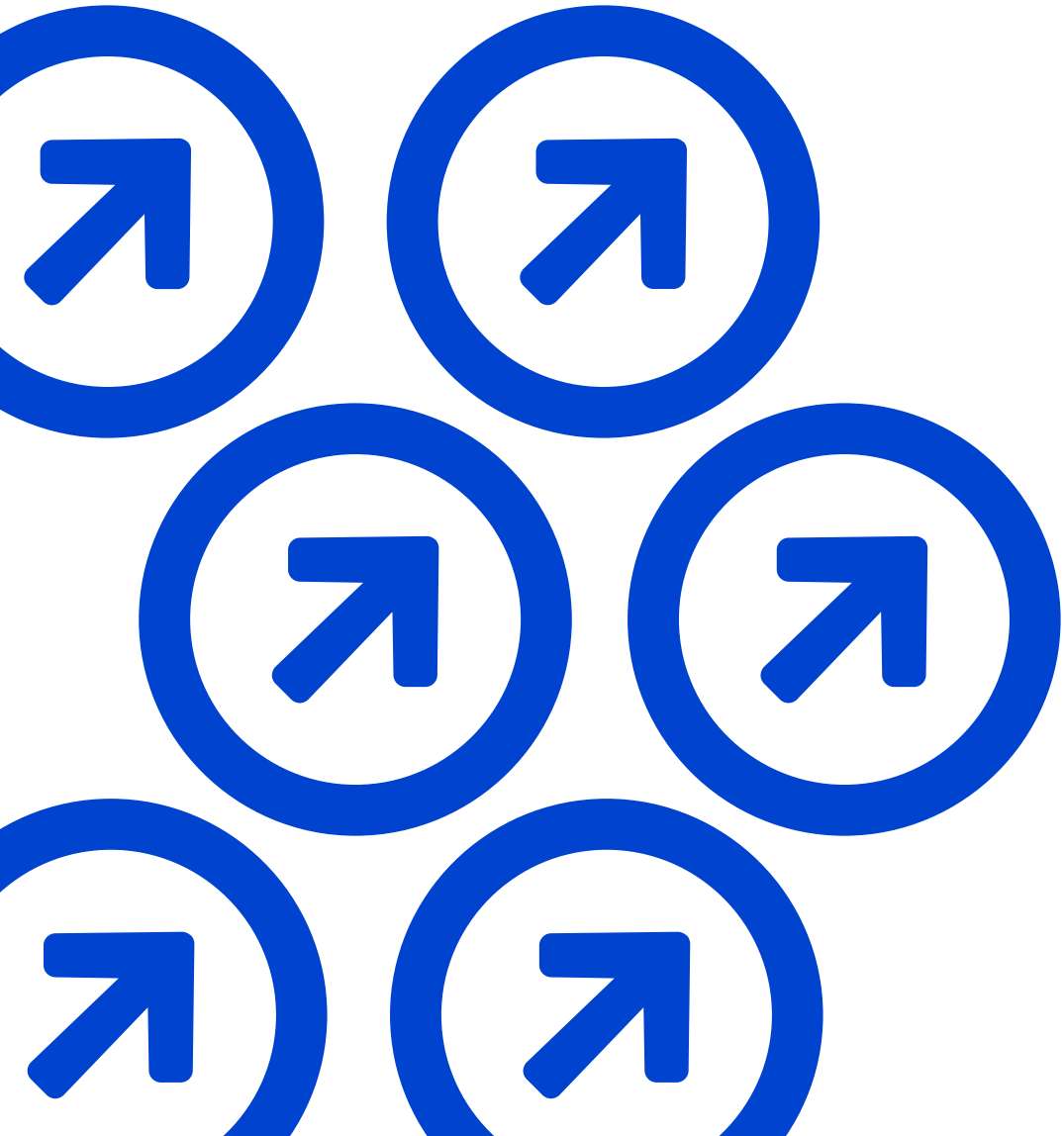
SmartLivingNEXT

Kompendium zur Datentreuhänderschaft



Inhaltsverzeichnis

Abbildungsverzeichnis

Impressum

Herausgeber

Lea Rabe, Thomas Heimer, Jenny Glöckner
Technopolis Group
Frankfurt am Main/Berlin
März 2025

Diese Studie wurde im Rahmen der Begleitforschung zum Programm *SmartLivingNEXT – Künstliche Intelligenz für nachhaltige Lebens- und Wohnumgebungen* des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) beauftragt.

