seite erhoffen sich aber Unternehmen durch den Betrieb eines Datentreuhänders auch die Entwicklung eines nachhaltigen Geschäftsmodells, etwa durch Gebühren für Datendienstleistungen.

Die Vielfalt potenzieller Anreize für den Betrieb eines Datentreuhänders spiegelt sich auch in den unterschiedlichen Anforderungen an seine Finanzierung und Trägerschaft wider. Denn je nachdem, welche Motivation im Vordergrund steht – seien es domänenspezifische Eigeninteressen, wirtschaftlicher Gewinn oder gemeinwohlorientiertes Handeln – unterscheiden sich die Erwartungen der beteiligten Datengebenden und -nutzenden an das geeignete Betriebsmodell erheblich.

2.6.2 *Organisatorische Aufstellung*

Mit Blick auf die Trägerschaft sind grundsätzlich drei verschiedene Modelle denkbar: Von *privaten Akteuren* betriebene Datentreuhänder können entweder gewinnorientiert **(For-Profit-Modell)** oder ohne Gewinnerzielungsabsicht **(Non-Profit-Modell)** agieren; in einem Modell ***öffentlicher Trägerschaft***, in staatlichen Institutionen oder Einrichtungen der Wohlfahrt können die Kosten und Investitionen durch staatliche Förderung und Subventionen getragen werden, d. h. über eine Umlegung auf steuerzahlende Personen oder Organisationen (Lipovetskaja et al., 2024; Stachon et al., 2023).

Diese Modelle lassen sich eng mit den jeweiligen Anreizen für den Betrieb und mit der Ausgestaltung der Governance verknüpfen, die sich in der Landschaft bestehender Datentreuhänder herausgebildet haben (Open Data Institute, 2019; Blankertz et al., 2020; Element AI & Nesta, 2019): In ***Unternehmensmodellen*** werden Dienste immer von privaten Akteuren und mit Gewinnerzielungsabsicht angeboten. Unternehmensmodelle sind ideal, wenn eine hohe Agilität und eine schnelle Anpassung an technologische Veränderungen und Markterfordernisse notwendig sind. Ein weiteres eingebrachtes Argument zugunsten von Unternehmensmodellen ist die Möglichkeit, Einnahmen gezielt zur Weiterentwicklung und Qualitätssicherung der Infrastruktur reinvestieren zu können. Allerdings können die hohen Anfangsinvestitionen und rechtliche Unsicherheiten eine Herausforderung darstellen. ***Mitgliedsorientierte Modelle*** beruhen auf einer Trägerschaft durch Verbände, Vereine oder genossenschaftlich organisierte Zusammenschlüsse. Auch sie sind über private Akteure organisiert, können aber sowohl profit- als auch nicht profitorientiert agieren. Aufgrund des hohen Koordinationsaufwands eignen sich solche Modelle insbesondere für bereits etablierte Netzwerke mit einem klar definierten gemeinsamen Interesse, etwa in domänenspezifischen Datenräumen. ***Institutionelle Modelle*** sind etwa an einer Behörde oder Hochschule angesiedelt und operieren in der Regel in staatlicher Trägerschaft oder unter staatlicher Aufsicht (Gebühren, Steuern) ohne Gewinnerzielungsabsicht. Sie erscheinen aus Sicht der Begleitforschung besonders dann sinnvoll, wenn eine starke öffentliche Unterstützung erforderlich oder ein staatliches Eingreifen sogar wünschenswert ist, etwa in Märkten mit geringer Wettbewerbsintensität, hoher Marktmacht einzelner Akteure oder wo gemeinwohlorientierte Ziele im Vordergrund stehen.

Aktuelle Diskussionen unterstreichen die **Identität des betreibenden Akteurs als kritischen Hebel für Vertrauen und Akzeptanz**. Prinzipiell muss der Betreiber als neutraler und verlässlicher Vermittler wahrgenommen werden, der nicht im Verdacht steht, eigene Interessen über die der Datengebenden und -nutzenden zu stellen. Dies schließt allerdings nicht zwingend gewinnorientierte Akteure aus. Zwar zeigt sich in den empirischen Erhebungen, insbesondere in hochsensiblen Domänen wie dem Gesundheitsbereich, eine ausgeprägte Präferenz für öffentliche Stellen, Forschungseinrichtungen oder gemeinwohlorientierte Vereine als Betreiber, doch werden auch privatwirtschaftliche Firmen prinzipiell als geeignete Träger bewertet – vorausgesetzt, das Geschäftsmodell ist so ausgestaltet, dass keine Nutzung der geteilten Daten und sonstigen Informationen erfolgt, die die Datengebenden und -nutzenden negativ tangieren würde. Neben der Transparenz über Zweckbindung und Datennutzung scheint die **Reputation** und wirtschaftliche Tragfähigkeit des Betreibers entscheidend: So wurde betont, dass Vertrauen auch davon abhängt, ob ein Betreiber glaubhaft versichern kann, langfristig am Markt zu bestehen, sodass geteilte Daten bei ihm auch langfristig sicher aufgehoben wären. Ein öffentliches Institut oder ein etabliertes Unternehmen könne diese langfristige Verlässlichkeit eher verkörpern als ein junges Start-Up.

Ein weiterer Ansatz, um Vertrauen aufzubauen, sind **strategische Partnerschaften** mit etablierten Akteuren mit hohem Standing in der jeweiligen Branche oder Domäne. Beispiele für solche Partner sind z. B. Verbände, große und bekannte Firmen oder in manchen Fällen auch Staatsbetriebe. Datentreuhänder können so in einem gewissen Maß von der **Reputation anderer Organisationen profitieren** und signalisieren ihre eigene Vertrauens- und Glaubwürdigkeit. Die Partner können auch als Multiplikatoren dienen, um Datengebende und

-nutzende zu rekrutieren. Schließlich können Datentreuhänder auch **Repräsentanten von Datengebenden und -nutzenden** in den Aufsichtsrat oder Vorstand des Datentreuhänders aufnehmen oder sie als Miteigentümer beteiligen.

Diese Erwägungen machen deutlich, dass Vertrauen in Datentreuhänder weniger durch deren Rechtsform oder das Gewinnmotiv allein bedingt ist, sondern dass vielmehr strukturelle Absicherungen gegen Interessenkonflikte für deren langfristige Glaubwürdigkeit entscheidend sind. Die Betreiberidentität ist damit ein zentrales Gestaltungselement zur Schaffung von Legitimität.

2.6.3 Bepreisungsansätze

Unabhängig davon, ob ein Datentreuhänder for-profit oder non-profit betrieben wird und welche Leistungen er anbietet, ist sein laufender Betrieb mit Kosten verbunden (insbesondere für Personal, die technische Infrastruktur und die rechtliche Absicherung). **Nachhaltige Finanzierungsmodelle** stellen, insbesondere im C2B-Kontext, weiterhin eine große Herausforderung dar. Im Anfangsstadium sind externe Anschubfinanzierungen durch die öffentliche Hand oder Dritte häufig essenziell, um die Entwicklung und Etablierung von Datentreuhändern abzusichern (Schneider, 2022). Allerdings sollte der Staat für eine *öffentliche Finanzierung*, die eine Umverteilung der Kosten auf das Kollektiv der Steuerzahlenden bedeutet, eine klare Legitimation für die staatliche Intervention vorlegen (Blankertz & Specht-Riemenschneider, 2021). Für eine dauerhafte Etablierung am Markt ist eine interne oder selbsttragende Finanzierungsperspektive entscheidend. Grundsätzlich lässt sich dabei zwischen Pay-per-Use-Modellen (nach Datenvolumen oder nach Anzahl Transaktionen), Abonnementmodellen und Mitgliedschaften unterscheiden (Lindner & Straub, 2023; Otto et al., 2022). Auch gibt es Ansätze, Datentransaktionen (also die technische Datenbereitstellung und die Föderation) unentgeltlich anzubieten; zusätzlich könnten hierauf aufsattelnde Mehrwertdienste kommerziell angeboten werden. Auch Mischformen sind denkbar, etwa in Form einer Mitgliederpauschale oder aber eines Pay-per-Use-Ansatzes für einzelne Datenprodukte.

All diesen Bepreisungsansätzen ist eine wesentliche Herausforderung gemeinsam: die **Bepreisung von Daten** und Datendienstleistungen. Denn es gibt bislang weder etablierte Marktpreise noch allgemein akzeptierte Bewertungsmechanismen für viele Arten von Daten.

Exkurs: Schwierigkeit der Bepreisung von Daten

Eine ökonomische Bewertung von Daten ist anhand von verschiedenen Ansätzen möglich (Krotova et al., 2019): Bei der (1) **marktorientierten Methode** wird der Wert von Daten durch den Preis bestimmt, den der Markt für vergleichbare Daten verlangt. Der Wert basiert also auf verfügbaren Marktpreisen oder marktähnlichen Transaktionen. Diese Methode setzt bereits einen aktiven Markt für den Datenhandel voraus. Die (2) **kostenorientierte Methode** beschreibt einen Ansatz, der den Wert anhand der Kosten berechnet, die für die Erhebung, Verarbeitung und Vermittlung von Daten entstehen. Die (3) **nutzenorientierte Methode** ermittelt den Wert basierend auf dem erwarteten Nutzen, den die Daten den Datennutzenden bringen, z. B. durch Einsparungen oder erhöhte Effizienz. Sie betrachtet also den tatsächlichen wirtschaftlichen Nutzen und ist deshalb besonders hilfreich für die Messung des potenziellen Werts von Daten, bei denen eine deutliche Wertasymmetrie zwischen der Wertzuschreibung seitens der Datengebenden und -nutzenden besteht.

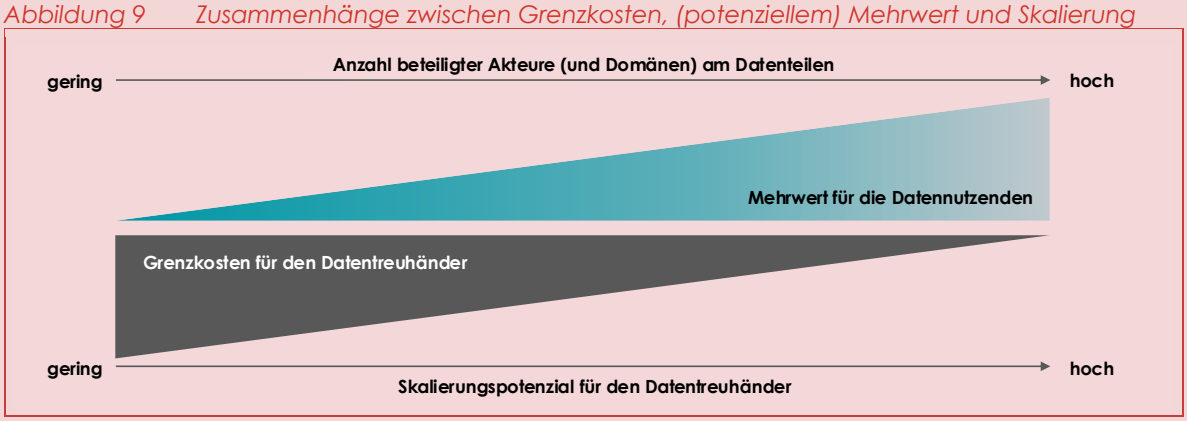
Bei der **Preissetzung** verweisen die empirischen Ergebnisse der Begleitforschung auf eine Präferenz für **kostenbasierte Ansätze**; d. h., dass der Preis auf der Grundlage der Kosten und einer zusätzlichen Marge festgelegt wird. In einigen Pilotprojekten wurde auch ein nutzenorientierter Ansatz als zielführend bewertet. Die marktorientierte Methode wurde hingegen nur selten als geeignet betrachtet.

Ein zentrales Spannungsfeld betrifft das umgekehrte Verhältnis von **Grenzkosten** für den Datentreuhandbetrieb und dem **erwarteten Mehrwert** für Datennutzende: Je mehr Akteure

(insbesondere unterschiedlicher Domänen) in einen Datenraum eingebunden sind, desto geringer werden die Grenzkosten für den Datentreuhänder – und desto größer kann der potenzielle Nutzen für Datennutzende werden. Gleichzeitig steigt mit wachsender Komplexität der Datenökosysteme aber auch die Heterogenität der Mehrwerte: Der tatsächliche Nutzen variiert stark je nach Akteur, Anwendungskontext und verfügbarer Expertise.

Daraus ergibt sich eine Herausforderung für die Bepreisung: Datentreuhänder mit vielen Beteiligten (insbesondere solchen aus unterschiedlichen Domänen) haben zwar aufgrund der sinkenden Grenzkosten ein hohes Skalierungspotenzial, sodass sie von nutzenbasierten Preismodellen stärker profitieren könnten als von rein kostenbasierten. Allerdings ist dieser potenzielle Nutzen vorab schwer zu bestimmen, da er sich oft indirekt und dynamisch im Verlauf der Informationsverarbeitung entfaltet. Dieses Phänomen entspricht dem **Arrow-Theorem** (Arrow, 1991), bei dem ein optimales Wohlfahrtsniveau durch den Markt nicht gewährleistet ist, da der Informationswert oft erst nach der Nutzung erkennbar wird. Dies gilt hier auch, da der Informationswert hochgradig kontextabhängig, subjektiv (Otto et al., 2022) und in vielen Fällen nicht transparent ist, etwa wenn er Bestandteil von Geschäftsgeheimnissen ist. Die folgende Abbildung veranschaulicht dies.

Abbildung 9 Zusammenhänge zwischen Grenzkosten, (potenziellem) Mehrwert und Skalierung



Quelle: Eigene Darstellung.

In der Praxis zeigt sich bei der Wahl des Finanzierungsmodells aktuell eine klare **Präferenz für Abonnementmodelle**, teilweise auch als zielgruppenspezifisch abgestuftes Preismodell. Vereinzelt werden Preisreduktionen oder eine kostenfreie Nutzung von Akteuren aus dem öffentlichen Sektor oder der Forschung angedacht. Einzelpreise pro Datensatz oder volumenbasierte Modelle gelten dagegen oft als zu aufwendig in der Umsetzung, da die Werthaltigkeit der Daten variieren kann. Auch könnten solche Ansätze bei profitorientierten Datentreuhändern Anreize dafür liefern, mehr Daten an mehr Datennutzende zu „verkaufen" als nötig, was das Missbrauchspotenzial erhöhen könnte (Blankertz & Specht-Riemenschneider, 2021). Allerdings sind auch Situationen denkbar, in denen sich gerade bei großen Datenmengen oder einer großen Zahl von Datenzugriffen wie bei realen Wetterdaten ein datenvolumen- oder zugriffsbasiertes Bezahlmodell als sinnvoll erweist.

Ein weiterer Ansatz zur Refinanzierung liegt in der Bereitstellung von **Analysediensten** (vergleiche Fallgruppe 3 der Datentreuhandmodelle), die, wie in Kapitel 2.3.5 bereits angeschnitten, das größte Skalierungspotenzial haben. Denn die Vermittlung, Verwaltung und Aufbereitung von Daten sowie die Wartung der Infrastruktur durch den Datentreuhänder sind mit kontinuierlichem Aufwand und Kosten verbunden. Ergänzende analytisch orientierte Dienste bieten hier die Möglichkeit, diese Kosten zu kompensieren – zumal sie, einmal

eingerichtet, mit vergleichsweise geringen Grenzkosten betrieben und auf zahlreiche Anwendungsfälle übertragen werden können. In B2B-Kontexten – in denen kleinere Datenvolumina und eindeutigere rechtliche Zuordnungen vorliegen – erscheinen solche Dienste als tragfähige Grundlage eines Geschäftsmodells. In B2C-Märkten hingegen beschränkt sich das Angebot häufig auf die Initiierung, Realisierung und Überwachung des Datentransfers, da hier in der Regel eine geringere Transparenz hinsichtlich der konkreten Verwendung der Daten vorherrscht.

Abzuwarten bleibt, inwieweit **die Finanzierung über weitere Mehrwertdienste aus europäischer regulatorischer Sicht** erlaubt sein wird: Unter dem DGA darf ein Datenvermittlungsdienst keine kommerziellen Interessen an den vermittelten Daten verfolgen, also weder die Daten noch die daraus gewonnenen Erkenntnisse für eigene kommerzielle Zwecke nutzen (Art. 12 DGA). Entsprechend ist lediglich eine Refinanzierung durch die „Verwaltung" der Daten / des Datenökosystems / des Datenraums möglich (RfII, 2021). Auch die im DGA verankerten **Neutralitätsanforderungen** und der damit verbundene Ausschluss von Abhängigkeiten zwischen Datenvermittlungsdiensten und Datengebenden wie -nutzenden bergen Unsicherheiten, welche Leistungen sie anbieten und in Rechnung stellen dürfen.

2.6.4 Auswirkungen von Datentreuhändern auf Datenmärkte

In der Diskussion um die Entwicklung von Datentreuhändermodellen findet sich die Befürchtung, dass es sich bei diesem Markt um einen Bowley-Wettbewerbsmarkt handeln könnte, der sich durch ständig sinkende Grenzkosten bei Ausdehnung der Nutzeranzahl auszeichnet (Otto et al., 2022; Bowley, 1924). Märkte mit bei Ausdehnung der Zahl von Datennutzenden stetig sinkenden Grenzkosten bzw. stetig steigenden Skalenerträgen werden auch als Märkte eines natürlichen Monopols bezeichnet (Knieps, 2008; Element AI & Nesta, 2019; Specht-Riemenschneider & Kerber, 2022). In diesen Märkten trifft die Annahme eines auf einen Gleichgewichtspreis tendierenden Preisniveaus nicht zu. Vielmehr haben die monopolistischen Anbieter die Chance, höhere Preise durchzusetzen. Außerdem können sie strategische Entscheidungen sowohl über den Zugang zum Datenraum als auch zum Umfang der nutzbaren Daten treffen. Dies könnte etwa zu partiellem Ausschluss von Datennutzenden oder der ungleichen Zugangsgeschwindigkeit zu Daten führen. Grundvoraussetzung für die Entstehung eines Bowley-Marktes wäre, dass sowohl aus technischer wie auch organisatorischer und regulativer Sicht keine steigenden Kosten auf Seiten des Datentreuhänders entstehen. In Folge der stetig sinkenden Grenzkosten würde sich ein „Lock-in" (Arthur, 1989) in einen Datentreuhänder ergeben, wie dies ansatzweise in den Social - Media-Plattformen zu beobachten ist.[7]

Die Entstehung eines natürlichen Monopols bzw. eines engen Dyopols ist aus wettbewerbspolitischer Perspektive negativ konnotiert. Bei der Analyse der Gefahr der Entstehung einer solchen Marktform haben sich zwei Perspektiven herauskristallisiert, wie diese zu verhindern ist: (1) regulatorische Ansätze und (2) wettbewerbliche Anreize. Aus der **regulatorischen Perspektive** haben die Europäische Union und das deutsche Wettbewerbsrecht bereits Maßnahmen ergriffen, die eine wettbewerbsverzerrende Marktform verhindern können. Insbesondere die regulatorischen Maßnahmen des Digital Market Acts, des Digital Service Acts sowie des DGA setzen hier dem Trend hin zu hochkonzentrierten Marktformen Grenzen.

Aus der Sicht der **wettbewerblichen Anreize** werden aber auch immer wieder seitens Expertinnen und Experten Zweifel geäußert, ob der **Gesamtmarkt für Datentreuhänder** wirklich die Eigenschaften eines natürlichen Monopols bzw. eines engen Dyopols aufweist. Das Kernargument gegen eine hohe Marktkonzentration lautet, dass es nicht einen Datenraum

[7] Es muss betont werden, dass selbst in den Social-Media-Plattformen kein wirkliches Monopol, sondern ein enges Dyopol vorliegt. So konkurrieren die Anwendungen des Meta-Konzerns mit Anwendungen von TikTok des ByteDance Unternehmens um Nutzende.

gäbe, der alle Daten in sich vereinige, sondern unterschiedliche Gruppen von Datengebenden und -nutzenden, die in unterschiedlichen zumindest teilseparaten Datenräumen agieren. Die Grundlage für diese Ansicht ist der erhebliche Kompetenzbedarf für die Schaffung domänenspezifischer Datenräume sowie die Schaffung von Vertrauen. Beide lassen sich nicht einfach von einer Anwendungsdomäne auf eine andere Anwendungsdomäne direkt übertragen. Vielmehr stellte sich ein geringerer Aufwand für die Datengebenden und -nutzenden ein, wenn ein Datentreuhänder domänenspezifisch aufgestellt ist, da dann die Kompetenz über die Daten und die vertrauensbildenden Maßnahmen leichter zu realisieren sind. Dieses Argument weist aber das Problem auf, dass es in einzelnen Anwendungsdomänen dann doch wiederum eine hohe Marktkonzentration geben kann. Diese wäre aber weniger problematisch, da dann die Reichweite der Marktkonzentration relativ begrenzt ist. Eine Vernetzung von domänenspezifischen Datentreuhändern über Konnektoren sei aber denkbar, führt dann aber nicht zu den wettbewerbsbeschränkenden Marktformen.

Im Unterschied zur Entstehung eines wettbewerbsverzerrenden Gesamtmarktes für Datentreuhandleistungen ist das Auftreten von **wettbewerbsbeschränkenden Marktformen** bei der Betrachtung von Datentreuhandleistungen **in einzelnen Anwendungsdomänen** durchaus möglich. Je nach Datenaufkommen, Umfang der Anzahl der Akteure in der Anwendungsdomäne sowie der Heterogenität der gemeinsam im Datenraum genutzten Daten sind wettbewerbshinderliche Marktformen denkbar. Da es sich dabei in der Regel jedoch um überschaubare Märkte handelt, gehen die im Rahmen der Begleitforschung befragten Expertinnen und Experten jedoch davon aus, dass das Problem mit vorhandenen wettbewerbspolitischen Instrumenten beherrschbar ist.

Neben den Monopolisierungstendenzen bei den Anbietern von Datentreuhandleistungen finden sich Monopolisierungsrisiken möglicherweise auch im B2B-Umfeld seitens der **Datengebenden oder -nutzenden**. In der Automobilbranche etwa besteht die Gefahr, dass die „Gatekeeper-Position der Autohersteller" Wettbewerb und Innovationen in Bezug auf die Daten hemmt. Neue oder weiterentwickelte Datentreuhandmodelle können dieses Machtungleichgewicht teilweise beseitigen und einen offeneren Datenzugang unter Datenschutzvoraussetzungen wie auch die Entwicklung eines fairen Markts fördern (Specht-Riemenschneider & Kerber, 2022; Element AI & Nesta, 2019). Besonders in Konstellationen mit starker Machtasymmetrie oder geringer Konkurrenz, z. B. marktbeherrschende Stellung globaler Plattformen vs. Markteinsteiger, Asymmetrien zwischen Datengebenden (z. B. Verbraucherinnen und Verbraucher) sowie Datennutzenden (z. B. Forschende) können Datentreuhänder von besonderer Relevanz sein (RfII, 2020; Blankertz & Specht-Riemenschneider, 2021).

2.6.5 Schlussfolgerungen und Handlungsbedarf

Welches **Betriebsmodell** sich für das jeweilige Datentreuhandmodell eignet, hängt von verschiedenen Faktoren ab, etwa dem Anreiz zum Betrieb, den angebotenen Funktionalitäten des Datentreuhänders, der Anwendungsdomäne und den beteiligten Akteursgruppen sowie der Art und Sensibilität der Daten.

- Insgesamt zeigt die Begleitforschung, wie schwer es ist, ein tatsächlich funktionierendes Geschäftsmodell für Datentreuhänder zu entwickeln. Eine zentrale Herausforderung bildet auch bei der Entwicklung von Geschäftsmodellen die Rechtsunsicherheit.
- Wichtige **Aspekte des Geschäftsmodells** betreffen die vom anvisierten Datentreuhänder anzubietenden Funktionen (inklusive der Entscheidung für oder gegen hierauf aufsetzende Mehrwertdienste), der Datenraum und die Domäne, in der dieser sich bewegen soll, die Zahlungsbereitschaft der Akteure, die Wahl eines geeigneten, vertrauensbildenden Betreibers und die Wahl des Finanzierungsmodells.

- Ein Datentreuhänder kann grundsätzlich privat (non- oder for-profit) oder öffentlich **betrieben** werden. Als mögliche **Governance-Formen** können Datentreuhandbetreiber dabei zwischen institutionellen, mitgliedsorientierten und Unternehmensmodellen wählen.
- Bei den **Bepreisungsansätzen** können Anbieter zwischen Pay-per-Use-Modellen (nach Datenvolumen oder nach Anzahl Transaktionen), Abonnementmodellen, Mitgliedschaften oder der **Finanzierung** über aufsetzende Mehrwertdienste unterscheiden. Die in dieser Studie begleiteten Pilotprojekte zeigen eine leichte Tendenz zu Abonnementmodellen.
- Auch aus Geschäftsmodellsicht hat die **Fallgruppe der geteilten Analyseergebnisse** (vergleiche Datentreuhandmodelle 3.1 und 3.2 in der Abbildung 5) aufgrund der geringen Grenzkosten das größte Skalierungspotenzial. Gleichzeitig bestehen hier jedoch auch die größten Unsicherheiten, was die Zulässigkeit solcher Modelle unter dem DGA betrifft.

Im nächsten und letzten Unterkapitel wird das Potenzial für die Skalierung erfolgreicher Datentreuhänder beleuchtet.

2.7 Skalierung von Datentreuhandmodellen

Das Wichtigste zu Skalierung in Kürze:

- Die meisten Datentreuhänder in Europa befinden sich noch im Aufbau und konzentrieren sich bislang meist auf **nationale Kontexte** und **einzelne Domänen**. Domänenübergreifende oder europaweite Modelle sind noch selten und mit hohen Aufbauhürden verbunden.
- Mittelfristig wird eine stärkere Vernetzung als sinnvoll erachtet, vor allem in Form interoperabler, föderierter Zusammenschlüsse im Einklang mit Initiativen wie Gaia-X und der IDSA.
- Um spätere (insbesondere domänenübergreifende) Zusammenschlüsse zu erleichtern, sollten Datentreuhänder frühzeitig auf **gemeinsame Standards, Schnittstellen und Konnektoren** setzen.

2.7.1 Geografische und sektorale Skalierung

Europaweit scheinen sich die meisten Datentreuhänder noch in relativ frühen Aufbaustadien zu befinden. Was sinnvolle und realistische Skalierungsziele sind, ist daher noch schwer abzuschätzen. Grundsätzlich müssen sich Datentreuhänder im Laufe ihrer Entwicklung entscheiden, ob sie primär eine Domäne adressieren wollen oder Akteure domänenübergreifend zusammenbringen wollen. Ebenso müssen sie entscheiden, ob sie nur eine Teilmenge der potenziell relevanten Domänenakteure in ihrem Land als Teilnehmende (Datengebende und -nutzende) gewinnen wollen, ob sie alle inländischen Akteure einbeziehen wollen oder ob eine europa- oder weltweit offene Teilnahme angestrebt wird.

Mit wenigen Ausnahmen (z. B. die UK Biobank) scheinen die meisten Datentreuhänder in Deutschland und Europa in der Praxis bislang meist noch einen **primär nationalen Fokus** zu haben. Auch konzentrieren sie sich bislang oft noch auf **einzelne Domänen** (z. B. Mobilität). Übergreifende Datentreuhänder, die **multiple Domänen** adressieren, sind **seltener** zu beobachten. Die Gründe hierfür dürften in erster Linie in der allgemeinen Schwierigkeit, Datentreuhänder aufzubauen, begründet liegen: Um den Hochlauf nicht noch weiter zu verkomplizieren, konzentrieren sich Projekte verständlicherweise meist zuerst auf ein Land und eine Domäne.

Mittel- bis langfristig jedoch wird eine **stärkere Europäisierung** oft als sehr wünschenswert erachtet, ebenso wie **domänenübergreifende Zusammenschlüsse**. Beides scheint dabei meist mehr als interoperabler Zusammenschluss föderierter, aber eigenständiger Datentreuhänder konzipiert zu werden denn als klassische „Expansion“ in einen neuen Markt. Das wäre auch im Einklang mit den Aktivitäten von Gaia-X und der IDSA, föderierte und interoperable Dateninfrastrukturen aufzubauen.

Sollten Datentreuhänder tatsächlich, wie in Kapitel 2.2 diskutiert, zunehmend als Ökosystem-Orchestratoren auftreten, könnte dies eine Skalierung über multiple Domänen bzw. Ökosysteme hinweg zunächst verlangsamen: Ein solcher Datentreuhänder (Orchestrator) dürfte seinen Fokus vorerst noch stärker auf das eigene unmittelbare Ökosystem richten, um dieses zum Laufen zu bringen. Mittelfristig jedoch könnte der Aufbau von Verbindungen zu weiteren Ökosystemen eine wichtige Aufgabe für Orchestratoren werden.

Unter den Pilotprojekten selbst blieben die **Skalierungsziele** bis zum Ende der Laufzeit der Begleitforschung **heterogen**. In Befragungen gab die Mehrzahl der Projekte als Skalierungsziel an, mittelfristig die meisten Akteure in ihrer adressierten Domäne in Deutschland oder sogar Europa als aktive Teilnehmende im Datentreuhandmodell gewinnen zu wollen. Eine Minderheit sah darin jedoch keinen Vorteil und wollte auch langfristig klein bleiben. Die meisten, aber nicht alle Pilotprojekte glaubten ebenfalls, dass stärkere Interoperabilität und Zusammenschlüsse zwischen Datentreuhändern in unterschiedlichen Domänen erheblichen Mehrwert schaffen könnte. In der Praxis jedoch blieben die Anstrengungen meist national und auf einzelne Domänen fokussiert, was allerdings schlicht dem frühen Entwicklungsstand der Projekte geschuldet war.

2.7.2 Skalierungsstrategien

Aufgrund des frühen Entwicklungsstands der meisten Datentreuhänder zeichnen sich systematische Strategien zur Skalierung bislang kaum ab. Eine Ausnahme bildet die UK Biobank, die eine Art *public-private partnership*-Ansatz entwickelt hat, um ihre Datenbestände stetig zu erweitern. Kern der UK Biobank sind die Gesundheitsdaten von rund 500.000 Datenspendenden (Privatpersonen), die Forschenden weltweit gegen einen geringen Unkostenbeitrag zur Verfügung stehen. Diese Daten systematisch zu erweitern (z. B., indem für eine größere Anzahl der Spender zusätzliche CT-Scans, Genomsequenzierungen oder andere Datenerhebungen durchgeführt werden), ist sehr wertvoll, aber auch mit erheblichen Kosten verbunden. Die UK Biobank hat daher ein Modell entwickelt, bei dem privatwirtschaftliche Akteure (z. B. Pharmafirmen), welche die Kosten für die Erstellung eines neuen Datensets übernehmen, zunächst für neun Monate exklusiven Zugang zu diesen neuen Daten erhalten. Danach werden dieselben Daten allen UK Biobank-Nutzenden zugänglich gemacht. Dieses Modell erlaubt es der UK Biobank, ihre Datenbestände ohne Kostenexplosion kontinuierlich zu erweitern.

Eine weitere Strategie, die bei Anwendungsfällen außerhalb der Pilotprojekte identifiziert wurde (siehe Anhang D für eine vollständige Liste), zielt darauf ab, den Datentreuhänder von vornherein so dezentral aufzustellen, dass eine Skalierung praktisch einprogrammiert ist. So versteht sich etwa Catena-X als offenes, kollaborativ angelegtes Datenökosystem, an dem über 130 Unternehmen beteiligt sind. Hier können verschiedene Partner an technischen Umsetzungslösungen fürs Datenteilen arbeiten, die anschließend von einem zentral eingerichteten Verein zertifiziert werden. Der Datentreuhänder ist in diesem Fall an ein bereits bestehendes Ökosystem aus Unternehmen angeschlossen, die entlang der Wertschöpfungskette über Geschäftsbeziehungen miteinander verbunden sind. Dadurch kann der Datentreuhänder schrittweise und modular neue Teilnehmende und Themenbereiche eingliedern.

2.7.3 Schlussfolgerungen und Handlungsbedarf

Angesichts der zahlreichen Herausforderungen beim Aufbau von Datentreuhändern scheinen rasche **europäische** und **domänenübergreifende Skalierungen** von Datentreuhändern unrealistisch. Aufgrund der Heterogenität der von verschiedenen Datentreuhändern adressierten Domänen ist es zudem unplausibel, dass in allen Fällen das gleiche Skalierungsziel angestrebt werden sollte. Welches jeweils die optimale Skalierung ist, wird sich in vielen Fällen auch erst über weitere praktische Erprobungen herausstellen.

Gleichwohl sollten Datentreuhänder befähigt werden, domänenübergreifende Zusammenschlüsse möglichst leicht umzusetzen, falls sich diese im Laufe ihrer Entwicklung als

zweckmäßig herausstellen. Das bedeutet insbesondere, dass weitere Standardisierung von Daten, Governance und technischen Schnittstellen anzustreben ist. Datentreuhänder sollten zudem möglichst einheitliche Konnektoren und technische Komponenten – wie die der IDSA – implementieren, um Zusammenschlüsse zu ermöglichen.

3 Resümee und Handlungsempfehlungen

3.1 Resümee

Die Begleitforschung hat eingangs die **Hypothese** aufgestellt, dass Datentreuhänder ein mögliches Instrument zur positiven Beeinflussung des Wert-Risiko-Dilemmas und somit zum Aufbau florierender Datenökosysteme unter Einbezug von politischen Entscheidungsträgern und öffentlicher Verwaltung, Wirtschaft und Wissenschaft in verschiedenen Domänen darstellen. Diese These konnte aufgrund der konzeptionellen Überlegungen theoretisch und in Anbetracht der empirischen Befunde praktisch **validiert** werden. Die BMFTR-geförderten Pilotprojekte konnten insbesondere technische und rechtliche Anforderungen und Lösungsansätze für den Aufbau von Datentreuhändern in verschiedenen Domänen erproben. Gleichzeitig bestätigen die von den Pilotprojekten aufgeworfenen Fragen und weiteren Befunde der Begleitforschung, dass verschiedene Herausforderungen einem breiten Einsatz von Datentreuhändern derzeit noch entgegenstehen. Lösungsansätze für einige dieser Herausforderungen konnten von der Begleitforschung empirisch identifiziert und konzeptionell weiterentwickelt werden.

Um Datengebende und -nutzende **anzuwerben**, ist es entscheidend, dass Datentreuhänder ihnen einen klaren Wert bieten, der die ihnen entstehenden Kosten und Risiken übersteigt. Vor allem aber ist es erforderlich, dass sie bei diesen Akteuren Vertrauen schaffen, um sie so zur Nutzung des Datentreuhänders zu bewegen.

Die hohe **Rechtsunsicherheit** in Bezug auf Compliance-Fragen bremst den Aufbau von Datentreuhändern aus. Die Begleitforschung hat eine **Toolbox** entwickelt, anhand derer sich verschiedene Datentreuhandmodelle je nach angestrebter Funktionalität und der im jeweiligen Anwendungsgebiet aufzulösenden Interessenskonflikte zwischen Datengebenden und -nutzenden einordnen lassen. Hieraus können geeignete **rechtliche und technische Bausteine** gewählt werden. Aus technischer Sicht müssen insbesondere Interoperabilität, Datensicherheit und -minimierung gewährleistet sein.

Das zu wählende **Geschäftsmodell** für einen Datentreuhänder hängt vom jeweiligen Anwendungsfall ab. Für die Bepreisung der zu teilenden Daten, die Finanzierung des Datentreuhandbetriebs sowie die Rechtsform gibt es jeweils unterschiedliche Optionen.

In Zukunft können **Standards und Zertifizierungen** eine stärkere Rolle bei der geografischen und domänenübergreifenden **Skalierung** von Datentreuhändern spielen. Skalierung wird dabei aller Wahrscheinlichkeit über den föderierten Zusammenschluss verschiedener Datentreuhänder geschehen.

Im Folgenden formuliert die Begleitforschung **Handlungsempfehlungen** an **Betreiber von Datentreuhändern.** Diese können als **Toolbox** verstanden werden. Eine zentrale Erkenntnis der Begleitforschung ist allerdings auch, dass der Erfolg von Datentreuhändern von mehr Rahmenbedingungen abhängig ist als initial angenommen und dass diese zudem meist nicht direkt durch den Datentreuhänder beeinflusst werden können. Daher richten sich weitere Handlungsempfehlungen an diejenigen Akteure, die rechtliche, technische und ökonomische Faktoren beeinflussen können, nämlich an **politische Entscheidungsträger und die öffentliche Verwaltung, an Wissenschaft und Wirtschaft**. Das gemeinsame Ziel aller Akteure sollte dabei die Überwindung des eingangs aufgeworfenen Wert-Risiko-Dilemmas sein.

3.2 Empfehlungen an Betreiber von Datentreuhändern

(Potenzielle) Betreiber von Datentreuhändern sollten sich in einem ersten Schritt über ihr **Problemverständnis, ihre Zielsetzung sowie ihr spezifisches Wertversprechen** klarwerden.

- Datentreuhänder müssen zunächst die Akteure in ihrem anvisierten Anwendungsbereich identifizieren, die als Datengebende und -nutzende fungieren können. Sodann gilt es, diesen ein klares und belastbares Wertversprechen zu geben. Zunächst sollten Betreiber daher

ihren **Nutzen bzw. Mehrwert** für Datengebende sowie -nutzende sorgfältig analysieren, so gut dies angesichts der Heterogenität und Segmentierung in oftmals noch diffusen Datenökosystemen möglich ist. Je nach Zielsetzung kann ein Datentreuhänder unterschiedlichste Funktionalitäten erfüllen. Sowohl im Aufbau als auch im laufenden Betrieb gilt es daher zu prüfen, welche **Funktionen** das Datenteilen über den Datentreuhänder besonders attraktiv machen. Um das Wertversprechen realisieren zu können, müssen Datentreuhänder dabei oft mehr tun, als nur die Bereitstellung von Daten zu ermöglichen. Sie sollten insbesondere erwägen, als Ökosystem-Orchestratoren aufzutreten. Auch Mehrwertdienste wie auf den geteilten Daten aufbauende Analysen und Harmonisierung heterogener Datenbestände können attraktive Funktionen darstellen, erhöhen allerdings auch den technisch-organisatorischen Aufwand und die Komplexität des Datenteilungsvorgangs.

- Die **Motive** aber auch die **praktischen Hindernisse** für das Datenteilen können je nach Akteur und Domäne höchst unterschiedlich sein. Datentreuhänder sollten daher die Spezifika der von ihnen adressierten Akteure und Communitys analysieren, um das passende Instrument auszuwählen, und gegebenenfalls mit unterschiedlichen Ausgestaltungen experimentieren. Im land- und forstwirtschaftlichen Bereich können Datentreuhänder etwa Partnerschaften mit Maschinenherstellern eingehen, um Schnittstellen für eine reibungslose Datenweitergabe direkt in Harvestern zu integrieren. Eine andere Strategie kann sein, sich zunächst auf Akteure zu konzentrieren, zwischen denen bereits geschäftliche oder andere Beziehungen bestehen, und zu versuchen, diese Beziehungen durch die verstärkte Nutzung und das verstärkte Teilen von Daten weiter aufzuwerten. Neben dem konkreten Nutzen sollten dabei umgekehrt die möglichen **Interessenkonflikte** (insbesondere Compliance-Risiken) für Datengebende und -nutzende analysiert werden, die sie durch den Aufbau entsprechender Datentreuhänder lösen möchten (und die implizit in Abwesenheit des Datentreuhänders das Datenteilen ausbremsen oder vereiteln). Hierfür sollten Betreiber frühzeitig auch auf die (anvisierten) Datengebenden und -nutzenden zugehen und vertrauensvolle Beziehungen anbahnen, etwa durch Aufnahme dieser Akteure oder ihrer Repräsentanten in einen Aufsichtsrat.
- Daneben könnte es hilfreich sein, frühzeitig auch (zivilgesellschaftliche, politische und wirtschaftliche) Schlüsselakteure und Interessensvertretungen (z. B. von Patientinnen und Patienten in der Medizinforschung) als sogenannte „Vertrauensmultiplikatoren" miteinzubeziehen und mittels entsprechender **Öffentlichkeitsarbeit** für Vertrauen in die jeweilige Lösung zu werben. Dies könnte gerade vor dem Hintergrund der bestenfalls schleppenden Entwicklung von Zertifikaten für Datentreuhänder einen wichtigen Hebel für die Vertrauensgewinnung darstellen.

In einem zweiten Schritt sollten Betreiber von Datentreuhändern klären, mit welchen **technischen, organisatorischen und rechtlichen Verfahren** und Strukturen sie den Aufwand für das Datenteilen (und die damit einhergehenden Risiken) am effektivsten reduzieren können und wer die Compliance-Verantwortung für die Restrisiken übernimmt. Darauf aufbauend sollten sie sodann geeignete **Bausteine** für die Konstruktion der wahrzunehmenden Aufgaben ihres Datentreuhänders wählen. Dabei können sie sich an den in dieser Studie vorgestellten Fallgruppen orientieren (siehe insbesondere Kapitel 2.3 und 2.4).

- Aus **rechtlicher Sicht** sollten Betreiber außerdem prüfen, ob ihr Datentreuhänder als Data Broker (siehe Glossar) oder als Datenvermittlungsdienst auftreten soll, also ob er unter den DGA fallen soll oder nicht.
- Aus **technischer Sicht** ist es empfehlenswert, zunächst das notwendige Datentreuhandmodell festzulegen, darauf aufbauend die passenden technischen Bausteine zu wählen und eine Referenzarchitektur zu entwickeln. Für alle Bausteine sollte der Einsatz von Standards geprüft und bevorzugt werden – wo davon Abstand genommen wird, sollte dies gut begründet sein. Entsprechend dem festzulegenden Schutzbedürfnis der Daten sind geeignete Maßnahmen zur Nutzungskontrolle zu wählen. Erfahrungen aus den Pilotprojekten zeigen,

dass das notwendige Vertrauen nicht allein über technische Maßnahmen aufgebaut werden kann. Dementsprechend sind generell aber insbesondere auch für die Nutzungskontrolle technische Lösungen gemeinsam mit den rechtlichen und organisatorischen Maßnahmen zu entwickeln.

- Datentreuhänder könnten zudem mittels möglichst einheitlicher Konnektoren und technischer Komponenten unter Nutzung von Rahmenbedingungen und Architekturen wie Gaia-X und technischen Entwicklungen wie der IDSA Zusammenschlüsse ermöglichen und **Skalierung** erleichtern.
- Zudem ist ein geeignetes **Geschäftsmodell** zu wählen. Hierfür sollte zunächst festgelegt werden, welche Funktionen der Datentreuhänder anbieten soll und ob hierzu auch Mehrwertdienste wie die Analyse geteilter Daten gehören sollen. Außerdem müssen je nach Domäne und Anwendungsgebiet geeignete Preismodelle gewählt werden. Gegebenenfalls müssen diese im Pilotbetrieb erprobt werden, bevor ein Betreiber sich auf ein passendes Modell festlegt.
- Datentreuhänder sollten darauf hinwirken, als neutrale und verlässliche Akteure wahrgenommen zu werden. Um **Vertrauen** weiter aufzubauen, sollten sie daher ihre Rechtsform bewusst wählen sowie überlegen, strategische Partnerschaften einzugehen oder relevante Akteure bzw. ihre Repräsentanten in den Aufsichtsrat oder ähnliche Gremien aufzunehmen. In diesem Zusammenhang könnte langfristig auch die vorwettbewerbliche Zusammenarbeit von Datentreuhändern in einem eigenen Verband sinnvoll sein, gegebenenfalls auch, um eine gemeinsame politische Interessenvertretung zu organisieren und aus der Praxis getriebene Standards zu entwickeln.

Um das Datenökosystem in Gang zu bringen sind neben den Datentreuhändern selbst aber auch Datengebende und -nutzende aufgefordert, entsprechende Dienste zu nutzen, ihre Daten zu teilen und sich an entsprechenden Referenzprojekten zu beteiligen. Die erfolgreiche Etablierung von Datentreuhändern wird durch eine Kultur der Offenheit und Neugierde bei potenziellen Datengebenden und -nutzenden begünstigt. Über erfolgreiche Pilotbeispiele kann eine solche Kultur weitergehend gefördert werden.

3.3 Empfehlungen an politische Entscheidungsträger und öffentliche Hand

Politische Entscheidungsträger, Vollzugsbehörden und die öffentliche Verwaltung können den Aufbau und die Etablierung von Datentreuhändern über einige Hebel stärker unterstützen. Insbesondere können sie dazu beitragen, Komplexität und Aufwände für Datentreuhänder und für das Datenteilen zu reduzieren. Dafür sind insbesondere **regulatorische Maßnahmen** geeignet, die Rechtssicherheit schaffen. Hierbei spielt neben der nationalen auch die europäische Ebene eine wichtige Rolle, da wichtige Gesetzesakte wie der DGA auf dieser Ebene verabschiedet wurden, aber auch, da ein europäischer Rahmen die Skalierung erleichtert.

Die Begleitforschung sieht für den Gesetzgeber und die Vollzugsbehörden daher mehrere Hebel zum Schaffen von Rechtssicherheit und zur Förderung des Datenteilens:

- Der Gesetzgeber sollte seine Gesetze möglichst stärker so ausgestalten, dass sie es Datengebenden, -nutzenden und Datentreuhändern ermöglichen, das Wert-Risiko-Dilemma aufzulösen. Hierzu gehört insbesondere, die **Rechtsunsicherheit beim Datenteilen und für den Betrieb von Datentreuhändern zu reduzieren**, also unter anderem die Verteilung der Compliance-Verantwortung zu klären (vergleiche Kap. 3.3). Insbesondere der DGA sollte dahingehend angepasst werden, dass der Datentreuhänder all diejenigen Funktionen übernehmen kann, die nötig sind, um zur Auflösung des Wert-Risiko-Dilemmas im jeweiligen Ökosystem beizutragen, anstatt – wie derzeit – eigene Unsicherheit zu erzeugen. Hier ist also auch der europäische Gesetzgeber gefragt.

- **Standardisierung anstoßen bzw. unterstützen**: Politische Entscheidungsträger sollten Initiativen zur Entwicklung einheitlicher Standards und Schnittstellen in Bezug zu Datentreuhändern systematisch fördern. Insbesondere gilt dies für Standards in den Bereichen technische Sicherheit und Governance-Strukturen, Datenstandards, aus datenschutzrechtlicher Sicht auch für Standards zur Einholung wirksamer (weil nutzerfreundlicher) Einwilligungen sowie die Entwicklung sicherer Datenverarbeitungsumgebungen vor allem zur Sicherstellung der Datenqualität und/oder Anonymisierung (sei es zum Schutz von Geschäftsgeheimnissen, der IT-Sicherheit, des Wettbewerbs- und Datenschutzrechts oder nun auch der KI-Verordnung).
- Der Staat könnte daneben die gemeinsame Entwicklung von Standards durch Akteure aus Wissenschaft und Wirtschaft auch dadurch fördern, indem er die Einrichtung entsprechender Foren und **Austauschformate** unterstützt (wie z. B. im Falle der Nationalen Forschungsdateninfrastruktur[8], dem Mobility Data Space[9] oder der Medizininformatik-Initiative[10]) – dies idealerweise sowohl auf europäischer als auch auf nationaler Ebene (im engen Austausch miteinander). Dies kann auch in Form von staatlich unterstützten De-facto-Standards erfolgen, die durch kooperative Verfahren durch die Wirtschaft und Wissenschaft entwickelt werden. Der Beitrag von Akteuren der Wissenschaft und Wirtschaft zu europäischen und auch internationalen Standardisierungsaktivitäten sollte daher förderfähig sein.
- In einem mittelfristigen Ansatz sollten Anreize gesetzt werden, die dann existierenden Standards auch umzusetzen. Außerdem sollte der Staat ein Akkreditierungssystem aufbauen, das die **Zertifizierung** von vertrauenswürdigen Datentreuhändern ermöglicht. Ein erster Schritt zum Aufbau eines Akkreditierungssystems ist mit den EU-Registern für nach dem DGA anerkannte Datenvermittlungsdienste und datenaltruistische Organisationen bereits erfolgt.[11] Diese Register könnten erweitert werden, um auch solche Datentreuhänder aufzunehmen, die nicht unter den DGA fallen, aber vertrauenswürdig sind. Sodann könnten etablierte Zertifizierungsorganisationen mit dem Aufbau von Zertifizierungsprogrammen für Datentreuhänder beginnen. Durch einen wachsenden Markt sollten sich hier genügend kommerzielle Anreize entwickeln. Falls sich dies nicht so einstellen sollte, dann wäre auch hier eine staatliche Anschubförderung zu erwägen.
- Die öffentliche Hand sollte auch selbst eine **Vorreiterrolle** einnehmen und als Impulsgeber agieren: Indem etwa Behörden und Verwaltungen eigene Daten kontrolliert über Datentreuhänder teilen, kann der Staat Vertrauen in das Modell stärken und zur breiten Etablierung entsprechender Infrastrukturen beitragen, aber auch direkt für Wirtschaft und Wissenschaft Nutzen durch die Verfüg- und Nutzbarkeit von Daten schaffen.
- Vollzugsbehörden sollten sämtliche Fälle, die sie entscheiden, in einem gemeinsamen **Use Case Repository** systematisiert sammeln und der Öffentlichkeit (insbesondere Datengebenden und Datentreuhändern) zur Verfügung stellen.[12] Diese wichtige Rolle könnten z. B. das Dateninstitut oder das DatenTreuhand Kompetenznetzwerk übernehmen.

Daneben könnte die Bundesregierung auch durch **Förderpolitik** die Verstetigung von Datentreuhändern unterstützen. Hierbei könnte sie auf den bereits veröffentlichten Förderrichtlinien des BMFTR sowie anderen bundespolitischen Maßnahmen wie der Flankierung

---

[8] https://www.nfdi.de/section-metadata/ (zuletzt abgerufen am 5. Juni 2025).

[9] https://mobility-dataspace.eu (zuletzt abgerufen am 5. Juni 2025).

[10] https://www.medizininformatik-initiative.de/ (zuletzt abgerufen am 5. Juni 2025).

[11] Das EU-Register für Datenvermittlungsdienste ist einsehbar unter https://digital-strategy.ec.europa.eu/de/policies/data-intermediary-services; das Register für datenaltruistische Organisationen unter https://digital-strategy.ec.europa.eu/en/policies/data-altruism-organisations (beide zuletzt abgerufen am 30.06.2025). Für Cloud-Anbieter gibt es eine vergleichbare Initiative des BMWi: https://www.trusted-cloud.de (zuletzt abgerufen am 5. Juni 2025).

[12] Die geplante bundeseinheitliche Justizcloud könnte ein wichtiger Infrastrukturbaustein hierfür sein: https://www.bmj.de/DE/themen/digitales/digitalisierung_justiz/digitalisierungsinitiative/_articles/justizcloud_artikel.html (zuletzt abgerufen am 5. Juni 2025).

von Gaia-X (BMWE und BMFTR) oder der Förderung von Datenräumen wie dem Mobility Data Space (BMDS) aufbauen.

- Zwar ist der Staat in vielen Fällen nicht für den direkten Betrieb von Datentreuhändern geeignet. Dennoch kann er eine wichtige Rolle als neutraler Akteur bei deren **Anschubfinanzierung** spielen. Hierdurch können erfolgreiche Anwendungsbeispiele entstehen, die wiederum andere Akteure zur Einrichtung von Datentreuhändern in anderen Domänen anregen können. Aber auch finanzielle Unterstützung bei der Skalierung kann sinnvoll sein, insbesondere bei gemeinwohlorientierten Datentreuhandmodellen. Die Förderung einer kleinen Anzahl größerer, längerfristiger Projekte (mit der Festlegung mittelfristiger Meilensteine) scheint dabei zielführender als die Förderung vieler kleiner Projekte.

Weitere Fördermaßnahmen sollten dabei an **bestimmte Bedingungen** geknüpft sein, um Fragmentierung und Parallelentwicklungen zu vermeiden und die öffentliche Wirkung der Förderung zu maximieren:

- Geförderte Projekte sollten dazu angehalten werden, zentrale Ergebnisse – insbesondere Software-Komponenten, methodische Bausteine und erprobte Anwendungsfälle – in öffentlich zugänglichen Repositorien verfügbar zu machen.
- Die Nachnutzung bestehender Standards, Open-Source-Komponenten und interoperabler Bausteine sollte als verbindliche Auflage in Förderprogrammen verankert werden (wie bereits in den späteren Förderrichtlinien des BMFTR geschehen). Falls dies im Einzelfall nicht möglich ist, muss dies nachvollziehbar begründet werden. Gleichzeitig sollte ein Beitrag zur Weiterentwicklung dieser Standards Teil der Projektziele sein.
- Eigenentwicklungen, die im Rahmen öffentlicher Förderung entstehen, sollten grundsätzlich öffentlich weiterverwendbar sein. Ausnahmen sollten nur bei triftigen Gründen möglich sein.

Wo der Staat den Aufbau von Datentreuhändern fördert, sollte er (je nach Anwendungsfall) auf eine **Beteiligung der organisierten Zivilgesellschaft sowie von Interessengruppen** hinwirken, um Akzeptanz und Relevanz der Modelle zu erhöhen. Umgekehrt ist die organisierte Zivilgesellschaft aufgefordert, den Aufbau von Datentreuhändern in verschiedenen Anwendungsbereichen konstruktiv und kritisch zu begleiten.

3.4 Empfehlungen an Wissenschaft

Die Wissenschaft generiert einen beträchtlichen Teil der Daten, die für die Lösung gesamtgesellschaftlicher Probleme von Relevanz sind. Sie findet sich daher oft in der Rolle der Datengebenden wieder, aber auch der Datennutzenden, wenn sie Forschung auf Grundlage von Daten Dritter betreibt, z. B. im Medizinbereich. Wissenschaftseinrichtungen spielen daher eine zentrale Rolle bei der Unterstützung des Aufbaus von Datentreuhändern zur Förderung des Datenteilens sowohl innerhalb dieser Domäne als auch zwischen Wissenschaft und Wirtschaft. Die Begleitforschung empfiehlt der Wissenschaft daher Folgendes:

- Die weitere **Datenstandardisierung** sollte vorangetrieben werden, um diese brauchbarer und leichter teilbar zu machen. Die Wissenschaft, insbesondere Forschungseinrichtungen, sollte auch an der Entwicklung relevanter technischer Schnittstellen für das Datenteilen mitwirken. Auch an der Weiterentwicklung plattformübergreifender Standards und Schnittstellen für die Autorisierung von Datenzugriffen sollte die Wissenschaft sich beteiligen. Neben der (Weiter-)Entwicklung von Standards sollten auch bestehende Standards im Verbund mit Praxispartnern anhand weiterer Use Cases ausprobiert und für spezifische Anwendungsdomänen implementiert werden. Zu guter Letzt kann die Wissenschaft domänenspezifische Standards für Interoperabilität mitentwickeln. Insbesondere sollten dabei semantische Verfahren vorangetrieben werden, die heterogene Systeme interoperabel werden lassen.
- Weitere **Forschung** zur Entwicklung tragfähiger Datentreuhandmodelle sollte regelmäßig **interdisziplinär** stattfinden, da diese Beiträge aus Informatik, Rechtswissenschaft, Sozialwis-

senschaft und Ökonomie erfordert. Die Entwicklung von Datentreuhändern sollte weiter erforscht werden, um zentrale Handlungsempfehlungen in Form von Handreichungen an Betreiber auszuarbeiten.

- Wissenschaftsorganisationen sollten das **Verfügbarmachen von Date**n bzw. die **Schaffung geeigneter Datentreuhänder** als wissenschaftliche Leistung analog zum Transfer anerkennen.
- Auch sollte die Wissenschaft durch die Nutzung von Datentreuhändern zu deren Etablierung beitragen

3.5 Empfehlungen an die Wirtschaft

Neben der Wissenschaft spielt die Wirtschaft eine zentrale Rolle beim Aufbau einer florierenden Datenökonomie. Unternehmen sind zentrale Akteure als Kunden von Datentreuhändern. Aus Sicht der Begleitforschung könnte die Wirtschaft den Aufbau von Datentreuhändern folgendermaßen unterstützen:

- In Kooperation mit der Wissenschaft sollte die Wirtschaft sich an der Entwicklung relevanter **Standards und Schnittstellen** in den in Kapitel 3.3 und 3.4 genannten Bereichen beteiligen.
- Unternehmen können sowohl (1) als Datennutzende Nachfrage für einen Datentreuhänder schaffen, (2) als Datengebende diese Daten zur Verfügung stellen, sie können aber auch (3) direkt durch finanzielle Beteiligung (z. B. über ein genossenschaftliches Modell) dessen Aufbau und Betrieb unterstützen.
- Im Sinne einer neuen **Kultur des Datenmanagements** könnten größere Unternehmen einen Beitrag zur Ankurbelung von Datenräumen leisten, indem sie intern anfallende Daten anschlussfähig machen (hierfür Verfügbarkeit und Qualität gewährleisten) und in sicheren Datenverarbeitungsumgebungen mit anderen Einrichtungen teilen, sofern Datenschutz und IT-Sicherheit gewährleistet sind.
- Unternehmen könnten einen wichtigen Beitrag zur Etablierung von Datentreuhändern leisten, indem sie sich aktiv an der **Entwicklung konkreter Anwendungsfälle** für wertschaffendes Datenteilen mittels dieser beteiligen. Indem sie entsprechende Potenziale aufzeigen und gemeinsam mit anderen Akteuren weiterentwickeln, können sie maßgeblich zur Etablierung tragfähiger Nutzungsszenarien beitragen.

4 Weiterer Forschungsbedarf und Ausblick

Die vorliegende Studie fasst Ergebnisse aus knapp drei Jahren Begleitforschung zu den BMFTR-geförderten Pilotprojekten im Bereich Datentreuhandmodelle zusammen. Dabei gibt es aus empirischer Perspektive viele unterschiedliche Entwicklungen in den einzelnen Pilotprojekten sowie außerdem noch unklare rechtliche und technisch-organisatorische Rahmenbedingungen, sodass die Ergebnisse kein vollumfängliches Bild zu Datentreuhändern liefern können. Aus Sicht der Begleitforschung gibt es einige weiterführende Fragen, die in Zukunft weiter beforscht werden sollten, damit Datentreuhänder erfolgreich etabliert und domänen- sowie sektorübergreifend skaliert werden können.

Unter dem Gesichtspunkt der Frage der **Akzeptanz für das Datenteilen** könnten folgende Aspekte näher untersucht und bewertet werden:

- Die Rolle von Datentreuhändern beim Zustandebringen von Beziehungen zwischen vormals sich unbekannten Datengebenden und -nutzenden als Beitrag zu einer neuen Kultur des Datenteilens und zur Initiierung und weiteren Entwicklung von Datenökosystemen. Daneben ist weitere Forschung zu **vertrauensbildenden Maßnahmen** wie Transparenzmechanismen, Rechenschaftspflichten und Beteiligungsformaten erforderlich.
- **Indikatoren für Gemeinwohlbeitrag**: Die Forschung sollte Bewertungsmaßstäbe für den gesellschaftlichen Nutzen von Datentreuhandmodellen erarbeiten.

Aus **technischer Perspektive** wäre es hilfreich, die folgenden Aspekte näher zu beforschen:

- Integration von föderiertem Lernen und Secure Multi-Party Computation (SMPC) in Datentreuhandkonzepte,
- Entwicklung von Mechanismen zur zuverlässigen Bewertung und Sicherung der Datenintegrität,
- verschiedene Ansätze zur Wahrung der optimalen Balance zwischen Datenschutz und Datennutzbarkeit,
- Förderung hybrider Datenhaltungskonzepte, die Vorteile zentraler und dezentraler Ansätze kombinieren,
- Kompatibilität zwischen verschiedenen Initiativen (z. B. zwischen SOLID und Gaia-X).

Im Hinblick auf die Entwicklung tragfähiger **Betriebsmodelle** für Datentreuhänder gibt die Empirie bislang allenfalls erste Indizien her. Insofern gibt es in diesem Bereich mehrere Fragestellungen, zu denen weitere Forschung dringend geboten erscheint. Insbesondere wären näher zu untersuchen:

- Das Thema Rechtsunsicherheit in Bezug auf zulässige Geschäftsmodelle (**Neutralitätsanforderung**). Gerade in domänenübergreifenden **Datenräumen** werfen Aspekte der Möglichkeit zum Angebot von Mehrwertdiensten zentrale Herausforderungen auf. Hierbei geht es neben reinen Diensten für die Datenbereinigung vor allem um Analyseangebote durch den Datentreuhänder.
- **Interaktion zwischen Rechtsformen und Geschäftsmodellen**: Die Auswirkungen unterschiedlicher Organisationsformen (z. B. Stiftung, Genossenschaft, Verein) auf Vertrauen, Effizienz und Skalierbarkeit müssen weiter erforscht werden. Zentral hierbei ist, dass Datentreuhänder dazu beitragen, den Nutzen des Datenteilens in spezifischen Anwendungsfällen klar zu benennen, so dass das Wert-Risiko-Dilemma für Datengebende und -nutzende überwunden werden kann. Hierfür müssen gangbare ökonomische Lösungen gefunden werden.
- **Bestimmung des geeigneten Betreibers und des optimalen Leistungsangebots in verschiedenen Domänen**: Über Anwendungsdomänen hinweg können sich Organisations- und Bepreisungsmodelle sowie die wahrgenommenen Funktionen unterschiedlich ausgestalten.

Wichtig für die weitere Forschung ist es aber auch, Ansätze zu identifizieren, die in einem solchen Ökosystem Interoperabilität und Skalierungschancen eröffnen.

- **Bepreisung von Daten und Finanzierungsmodellen**: Eine objektive Bestimmung des Werts von Daten und darauf aufbauend die Preisbildung für Datentreuhänderdienstleistungen ist ein ökonomisch bis heute nicht final gelöstes Problem. Insbesondere wenn sich diese Lösungen an der europäischen Regulierung orientieren sollen, lassen sich derzeit noch keine nachhaltigen Finanzierungsmodelle identifizieren.

Die oben aufgeworfenen Fragen werden zu einem großen Teil bereits empirisch in den durch das BMFTR in der zweiten bis vierten Förderrichtlinie geförderten Datentreuhänder-Projekten beforscht (BMFTR 2023a, BMFTR 2023b, BMFTR 2025b). Auch hier bietet sich eine projektübergreifende Begleitforschung an.

Die **Studienergebnisse leisten darüber hinaus auch einen Impuls zur Debatte über die Weiterentwicklung der Datenökonomie**. Auch wenn sich die Studienergebnisse explizit auf Datentreuhänder beziehen, könnten sie auch relevant sein in Bezug auf den Aufbau von Datenräumen im deutschen und europäischen Kontext, etwa im Kontext von Standardisierungsbestrebungen (vergleiche Moonen et al., 2025).[13] Die Ergebnisse sind auch vor dem Hintergrund der in Kapitel 2.1 eingeführten Debatte zur Bedeutung von Daten für den Aufbau europäisch geprägter KI-Lösungen relevant. Derzeit wird zudem verstärkt diskutiert, inwiefern Europa eigene Lösungen in den Bereichen KI, Cloud-Infrastruktur und Betriebssysteme aufbauen sollte („EuroStack", vergleiche Bria 2025). Zu guter Letzt wird derzeit auch auf europäischer Ebene die Bedeutung von Open-Source-Technologien und kritischer digitaler Infrastruktur für den Schutz digitaler Souveränität diskutiert (Gates et al. 2025). Auch in diesem Zusammenhang leistet die vorliegende Studie einen Beitrag, in dem er aufzeigt, wie Datentreuhänder beim Aufbau souveräner europäischer Datenökosysteme spielen können. Die ausgesprochenen Handlungsempfehlungen in Bezug auf die Anpassung des regulatorischen Rahmens für Datentreuhänder und Datenteilen leisten zudem einen Beitrag zu der durch den Draghi-Bericht aufgeworfenen Frage, wie die europäische Wirtschaft domänen- und sektorübergreifend im Bereich Datenteilen noch enger zusammenarbeiten kann, um so neue KI-Lösungen zu ermöglichen („AI Verticals", Draghi, 2004).

Abschließend lässt sich feststellen, dass die in der Studie identifizierten Herausforderungen aus Sicht der Begleitforschung zu meistern sind, und die Lösungsansätze erfolgreich zum Einsatz gebracht werden können, wenn politische Entscheidungsträger und öffentliche Verwaltung, Wissenschaft und Wirtschaft hier eng zusammenarbeiten. Unter dieser Voraussetzung können Datentreuhänder ihr Potenzial voll entfalten und einen wertvollen **Beitrag zum Aufbau von Datenökosystemen** leisten, mit entsprechenden positiven Wirkungen auf Innovation und Wertschöpfung in Deutschland und in Europa.

[13] Ein Überblick über Datentreuhand- und Datenrauminitiativen in Deutschland findet sich unter https://map.datnet.eu (zuletzt abgerufen am 1. August 2025).

Anhang A Literaturverzeichnis inkl. weiterführender Literatur

Acharya, S., & Mekker, M. (2022). Measuring data sharing intention and its association with the acceptance of connected vehicles. *Transportation Research Part F: Traffic Psychology and Behaviour, 89*, 423–436. https://doi.org/10.1016/j.trf.2022.07.014

Administrative Data Research Facilities Network. (2018). *Data sharing governance and management*. https://repository.upenn.edu/admindata_reports/2

Apple (o. J.). *Pop-Up-Werbung und Einblendfenster in Safari blockieren*. Abgerufen am 5. Juni 2025, von https://support.apple.com/de-de/102524

Arlinghaus, T., Kus, K., Kajüter, P., & Teuteberg, F. (2021). Datentreuhandstellen gestalten: Status quo und Perspektiven für Geschäftsmodelle. *HMD Praxis der Wirtschaftsinformatik, 58*(3), 565–579. https://doi.org/10.1365/s40702-021-00739-3

Arrow, K. J. (1991). An extension of the basic theorems of classical welfare economics. In K. J. Arrow & F. H. Hahn (Hrsg.), *General competitive analysis* (12. Aufl.) (S. 1–16). Wiley.

Arthur, B. W. (1989). Competing Technologies, Increasing Returns, and Lock-In by Historical Events. *The Economic Journal, 99*(394), 116–131. https://doi.org/10.2307/2234208

Beise, C. (2021). Datensouveränität und Datentreuhand. *Recht Digital, 2*, 597–600.

Blankertz, A. (2020). *Designing data trusts: Why we need to test consumer data trusts now*. Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/designing_data_trusts.pdf

Blankertz, A., Braunmühl, P. V., Kuzev, P., Richter, F., Richter, H., & Schallbruch, M. (2020). *Datentreuhandmodelle – Themenpapier*. MPG Publication Repository. https://pure.mpg.de/rest/items/item_3222478_2/component/file_3222479/content

Blankertz, A., & Specht-Riemenschneider, D. L. (2021). *Wie eine Regulierung für Datentreuhänder aussehen sollte*. Stiftung Neue Verantwortung. https://www.interface-eu.org/storage/archive/files/regulierung_fuer_datentreuhaender.pdf

Bowley, A. L. (1924). *Mathematical groundwork of economics*. Oxford University Press.

Bria, F., Timmers, P., & Gernone, F. (2025). *EuroStack – A European Alternative for Digital Sovereignty*. Bertelsmann Stiftung. https://doi.org/10.11586/2025006

Brown, C., Regan, A., & van der Burg, S. (2022). Farming futures: Perspectives of Irish agricultural stakeholders on data sharing and data governance. *Agriculture and Human Values, 40*, 565–580. https://doi.org/10.1007/s10460-022-10357-8

Bundesministerium der Justiz und für Verbraucherschutz (2025). *Konzeption einer bundeseinheitlichen Justizcloud*. Abgerufen am 5. Juni 2025, von https://www.bmj.de/DE/themen/digitales/digitalisierung_justiz/digitalisierungsinitiative/_articles/justizcloud_artikel.html

Bundesministerium für Bildung und Forschung (2021). *Bekanntmachung*. Richtlinie zur Förderung von Projekten zur Entwicklung und praktischen Erprobung von Datentreuhandmodellen in den Bereichen Forschung und Wirtschaft. *Bundesanzeiger vom 08.01.2021*. Abgerufen am 5. Juni 2025, von https://www.bmbf.de/bmbf/shareddocs/bekanntmachungen/de/2021/01/3292_bekanntmachung

Bundesministerium für Forschung, Technologie und Raumfahrt (2023). *Förderung von Projekten zur Skalierung und Akzeptanzsteigerung von intersektoralen Datentreuhandmodellen in der Praxis*. Abgerufen am 30. Juli 2025, von https://www.bildung-

forschung.digital/digitalezukunft/de/wissenschaft_und_forschung/datentreuhandmodelle/dtm-3-0/dtm-3-0_node.html.

Bundesministerium für Forschung, Technologie und Raumfahrt (2023). *Projektstart: 20 Vorhaben entwickeln Lösungsbausteine für Datentreuhandmodelle*. Abgerufen am 30. Juli 2025, von https://www.bildung-forschung.digital/digitalezukunft/de/wissenschaft_und_forschung/datentreuhandmodelle/dtm-2-0-projektvorstellung/dtm-2-0-projektvorstellung.html#:~:text=Ziel%20der%20Förderrichtlinie,maximal%20500.000%2C00%20EUR%20gefördert.

Bundesministerium für Forschung, Technologie und Raumfahrt (2025). *BMBF fördert Datentreuhänder - Pilotprojekte im Portrait*. Abgerufen am 25. Juni 2025, von https://www.bildung-forschung.digital/digitalezukunft/de/wissenschaft_und_forschung/datentreuhandmodelle/datentreuhandpioniere_im_portrait/datentreuhandpioniere_im_portrait.html?nn=249022

Bundesministerium für Forschung, Technologie und Raumfahrt (2025). *Förderung einer gelebten Kultur der organisations- und sektorenübergreifenden Datennutzung durch Datentreuhandmodelle*. Abgerufen am 30. Juli 2025, von https://www.bildung-forschung.digital/digitalezukunft/de/wissenschaft_und_forschung/datentreuhandmodelle/gelebte_datenkultur_durch_dtm/gelebte_datenkultur_durch_dtm_node.html.

Bundesministerium für Forschung, Technologie und Raumfahrt (2025). *Datentreuhandmodelle: BMBF fördert Pilotvorhaben*. Abgerufen am 25. August 2025, von https://www.bildung-forschung.digital/digitalezukunft/de/wissenschaft_und_forschung/datentreuhandmodelle/datentreuhandmodelle_pilotvorhaben/datentreuhandmodelle_pilotvorhaben_node.html

Bundesministerium für Wirtschaft und Klimaschutz (o. J.). *Label & Zertifizierungen rund um Datenschutz und Cloud*. Abgerufen am 5. Juni 2025, von https://www.trusted-cloud.de

Bria, F., Blankertz, A., Fernández-Monge, F., Gelhaar, J., Grafenstein, M. v., Haase, A., Kattel, R., Otto, B., Sagarra Pascual, O., & Rackow, L. (Hrsg.). (2023). *Governing urban data for the public interest*. The New Hanse Project Blueprint.

Bundesamt für Sicherheit in der Informationstechnik. (2021). *Eckpunktepapier für Self-sovereign Identities (SSI) unter besonderer Berücksichtigung der Distributed-Ledger-Technologie (DLT)*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Eckpunkte_SSI_DLT.pdf?__blob=publicationFile&v=2

Buchheim, J., Augsberg, S., & Gehring, P. (2022). Transaktionsbasierte Datentreuhand: Nutzungsszenarien, Kennzeichen und spezifische Leistungen eines neuen Modells gemeinsamer Datennutzung. *JuristenZeitung, 77*(23), 1139–1147.

Buchholtz, B., Brauneck, A., & Schmalhorst, L. (2023). Gelingensbedingungen der Datentreuhand – rechtliche und technische Aspekte. *Neue Zeitschrift für Verwaltungsrecht, 42*(4), 206–212.

Buchner, B., Haber, A., Hahn, H., Kusch, H., Prasser, F., Sax, U., & Schmidt, C. (2021). Das Modell der Datentreuhand in der medizinischen Forschung. *Datenschutz und Datensicherheit, 45*, 806–810. https://doi.org/10.1628/jz-2022-0368

Catena-X (o. J.). *Catena-X: Das erste offene und kollaborativ angelegte Datenökosystem*. Abgerufen am 5. Juni 2025, von https://catena-x.net/de/ueber-uns

Centre for Data Ethics and Innovation. (2021). *Unlocking the value of data: Exploring the role of data intermediaries*. https://www.gov.uk/government/publications/unlocking-the-value-of-data-exploring-the-role-of-data-intermediaries/unlocking-the-value-of-data-exploring-the-role-of-data-intermediaries.

Chavez, A. (2024, 22. April). Next steps for Privacy Sandbox and tracking protections in Chrome. *The Privacy Sandbox*. Abgerufen am 5. Juni 2025, von https://privacysandbox.com/news/privacy-sandbox-next-steps/

Chavez, A. (2024, 22. Juli). A new path for Privacy Sandbox on the web. *The Privacy Sandbox*. Abgerufen am 5. Juni 2025, von https://privacysandbox.com/news/privacy-sandbox-update/

Choi, W., Chang, S.-H., Yang, Y.-S., Jung, S., Lee, S.-J., Chun, J.-W., Kim, D.-J., Lee, W., & Choi, Y.I. (2022). Study of the factors influencing the use of MyData platform based on personal health record Data Sharing system. *BMC Medical Informatics and Decision Making*, 22(182). https://doi.org/10.1186/s12911-022-01929-z

Data Spaces Support Centre (2023). *Starter kit for data space designers*. Abgerufen am 5. Juni 2025, von https://dssc.eu/space/SK/29523973/Starter+Kit+for+Data+Space+Designers+%7C+Version+1.0+%7C+March+2023

DaTNet (2025). *Die Interaktive Datenraumlandkarte*. Abgerufen am 1. August 2025, von https://map.datnet.eu

Delacroix, S., & Lawrence, N. D. (2019). Bottom-up data trusts: Disturbing the 'one size fits all' approach to data governance. *International Data Privacy Law*, 9(4), 236–252. https://doi.org/10.1093/idpl/ipz014

Deutsche Industrie- und Handelskammer (o. J.-a). *Datenintermediär*. Abgerufen am 5. Juni 2025, von https://www.dihk.de/de/themen-und-positionen/wirtschaft-digital/dihk-durchblick-digital/datenintermediaer-89074

Deutsche Industrie- und Handelskammer (o. J.-b). *Datentreuhänder*. Abgerufen am 5. Juni 2025, von https://www.dihk.de/de/themen-und-positionen/wirtschaft-digital/dihk-durchblick-digital/datentreuhaender-86396

Draghi, M. (2024, 9. September). *The future of European competitiveness: A competitiveness strategy for Europe* (Part A). European Commission. Abgerufen am 15. Juli 2025. https://commission.europa.eu/document/97e481fd-2dc3-412d-be4c-f152a8232961_en

Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science*, 9(3–4), 211–407. https://doi.org/10.1561/0400000042

Element AI, & Nesta. (2019). *Data Trusts. A new tool for data governance*. https://evergreen.ca/resource-hub/wp-content/uploads/2019/07/elementai-data-trusts-july-2019.pdf

Europäischer Gerichtshof (2018, 10. Juli). Urteil in der Rechtssache C-25/17 – Zeugen Jehovas.

Europäischer Gerichtshof (2024, 7. März). Urteil in der Rechtssache C-604/22 – IAB Europe.

European Commission (o. J.). *EU register of data intermediation services*. Abgerufen am 7. August 2025, von https://digital-strategy.ec.europa.eu/en/policies/data-intermediary-services

European Commission (o. J.). *EU register of recognised data altruism organisations*. Abgerufen am 25. August 2025, von https://digital-strategy.ec.europa.eu/en/policies/data-altruism-organisations

European Union Agency for Cybersecurity, Hansen, M., Jensen, M., & Hoepman, J.-H. (2015). *Readiness analysis for the adoption and evolution of privacy enhancing technologies.* European Network and Information Security Agency. https://doi.org/10.2824/614444

EuroDaT. (2022). *Datensouveränität in vernetzten Ökosystemen. EuroDaT im Überblick*. https://www.eurodat.org/fileadmin/user_upload/Broschuere_EuroDaT.pdf

Forschungsdatenzentren (o. J.-a). Zugang zu den Mikrodaten. Abgerufen am 5. Juni 2025, von https://www.forschungsdatenzentrum.de/de/zugang

Forschungsdatenzentren (o. J.-b). Anonymität. Abgerufen am 5. Juni 2025, von https://www.forschungsdatenzentrum.de/de/anonymitaet

Fraunhofer ISST. (2022). *Anreizsysteme und Ökonomie des Data Sharings*. https://ieds-projekt.de/wp-content/uploads/2022/03/IEDS-Whitepaper-1.pdf

Future of Privacy Forum. (2017). Understanding Corporate Data Sharing Decisions: Practices, Challenges, and Opportunities for Sharing Corporate Data with Researchers. https://fpf.org/wp-content/uploads/2017/11/FPF_Data_Sharing_Report_FINAL.pdf

Gabler Wirtschaftslexikon (o. J.). *Datenmodellierung*. In Gabler Wirtschaftslexikon. Abgerufen am 5. Juni 2025, von https://wirtschaftslexikon.gabler.de/definition/datenmodellierung-51820/version-274971

Gal, M. S., & Rubinfeld, D. L. (2019). Data Standardization. *New York University Law Review 94*(4), 737–770.

Gates, N., Tridgell, J., Torraco, R. M., Schwäbe, C., Reda, F., Hummler, A., Streinz, T., Carlberg, A. N., Blind, K. A Study on the Economic, Legal and Political Feasibility of an EU Sovereign Tech Fund (EU-STF). https://eu-stf.openforumeurope.org/wp-content/uploads/2025/07/Funding-Europes-Open-Digital-Infrastructure.pdf

Gesmann-Nuissl, D., Tacke, I. M., & Meyer, S. (2024). „Stop it, Fridge!" – Legally Secure and Interest-Based Data Sharing in the Age of Modern (Cyber) Technology, *Journal of Universal Computer Science*, *30*(9), 1205–1223.

Grafenstein, M. v. (2022). *Reconciling Conflicting Interests in Data through Data Governance. An Analytical Framework*. HIIG Discussion Paper Series. https://zenodo.org/records/7390542.

Grafenstein, M. v. (2023). Why and how to mandate urban data sharing. In F. Bria, A. Blankertz, F. Fernández-Monge, J. Gelhaar, M. v. Grafenstein, A. Haase, R. Kattel, B. Otto, O. Sagarra Pascual, & L. Rackow (Hrsg.), *Governing urban data for the public interest* (S. 24–36). The New Hanse Project Blueprint. https://thenewhanse.eu/en

Grossman, R. L., Heath, A., Murphy, M., Patterson, M., & Wells, W. (2016). A case for data commons: Toward data science as a service. *Computing in Science & Engineering, 18*(5), 10–20. https://doi.org/10.1109/MCSE.2016.92

Grossman, R. L. (2018, 6. Juli). A proposed end-to-end principle for data commons. *Medium*. https://medium.com/@rgrossman1/a-proposed-end-to-end-principle-for-data-commons-5872f2fa8a47

Hennemann, M., & von Ditfurth, C. (2022). Datenintermediäre und Data Governance Act. *Neue Juristische Wochenschrift*, 1905–1908.

Houser, K. A., & Bagby, J. W. (2023). The data trust solution to data sharing problems. *Vanderbilt Journal of Entertainment and Technology Law, 25*(1), 113–180. https://scholarship.law.vanderbilt.edu/jetlaw/vol25/iss1/3

Hummel, P., Braun, M., Augsberg, S., Ulmenstein, U. Frhr. v., & Dabrock, P. (Hrsg.). (2021). *Datensouveränität*. Springer.

Huq, A. (2022). The public trust in data. *Georgetown Law Journal (110),* 333–402.

Kairouz, P., McMahan, H., Avent, B., Bellet, A., Bennis, M., Bhagoji, A., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R., D'Oliveira, R., Eichner, H., El Rouayheb, S., Evans, D., Gardner, J., Garrett, Z., Garcón, A., Ghazi, B., Gibbons, P., …, & Zhao, S. (2021). Advances and Open Problems in Federated Learning. *Foundations and Trends® in Machine Learning*, *14*(1–2), 1–210. https://doi.org/10.1561/2200000083

Kerber, W., & Gill, D. (2024). *The German Competition Case "Deutsche Bahn", Governance of Railway Mobility Data, and Data Trustee Solutions*. Social Science Research Network. https://doi.org/10.2139/ssrn.5125093

Knieps, G. (Hrsg.). (2008). *Wettbewerbsökonomie: Regulierungstheorie, Industrieökonomie, Wettbewerbspolitik* (3. Aufl.). Springer. https://doi.org/10.1007/978-3-540-78349-7

Köngeter, A., Schickhardt, C., Jungkunz, M., Bergbold, S., Mehlis, K., & Winkler, E. (2022). Patients'Willingness to Provide Their Clinical Data for Research Purposes and Acceptance of Different Consent Models: Findings From a Representative Survey of Patients With Cancer. *Journal of Medical Internet Research*, *24*(8). https://doi.org/10.2196/37665

Kühling J. (2021). Der datenschutzrechtliche Rahmen für Datentreuhänder. *Datenschutz und Datensicherheit, 45*, 783–788. https://doi.org/10.1007/s11623-021-1537-8

Kühling, J., Sackmann, F., & Schneider, H. (2020). *Datenschutzrechtliche Dimensionen Datentreuhänder*. IZA Institute of Labor Economics. https://ftp.iza.org/report_pdfs/iza_report_104.pdf

Kraemer, P., Niebel, C., & Reiberg, A. (2023). *Gaia-X und Geschäftsmodelle: Typen und Beispiele*. Gaia-X Hub Deutschland. https://gaia-x-hub.de/wp-content/uploads/2023/02/Whitepaper-Gaia-X-Geschaeftsmodelle.pdf

Kreutzer, S., Vogelsang, M., Dornbusch, F., & Heimer, T. (2022). *Wie Europa seine digitale Souveränität wiederherstellen kann*. Fraunhofer IMW. https://www.imw.fraunhofer.de/content/dam/moez/de/documents/220509_Thesenpapier_Digitale_Souver%C3%A4nit%C3%A4t_oeffentlich.pdf

Krotova, A., Rusche, C. & Spiekermann, M. (2019). *Die ökonomische Bewertung von Daten*. Institut der deutschen Wirtschaft. https://www.iwkoeln.de/fileadmin/user_upload/Studien/IW-Analysen/PDF/2019/Analyse129_Ökonomische_Bewerung_von_Daten.pdf

Kruse, L., & v. Grafenstein, M. (2025). Proprietary Data, Open Data, Data Commons: Who Owns the Data? How to Best Reconcile Conflicting Interests in Exploiting the Value of Data and Protecting Against its Risks. Social Science Research Network. http://dx.doi.org/10.2139/ssrn.5021150

Langford, J., Poikola, A., Janssen, W., Lähteenoja, V., & Rikken, M. (2020). *Understanding MyData Operators*. MyData Global. https://mydata.org/wp-content/uploads/2020/04/Understanding-Mydata-Operators-pages.pdf

Lau, J., Penner, J. & Wong, B. (2020). The basics of private and public data trusts. *Singapore Journal of Legal Studies*, 90–114.

Lauf, F., Scheider, S., Friese, J., Kilz, S., Radic, M., & Burmann, A. (2023). *Exploring Design Characteristics of Data Trustees in Healthcare - Taxonomy and Archetypes.* Thirty-first European Conference on Information Systems (ECIS 2023), Kristiansand, Norwegen. https://aisel.aisnet.org/ecis2023_rp/323

Lind, H.-G., & Suckfüll, H. (2013). *Die Initiative zu einer Deutschen Daten Treuhand (Dedate) als Ultima Ratio der persönlichen Digitalen Datenwirtschaft (PDD)*. Fraunhofer MOEZ. https://www.imw.fraunhofer.de/content/dam/moez/de/documents/Executive-Paper/DEDATE-gesamt.pdf

Lindner, M., & Straub, S. (2023). *Datentreuhänderschaft. Status quo und Entwicklungsperspektiven.* Institut für Innovation und Technik. https://www.iit-berlin.de/wp-content/uploads/2023/02/SDW_Datentreuhand.pdf

Lipovetskaja, A., Ciftci, S. A., Schweihoff, J., Janiesch, C., & Moeller, F. (2024). *Business Model Types for Data Trustees.* [Konferenzbeitrag]. 19th International Conference on Wirtschaftsinformatik, Würzburg, Deutschland.

Lomotey, R., Kumi, S., & Deters, R. (2022). Data Trusts as a Service: Providing a platform for multi-party Data Sharing. *International Journal of Information Management Data Insights*, *2*(1). https://doi.org/10.1016/j.jjimei.2022.100075

Marinotti, J. (2022). *Data Types, Data Doubts & Data Trusts.* Social Science Research Network. https://dx.doi.org/10.2139/ssrn.4058529

Martin, S., & Pasquale, W. (2019). *Exploring Data Trust Certifications*. Oxford Insights. https://theodi.cdn.ngo/media/documents/Report_-Exploring-Data-Trust-Certification.pdf

Medizin Informatik Initiative (o. J.) *Vernetzen. Forschen. Heilen.* Abgerufen am 5. Juni 2025, von https://www.medizininformatik-initiative.de/de/start

Mehta, S., Dawande, M., & Mookerjee, V. (2021, 2. August). Can data cooperatives sustain themselves? *LSE Business Review*. https://blogs.lse.ac.uk/businessreview/2021/08/02/can-data-cooperatives-sustain-themselves/

Meijer, A., & Potjer, S. (2018). Citizen-generated open data: An explorative analysis of 25 cases. *Government Information Quarterly, 35*(4), 613–621. https://doi.org/10.1016/j.giq.2018.10.004

Mills, S. (2019). *Who Owns the Future? Data Trusts, Data Commons, and the Future of Data Ownership.* Social Science Research Network. https://doi.org/10.2139/ssrn.3437936

Mobilty Data Space (o. J.). *Mobility Data Space: the data space for future mobility*. Abgerufen am 5. Juni 2025, von https://mobility-dataspace.eu

Mohr, S., & Cloos, J. (2022). Acceptance of Data Sharing in Smartphone Apps from Key Industries of the Digital Transformation: A Representative Population Survey for Germany. *Technology Forecasting and Social Change*, *176*. https://doi.org/10.1016/j.techfore.2021.121459

Moonen, N., Mollee, N., Wentzel, V., van den Born, A., Vossen, A. (2025). Sustainable Revenue Models for Data Sharing Initiatives. Abgerufen am 15. Juli 2025. https://open.overheid.nl/documenten/93097531-7897-408d-8d97-a9f9b3d2351b/file

Nabben, K. (2021). Decentralised Autonomous Organisations (DAOs) as Data Trusts: A General-purpose Data Governance Framework for Decentralised Data Ownership, Storage, and Utilisation. Social Science Research Network. Abgerufen am 15. Juli 2025. http://dx.doi.org/10.2139/ssrn.4009205

Nagel, L., & Douwe, L. (2021). *Design Principles for Data Spaces.* International Data Spaces Association. Abgerufen am 15. Juli 2025. https://doi.org/10.5281/zenodo.5244997

Nationale Forschungsdaten Infrastruktur (o. J.). *Sektion (Meta)daten, Terminologien, Provenienz.* Abgerufen am 5. Juni 2025, von https://www.nfdi.de/section-metadata/

Open Data Institute. (2019). *Data trusts: lessons from three pilots.* https://www.theodi.org/article/odi-data-trusts-report/

Open Knowledge Foundation (o. J.). *Open Definition 2.1*. Abgerufen am 5. Juni 2025, von http://opendefinition.org/od/2.1/en/

Otto, B., ten Hompel, M., & Wrobel, S. (Hrsg.). (2022). *Designing Data Spaces. The Ecosystem Approach to Competitive Advantage*. Springer. https://doi.org/10.1007/978-3-030-93975-5

Paprica, P. A., Sutherland, E., Smith, A., Brudno, M., Cartagena, R. G., Crichlow, M., Courtney, B. K., Loken, C., McGrail, K. M., Ryan, A., Schull, M. J., Thorogood, A., Virtanen, C., & Yang, K., (2020). Essential requirements for establishing and operating data trusts: practical guidance co-developed by representatives from fifteen Canadian organizations and initiatives. *International Journal of Population Data Science, 5*(1). https://doi.org/10.23889/ijpds.v5i1.1353

Poikola, A., Laszkowicz, P. J., Takanen, V., & Toivonen, T. (2023). *The technology landscape of data spaces*. SITRA. https://www.sitra.fi/app/uploads/2023/10/sitra-technology-landscape-of-data-spaces.pdf

Putnings, M. (2021). Datenökosystem. In: M. Putnings, H. Neuroth & J. Neumann (Hrsg.), *Praxishandbuch Forschungsdatenmanagement* (S. 7–10). Walter de Gruyter GmbH. https://doi.org/10.1515/9783110657807-001

Rat für Informationsinfrastrukturen. (2020) Stellungnahme des Rates für Informationsinfrastrukturen (RfII) Datentreuhandstellen gestalten – Zu Erfahrungen der Wissenschaft. https://d-nb.info/1209282283/34

Rat für Informationsinfrastrukturen. (2021). *Datentreuhänder: Potenziale, Erwartungen, Umsetzung*. Abgerufen am 15. Juli 2025. https://rfii.de/download/rfii-workshopbericht-datentreuhaender-potenziale-erwartungen-umsetzung-februar-2021/#

Reiberg, A., Appelt, D., Kraemer, P., & Smoleń, A. (2023). *Datentreuhänder, Datenvermittlungsdienste und Gaia-X*. Gaia-X Hub Deutschland. https://gaia-x-hub.de/wp-content/uploads/2024/02/WP-GX-Datentreuhaender.pdf

Richter, H. (2023). Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing. *GRUR Int., 72*(5), 458–470. https://doi.org/10.1093/grurint/ikad014

Rodrigues, N. (2022). CollMi: Technology for a more trustable and sustainable logistics value chain. I4Trust. https://i4trust.org/wp-content/uploads/CollMi-i4Trust-Impact-Story.pdf

Röhl, K.-H., Bolwin, L., & Hüttl, P. (2021). *Datenwirtschaft in Deutschland – Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse?* Institut der deutschen Wirtschaft. https://www.iwkoeln.de/studien/klaus-heiner-roehl-lennart-bolwin-wo-stehen-die-unternehmen-in-der-datennutzung-und-was-sind-ihre-groessten-hemmnisse.html

Ruhaak, A. (2022, 12. Mai). What is a data stewardship, and how could it address questions of power imbalance in the data economy? *Israel Public Policy Institute* https://www.ippi.org.il/what-is-data-stewardship-and-how-could-it-address-questions-of-power-imbalance-in-the-data-economy/

Rupp, V., & Grafenstein, M. v. (2024). Clarifying "personal data" and the role of anonymisation in data protection law: Including and excluding data from the scope of the GDPR (more clearly) through refining the concept of data protection. *Computer Law & Security Review*, *52*. https://doi.org/10.1016/j.clsr.2023.105932

Samaniego, M. (2018). *Data trust and IoT* [Konferenzbeitrag]. Proceedings of ACM Woodstrock conference (WOODSTOCK'18), New York, USA. https://doi.org/10.48550/arXiv.2205.14806

Scassa, T. (2020). Designing Data Governance for Data Sharing. Lessons from Sidewalk Toronto. *Technology and Regulation, 2020,* 44–56. https://doi.org/10.26116/techreg.2020.005

Schinke, L., & Roßmann, J. (2024). *Enabling Trustful Data Sharing in Industry 4.0 - A Comparison between Data Spaces, Data Markets and Other Related Concepts*. TechRxiv. https://doi.org/10.36227/techrxiv.172651024.46145536/v1

Schneider, I. (2022). *Datentreuhandschaft durch Intermediäre. Chancen, Herausforderungen und Implikationen.* Verbraucherzentrale NRW. https://www.verbraucherforschung.nrw/sites/default/files/2022-02/zth-2-schneider-datentreuhandschaft-durch-intermediaere.pdf

Schwartz, P., & Pfeiffer, K.-N. (2017). Datentreuhändermodelle - Sicherheit vor Herausgabeverlangen US-amerikanischer Behörden und Gerichte? *Computer und Recht, 33*(3), 165. https://doi.org/10.9785/cr-2017-0307

Simitis, S., Hornung, G., & Spiecker gen. Döhmann, I. (Hrsg.). (2021). *Datenschutzrecht* (2. Aufl.). C.H. Beck.

Specht-Riemenschneider, L., Blankertz, A., Sierek, P., Schneider, R., Knapp, J., & Henne, T. (2021). Die Datentreuhand. Ein Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierungserfordernisse für Datentreuhandmodelle. *Multimedia Recht*, *2021*, 25–47.

Specht Riemenschneider, L., & Kerber, W. (2022). *Datentreuhänder – Ein problemlösungsorientierter Ansatz.* Konrad-Adenauer-Stiftung. https://www.kas.de/de/einzeltitel/-/content/datentreuhaender-ein-problemloesungsorientierter-ansatz

Specht-Riemenschneider, L. (2024). Datenverarbeitung in sicheren Verarbeitungsumgebungen am Beispiel von MRT-Gehirnscans – zugleich ein Plädoyer für eine rechtssichere Forschungsgrundlage. *Bundesgesundheitsblatt,* 67, 180–188. https://doi.org/10.1007/s00103-023-03807-z

Stachon, M., Möller, F., Guggenberger, T., & Tomczyk, M. (2023). *Understanding Data Trusts* [Konferenzbeitrag]. Thirty-first European Conference on Information Systems (ECIS 2023), Kristiansand, Norwegen.

Stalla-Bourdillon, S. (2021). A Maturity Spectrum for Data Institutions. *IEEE Security & Privacy, 19*(5). https://doi.org/10.1109/MSEC.2021.3094985

Steinert, M., Tebernum, D., & Hupperz, M. (2024). *Design Features for Data Trustee Selection in Data Spaces* [Konferenzbeitrag]. Proceedings of the 13th International Conference on Data Science, Technology and Applications (DATA), Bilbao, Spanien. https://doi.org/10.5220/0012851400003756

Stevens, G., & Boden, A. (2022). Warum wir einen parteiische Datentreuhänder brauchen. Zum Modell der Datentreuhänderschaft als stellvertretende Deutung der Interessen individueller und kollektiver Identitäten. Verbraucherzentrale NRW. https://www.verbraucherforschung.nrw/sites/default/files/2022-02/zth-06-stevens-boden-warum-wir-parteiische-datentreuhaender-brauchen.pdf

Technopolis Group, Fraunhofer ISI, Law & Innovation, & RWTH Aachen (2024a). Wissenschaftliche Begleitung und Vernetzung der Projekte zur Entwicklung und praktischen Erprobung von Datentreuhandmodellen in den Bereichen Forschung und Wirtschaft. Arbeitspaket 1.1 Bestandsaufnahme. RWTH Aachen University. https://technopolis-group.com/wp-content/uploads/2024/04/BMBF-Datentreuhandmodelle-Begleitforschung-Bestandsaufnahme-1.pdf

Technopolis Group, Fraunhofer ISI, Law & Innovation, & RWTH Aachen (2024b). Wissenschaftliche Begleitung und Vernetzung der Projekte zur Entwicklung und praktischen Erprobung von Datentreuhandmodellen in den Bereichen Forschung und Wirtschaft. Arbeitspaket 1.2 Anforderungen und Umsetzungshemmnisse für Datentreuhandmodelle. RWTH Aachen University. https://technopolis-group.com/wp-content/uploads/2024/04/BMBF-Datentreuhandmodelle-Begleitforschung-Umsetzungshemmnisse-1.pdf

The Royal Society. (2019). *Protecting privacy in practice. The current use, development and limits of Privacy Enhancing Technologies in data analysis*. https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/Protecting-privacy-in-practice.pdf

Ulmenstein, U. Frhr. v. (2020). Datensouveränität durch repräsentative Rechtswahrnehmung. Begriffliche Prägung und normative Gestaltung sog. „Datentreuhänder". *Datenschutz und Datensicherheit, 44*(8), 528–534. https://doi.org/10.1007/s11623-020-1319-8

Verbraucherzentrale Bundesverband. (2020). *Datenintermediäre gesetzlich regeln*. Positionspapier des vzbv zu Datenintermediären. https://www.vzbv.de/publikationen/datenintermediaere-gesetzlich-regeln

Wernick, A., Olk, C., & Grafenstein, M. v. (2020). Defining Data Intermediaries. *Technology and Regulation*, 65–77. https://doi.org/10.71265/fk0zcq05

Yoon, A., & Lee, Y.Y. (2019). Factors of trust in data reuse. *Online Information Review*, *43*(7), 1245–1262. https://doi.org/10.1108/OIR-01-2019-0014

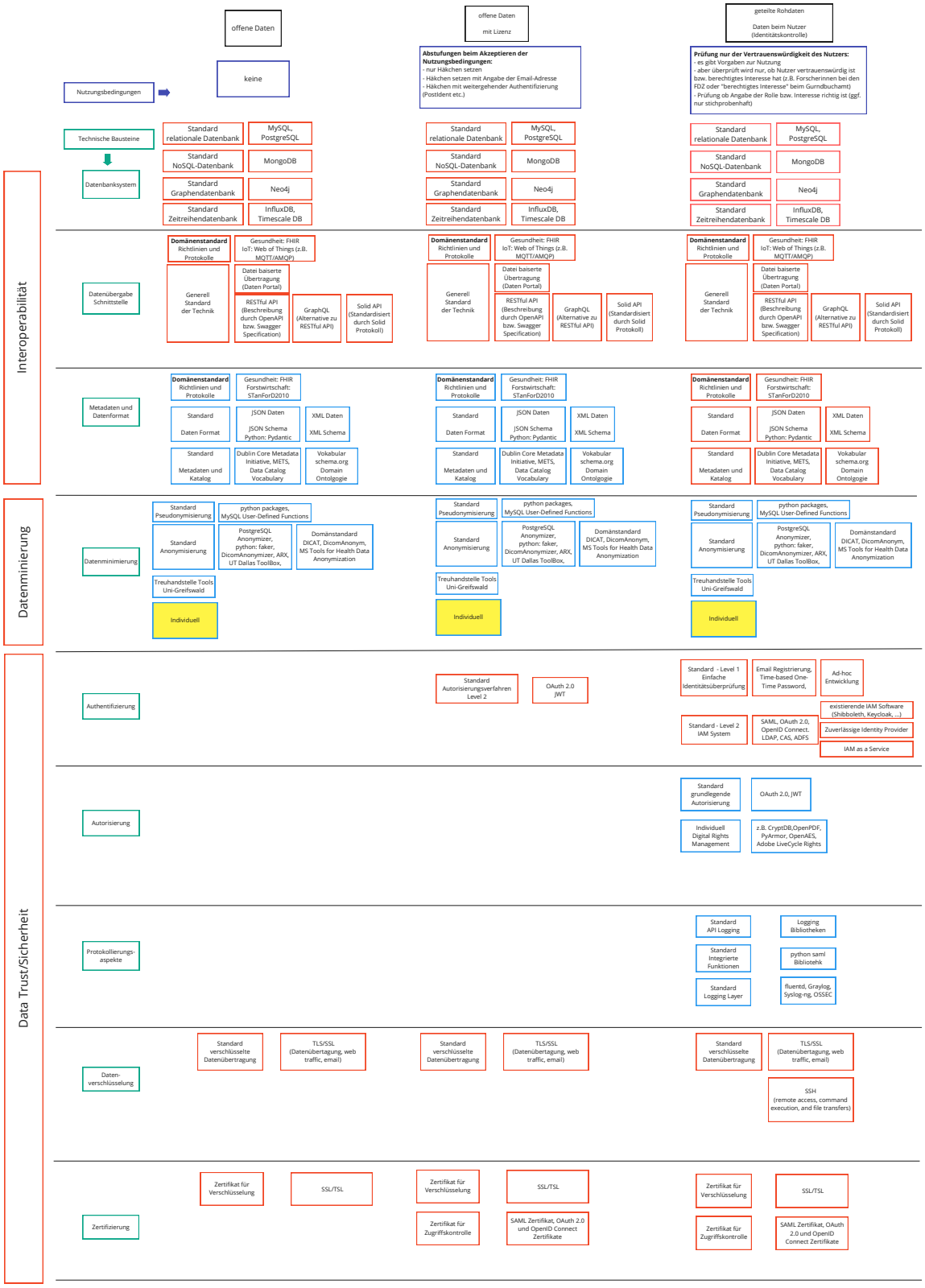
Young, M., Rodriguez, L., Keller, E., Sun, F., Sa, B., Whittington, J., & Howe, B. (2019). *Beyond Open vs. Closed: Balancing Individual Privacy and Public Accountability in Data Sharing*. FAT* '19: Proceedings of the Conference on Fairness, Accountability, and Transparency. https://doi.org/10.1145/3287560.3287577

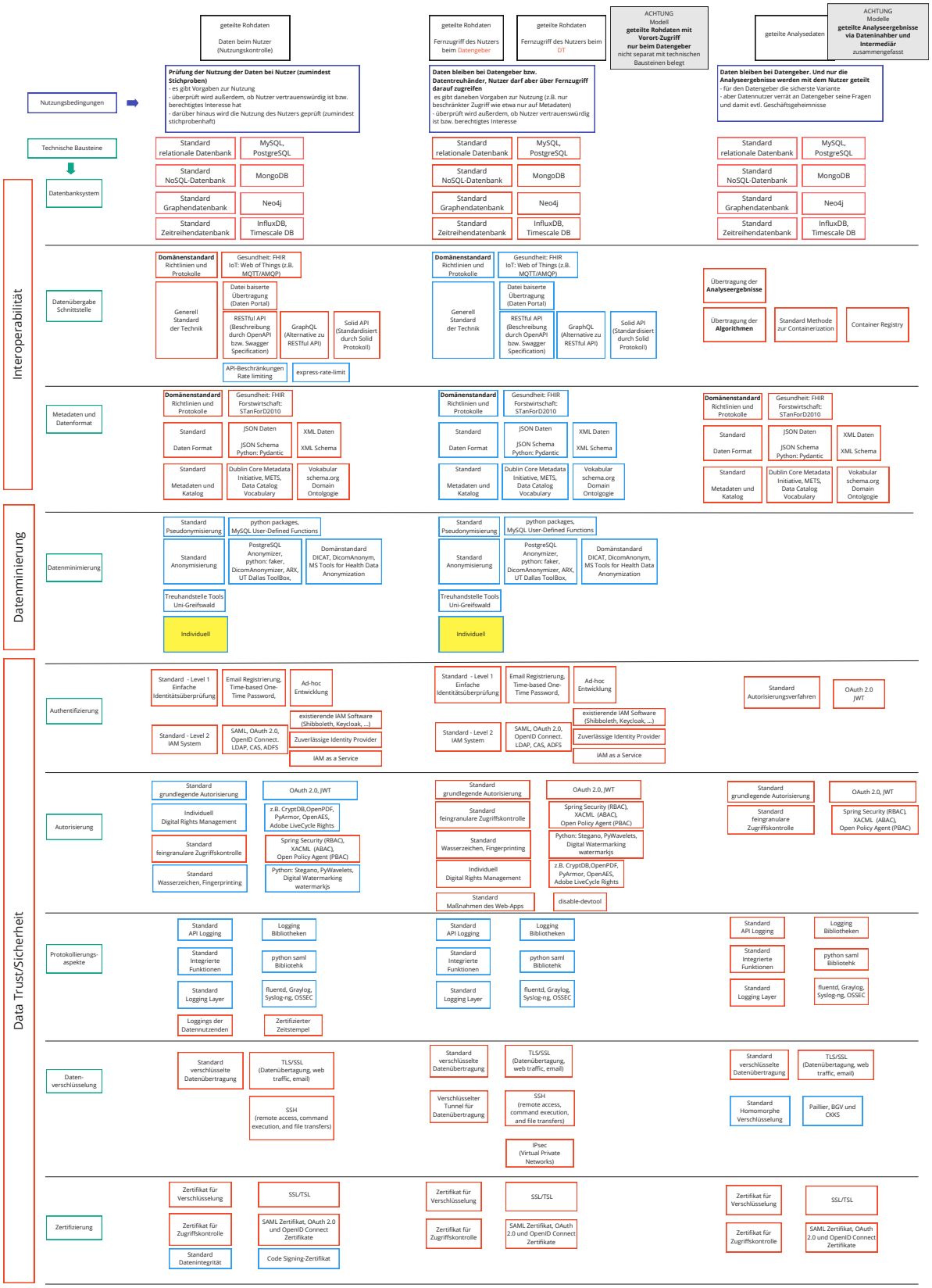
Zhang (2021). A commentary of Data trusts. *MIT Technology Review*, *1*(6), 834–835. https://doi.org/10.1016/j.fmre.2021.11.016

Zrenner J., Möller, F. O., Jung, C., Eitel, A., & Otto, B. (2019). Usage control architecture options for data sovereignty in business ecosystems. *Journal of Enterprise Information Management, 32*(3), 477–495. https://doi.org/10.1108/JEIM-03-2018-0058

Anhang B Framework des technischen Baukastens

Eine detaillierte Ansicht des technischen Baukastens findet sich unter https://ebc-tools.eonerc.rwth-aachen.de/.




Interoperabilität
Datenminimierung
Data Trust/Sicherheit
Nutzungsbedingungen
Technische Bausteine
Datenbanksystem
Datenübergabe Schnittstelle
Metadaten und Datenformat
Datenminimierung
Authentifizierung
Autorisierung
Protokollierungs-aspekte
Daten-verschlüsselung
Zertifizierung
geteilte Rohdaten
Daten beim Nutzer (Nutzungskontrolle)
geteilte Rohdaten
Fernzugriff des Nutzers beim Datengeber
geteilte Rohdaten
Fernzugriff des Nutzers beim DT
ACHTUNG Modell geteilte Rohdaten mit Vorort-Zugriff nur beim Datengeber nicht separat mit technischen Bausteinen belegt
geteilte Analysedaten
ACHTUNG Modelle geteilte Analyseergebnisse via Dateninhaber und Intermediär zusammengefasst
Prüfung der Nutzung der Daten bei Nutzer (zumindest Stichproben)
- es gibt Vorgaben zur Nutzung
- überprüft wird außerdem, ob Nutzer vertrauenswürdig ist bzw. berechtigtes Interesse hat
- darüber hinaus wird die Nutzung des Nutzers geprüft (zumindest stichprobenhaft)
Daten bleiben bei Datengeber bzw. Datentreuhänder, Nutzer darf aber über Fernzugriff darauf zugreifen
es gibt daneben Vorgaben zur Nutzung (z.B. nur beschränkter Zugriff wie etwa nur auf Metadaten)
- überprüft wird außerdem, ob Nutzer vertrauenswürdig ist bzw. berechtigtes Interesse
Daten bleiben bei Datengeber. Und nur die Analyseergebnisse werden mit dem Nutzer geteilt
- für den Datengeber die sicherste Variante
- aber Datennutzer verrät an Datengeber seine Fragen und damit evtl. Geschäftsgeheimnisse
Standard relationale Datenbank
MySQL, PostgreSQL
Standard NoSQL-Datenbank
MongoDB
Standard Graphendatenbank
Neo4j
Standard Zeitreihendatenbank
InfluxDB, Timescale DB
Domänenstandard Richtlinien und Protokolle
Gesundheit: FHIR IoT: Web of Things (z.B. MQTT/AMQP)
Generell Standard der Technik
Datei baiserte Übertragung (Daten Portal)
RESTful API (Beschreibung durch OpenAPI bzw. Swagger Specification)
GraphQL (Alternative zu RESTful API)
Solid API (Standardisiert durch Solid Protokoll)
API-Beschränkungen Rate limiting
express-rate-limit
Übertragung der Analyseergebnisse
Übertragung der Algorithmen
Standard Methode zur Containerization
Container Registry
Gesundheit: FHIR Forstwirtschaft: STanForD2010
Standard Daten Format
JSON Daten
JSON Schema Python: Pydantic
XML Daten
XML Schema
Standard Metadaten und Katalog
Dublin Core Metadata Initiative, METS, Data Catalog Vocabulary
Vokabular schema.org Domain Ontologie
Standard Pseudonymisierung
python packages, MySQL User-Defined Functions
Standard Anonymisierung
PostgreSQL Anonymizer, python: faker, DicomAnonymizer, ARX, UT Dallas ToolBox,
Domänstandard DICAT, DicomAnonym, MS Tools for Health Data Anonymization
Treuhandstelle Tools Uni-Greifswald
Individuell
Standard - Level 1 Einfache Identitätsüberprüfung
Email Registrierung, Time-based One-Time Password,
Ad-hoc Entwicklung
Standard - Level 2 IAM System
SAML, OAuth 2.0, OpenID Connect. LDAP, CAS, ADFS
existierende IAM Software (Shibboleth, Keycloak, ...)
Zuverlässige Identity Provider
IAM as a Service
Standard Autorisierungsverfahren
OAuth 2.0 JWT
Standard grundlegende Autorisierung
OAuth 2.0, JWT
Individuell Digital Rights Management
z.B. CryptDB,OpenPDF, PyArmor, OpenAES, Adobe LiveCycle Rights
Standard feingranulare Zugriffskontrolle
Spring Security (RBAC), XACML (ABAC), Open Policy Agent (PBAC)
Standard Wasserzeichen, Fingerprinting
Python: Stegano, PyWavelets, Digital Watermarking watermarkjs
Standard Maßnahmen des Web-Apps
disable-devtool
Standard API Logging
Logging Bibliotheken
Standard Integrierte Funktionen
python saml Bibliotehk
Standard Logging Layer
fluentd, Graylog, Syslog-ng, OSSEC
Loggings der Datennutzenden
Zertifizierter Zeitstempel
Standard verschlüsselte Datenübertragung
TLS/SSL (Datenübertagung, web traffic, email)
SSH (remote access, command execution, and file transfers)
Verschlüsselter Tunnel für Datenübertragung
IPsec (Virtual Private Networks)
Standard Homomorphe Verschlüsselung
Paillier, BGV und CKKS
Zertifikat für Verschlüsselung
SSL/TSL
Zertifikat für Zugriffskontrolle
SAML Zertifikat, OAuth 2.0 und OpenID Connect Zertifikate
Standard Datenintegrität
Code Signing-Zertifikat

Anhang C Liste der Pilotprojekte der ersten Förderrichtlinie

Name	Laufzeit	Domäne	Konsortialpartner	Weiterführende Links
BreedFides: Entwicklung eines nachhaltigen Datenökosystems für die Pflanzenzüchtung	01.01.2022 bis 31.12.2024	Pflanzenzüchtung	• Leibniz-Institut für Pflanzengenetik und Kulturpflanzenforschung • Gemeinschaft zur Förderung von Pflanzeninnovation e.V. • Julius Kühn-Institut • Johann Heinrich von Thünen-Institut • Vereinigte Informationssysteme Tierhalten w.V.	• Projektinformationen
DaRe: GesundheitsDAtentreuhand-REallabor zur Entwicklung und Erprobung der Ökosystemintegration datengetriebener Gesundheitsforschung	11.2022 bis 01.2025	Gesundheit	• Fraunhofer-Institut für Software- und Systemtechnik • Fraunhofer-Zentrum für Internationales Management und Wissensökonomie • Friedrich-Wilhelms-Universität Bonn • Universitätsklinik Bonn	• Projektinformationen
DaTHMed-LSA: Datentreuhandverb und biomedizinische Forschungsdaten Land Sachsen-Anhalt	01.01.2022 bis 31.12.2024	Gesundheit	• Otto-von-Guericke Universität Magdeburg • Martin-Luther-Universität Halle-Wittenberg	• Projektinformationen
DaTreFo: Datentreuhänder mit verschlüsselten Datenschätzen für die Forschung	01.11.2021 bis 31.11.2024	übergreifend	• Hochschule Trier • Deutsches Forschungszentrum für künstliche Intelligenz GmbH • Dedalus HealthCare GmbH • Duria eG	• Projektinformationen
Ddtrust: Dresden Data Trust Center	01.01.2022 bis 31.12.2024	Forschung	• Technische Universität Dresden • Papiertechnische Stiftung	• Projektinformationen • Interview
DEFENSIVE: Datentreuhänder Plattform zum dezentralen Austausch von IT-Sicherheitsvorfälle	01.07.2022 bis 30.06.2025	IT-Sicherheit	• Universität Regensburg • DFN-CERT Services GmbH	• Projektinformationen

FAIRWinDS: Findable, Accessible, Interpretable and Reusable Wind energy data in Data Spaces	01.01.2022 bis 31.12.2023	Energie	• Fraunhofer-Institut für Windenergiesysteme • Fraunhofer-Institut für Intelligente Analyse-und Informationssysteme • Fraunhofer-Institut für Energiewirtschaft und Energiesystemtechnik • Fraunhofer-Zentrum für Internationales Management und Wissensökonomie • Fraunhofer-Institut für Software- und Systemtechnik	• Projektinformationen • Interview
KickStartTrustee: Entwicklung eines branchenunabhängigen Frameworks für zielgerichtete Konzeption, beschleunigte Umsetzung und erfolgreichen Betrieb von Datentreuhändern	01.01.2022 bis 31.12.2023	übergreifend	• Fraunhofer-Institut für experimentelles Software Engineering	• Projektinformationen • Interview
KomDatTIS: Kommunale Datentreuhänder – Integration von Bürgern und Unternehmen zum souveränen Austausch von Daten in der Smart City	01.2021 bis 12.2024	Smart City	• Technische Universität Dortmund • Fraunhofer Institut für Software- und Systemtechnik • Daten-Kompetenzzentrum für Städte und Regionen	• Projektinformationen
LuftDatenNet	01.01.2022 bis 31.12.2024	Umweltschutz	• Breeze Technologies UG	• Projektinformationen
MANDAT: Methoden zum Austausch von unternehmensbezogenen Daten in treuhänderbasierten Datenökosystemen	01.2022 bis 12.2024	Wirtschaft	• Friedrich-Alexander-Universität Erlangen-Nürnberg • Karlsruher Institut für Technologie • DATEV eG	• Projektinformationen
MobiDataSol: Intelligente Datenprodukte für die Urbane Mobilitätswende mittels Ökosystem Data Governance in der Smart City Solingen	01.2022 bis 03.2024	Smart City	• Fraunhofer-Institut für Arbeitswirtschaft und Organisation • Universität Stuttgart • Institut für Energie- und Umweltforschung Heidelberg gGmbH • Fraunhofer-Institut für Software und Systemtechnik	• Projektinformationen • Interview

S3I-X: 3SI Trusted Data Exchange and Analytics	11.2021 bis 11.2024	Forst- und Holzwirtschaft	• RIF Institut für Forschung und Transfer e. V. • Institut für Mensch-Maschine-Interaktion • ComConsult GmbH • nexoma GmbH	• Projektinformationen • Interview
SouveMed: Vertrauenswürdiges Datentreuhandmodell zur souveränen Verwaltung und effektiven Nutzung von medizinischen Daten in der Schlafforschung	01.01.2022 bis 31.12.2023	Gesundheit	• Forschungszentrum Informatik • Universitätsklinikum Freiburg • Hochschule für Technik und Wirtschaft Berlin	• Projektinformationen • Interview
TRANSIT: Data Trusts for Enhancing Logistics Collaboration	01.2022 bis 06.2024	Logistik	• Universität Leipzig • Institut für Angewandte Informatik e. V. • fox-COURIER GmbH	• Projektinformationen
TRESOR: Treuhandplattform für die sichere und privatsphäreschützende Sammlung, Speicherung und Vermittlung von Daten mobiler Geräte	01.01.2022 bis 31.12.2024	übergreifend	• Hamburger Informatik Technologie-Center e. V. • umlaut solutions GmbH • Universität Hamburg	• Projektinformationen
TreuMed: Entwicklung und Erprobung von Datentreuhandmodellen am Beispiel der verteilten künstlichen Intelligenz in der Medizin	11.2021 bis 10.2024	Gesundheit	• Universität Hamburg • ePrivacy GmbH • Universität Greifswald	• Projektinformationen
TreuMoDa: Konzeptionierung und prototypische praxisnahe Erprobung einer Treuhandstelle für Mobilitäts-Daten im Anwendungsfeld Automatisiertes Fahren unter Nutzung des Testfelds für Autonomes Fahren Baden-Württemberg	01.01.2022 bis 31.12.2023	Mobilität	• Karlsruher Institut für Technologie • Leibniz-Institut für Informationsinfrastruktur • Forschungszentrum Informatik	• Projektinformationen • Interview

TrustDNA: Datenschutzrechtliches Reallabor für eine Datentreuhand in der Netzwerkmedizin	01.2022 bis 06.2024	Gesundheit	• Heidelberger Akademie der Wissenschaften • European Molecular Biology Laboratory • Charité-Universitätsmedizin	• Projektinformationen
TrustNShare: Partizipativ entwickeltes, Smart-contract basiertes Datentreuhandmodell mit skalierbarem Vertrauen und Inzentivierung	01.01.2022 bis 31.12.2024	übergreifend	• Universitätsklinikum Jena • DLR Institut für Datenwissenschaften • Institut für Digitale Medizin	• Projektinformationen • Interview

Die Begleitforschung bedankt sich herzlich für die Teilnahme der Vertreterinnen und Vertreter der Pilotprojekte an den empirischen Erhebungen.

Anhang D Liste von untersuchten externen Anwendungsfällen

Anwendungsfall	Gründung	Sektor	Verantwortliche Organisation(en)
Catena-X	2020	Automobilindustrie	133 Unternehmen der Automobilindustrie unter dem Dach des Catena-X Automotive Network e.V.
EuroDaT	2022	Finanzwirtschaft	Das EuroDaT Konsortium besteht aus Atos, d-fine, Deloitte, Deutsches Forschungszentrum für Künstliche Intelligenz, Goethe-Universität Frankfurt, Hessisches Ministerium für Wirtschaft, Energie, Verkehr und Wohnen, Lexemo, TechQuartier, T-Systems, Universität des Saarlandes und dem Zentrum Verantwortungsbewusste Digitalisierung (ZEVEDI). Das EuroDaT Konsor:um wird von d-fine als Konsortialführer koordiniert.
Evarest	2019	Lebensmittelindustrie, Agrarindustrie	DFKI (Konsortialführer), Lebensmittelunternehmen und Forschungsinstitutionen
Forschungs-datenzentren	2001	Forschung	Statistische Ämter des Bundes und der Länder
i4Trust	2020	Logistik, Energie, Landwirtschaft und Smart-City	Die i4Trust-Initiative ist ein von der Europäischen Union (EU) finanziertes Projekt zur Entwicklung einer vertrauenswürdigen und sicheren Rahmenstruktur für den Datenaustausch zwischen verschiedenen Organisationen in unterschiedlichen Branchen. I4Trust besteht aus zwei Hauptorganisationen, FIWARE Foundation und iShare Foundation.
UK Biobank	2006	Medizin	UK Biobank Limited

Anhang E Mitglieder des Projektbeirats

- Prof. Dr. Wolfgang Kerber, Universität Marburg
- Dr. Manuela Urban, COO Sovereign Cloud Stack
- Dr. Hilko Hoffmann, Deutsches Forschungszentrum für Künstliche Intelligenz
- Rebekka Weiß, Bitkom-Verband (bis 2023)
- Hauke Timmermann, eco-Verband der Internetwirtschaft (ab 2024)

Die Begleitforschung bedankt sich herzlich bei der Mitgliedern des Beirats für die fortlaufende fachliche Unterstützung im Rahmen der Begleitforschung.

Anhang F Liste der interviewten Expertinnen und Experten

- Tim Arlinghaus, Universität Osnabrück
- Steffen Biehs, Fraunhofer Software- und Systemtechnik
- Volker Berkhout, Fraunhofer-Institut für Energiewirtschaft und Energiesystemtechnik
- Olivier Dion, Themis X
- Stefan Faulstich, Fraunhofer-Institut für Energiewirtschaft und Energiesystemtechnik
- Marc Fliehe, TÜV-Verband
- Prof. Thomas Ganslandt, Friedrich-Alexander-Universität
- Marit Hansen, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
- Jack Hardinges, Open Data Institute London
- Rosemarie Hinsch, Bundesdruckerei GmbH
- Prof. Jürgen Kühling, Universität Regensburg
- Jens Knodel, Caruso GmbH
- Dr. Torsten Leddig, Universitätsmedizin Greifswald
- Lars Nagel, International Data Spaces Association
- Arno Pons, Themis X
- Michael Schäfer, Mobility Data Space
- Michael Schidlack, Zentralverband für Elektro- und Digitalindustrie
- Prof. Ingrid Schneider, Universität Hamburg
- Jaana Sinipuro, Data Space Europe
- Prof. Louisa Specht-Riemenschneider, Universität Bonn
- Dana Stahl, Unabhängige Treuhandstelle der Universitätsmedizin Greifswald
- Dr. Stefan Weisgerber, Deutsches Institut für Normung
- Dr. Dennis Wendland, FIWARE Foundation

Die Begleitforschung bedankt sich herzlich für die Teilnahme der Expertinnen und Experten an den Interviews.

technopolis group

www.technopolis-group.com