Design

PRpetuum GmbH

BEGLEITFORSCHUNG

INSTITUT FÜR INNOVATION UND TECHNIK technopolis group PRP

Executive Summary

Mit der steigenden Digitalisierung wächst die Verfügbarkeit von Daten sowie deren Nutzungschance für Unternehmen und Private. Für die Wettbewerbsfähigkeit von Unternehmen, insbesondere KMU, spielt die zunehmende Möglichkeit umfangreicher Datenanalysen in einem Datenraum eine entscheidende Rolle, etwa um Entscheidungsprozesse zu verbessern, innovative Produkte und Dienstleistungen zu entwickeln oder effizientere Geschäftsprozesse zu gestalten. Der Datenaustausch in einem Datenraum erfordert aber auch ständige Abfragen, ob die jeweils erforderlichen Informationen verfügbar sind und die jeweiligen Zugriffsrechte vorliegen. Zur Regelung des Datenaustauschs bedarf es eines neutralen und vertrauenswürdigen Intermediärs, wie z.B. eines Datentreuhänders, der diese Rolle zwischen den Datengebern und -nutzern ausübt. Das vorliegende Kompendium befasst sich mit der Problemstellung, welche rechtlichen und wirtschaftlichen Anforderungen an einen solchen Intermediär zu stellen sind. Insbesondere die Anforderungen an Datentreuhänder, deren Funktionen, die relevanten Regulierungsansätze und die Ansätze für Geschäftsmodelle werden intensiver betrachtet.

Die Analyse zeigt, dass die zentrale Herausforderung für einen Datentreuhänder in dem Wert-Risiko-Dilemma zu sehen ist. Dieses resultiert aus der Befürchtung von Privaten, dass ihre Daten missbräuchlich genutzt werden und der Unternehmen, dass sensible firmenspezifische Daten Konkurrenten zugänglich werden. Der Ansatz des Datentreuhänders bietet eine Lösung des Wert-Risiko-Dilemmas an, indem er als neutrale Institution zwischen den beiden Akteursgruppen agiert. Hierfür muss der Datentreuhänder sowohl die rechtlichen als auch die technologischen Anforderungen an eine neutrale Vermittlung beachten.

Hinsichtlich der Ausgestaltung einzelner Funktionen können Datentreuhänder variieren. Dass ein Datentreuhänder beispielsweise für die Qualitätssicherung der zu vermittelten Daten zuständig ist, kann bedeuten, dass er die Datensätze „nur“ auf fehlende Bestandteile prüft. In einem umfangreicheren Ansatz der Qualitätssicherung nimmt er eine logische Prüfung vor und kontrolliert, ob die Datensätze schlüssig sind. Auf der umfassendsten Stufe der Qualitätssicherung könnte der Datentreuhänder nach dem Entdecken von Unregelmäßigkeiten auf den Datengeber zurückkommen, um gemeinsam mit ihm Auffälligkeiten in den Datensätzen zu klären und zu beheben.

Die rechtlichen Rahmenbedingungen für Datentreuhänder wurden in den letzten Jahren ausgebaut. Zentral ist dabei die Datenschutz-Grundverordnung (DSGVO), die seit 2018 den Schutz personenbezogener Daten und die Rechte von Bürgerinnen und Bürgern stärkt. Ergänzend wurden im Rahmen der Europäischen Datenstrategie der Data Governance Act (DGA) und der Data Act (DA) eingeführt, um fairen Wettbewerb zu gewährleisten, den Zugang zu Daten zu verbessern und die Nutzung von Daten zu fördern. Die Regulierung von Datentreuhändern hat aber auch tiefgreifende Auswirkungen auf die Entwicklung von Geschäftsmodellen in diesem Bereich: Eine der größten Herausforderungen für Datentreuhänder besteht in der Balance zwischen dem Schutz der Privatsphäre und der Schaffung von Mehrwert durch Daten. Denn die Regulierungen beeinflussen sowohl die wirtschaftlichen Rahmenbedingungen als

auch die Art und Weise, wie Datentreuhänder ihre Leistungen anbieten und Vertrauen bei Datengebern und -nutzern aufbauen können. Aktuelle Regulierungsvorhaben werden deshalb von Rechtsexpertinnen und -experten als hinderlich wahrgenommen, weil sie den Handlungsspielraum von Unternehmen und Organisationen einschränken, als Datentreuhänder aktiv zu werden.

Bis heute ist empirisch noch kein marktgängiges Geschäftsmodell für Datentreuhänder auffindbar. Geschäftsmodelle werden zwischen unterschiedlichen Anwendungsfällen variieren. Institutionelle Modelle erscheinen besonders dann sinnvoll, wenn eine starke öffentliche Unterstützung erforderlich oder ein staatliches Eingreifen sogar wünschenswert ist, etwa in Märkten mit geringer Wettbewerbsintensität oder hoher Marktmacht einzelner Akteure. Mitgliedsorientierte Modelle bieten sich aufgrund ihres hohen Koordinationsaufwands eher für bereits gut etablierte Netzwerke an. Unternehmensmodelle sind geeignet, wenn eine hohe Agilität und eine schnelle Anpassung an Markterfordernisse notwendig sind, beispielsweise in dynamischen Märkten, in denen Innovationen und Monetarisierungspotenziale im Vordergrund stehen, jedoch können die hohen Anfangsinvestitionen und rechtliche Unsicherheiten eine Herausforderung darstellen. Insgesamt ist aber auch festzustellen, dass die bestehenden rechtlichen Unsicherheiten die derzeit noch größte Hürde für die Etablierung von Geschäftsmodellen für Datentreuhänder bildet.

Um einen Einblick in unterschiedliche Ansätze zu erhalten, werden in der Studie zwei Use Cases bearbeitet. Der eine Use Case (Health-X dataLOFT) diskutiert einen vom BMWK geförderten Ansatz, einen Datenraum für Gesundheitsdaten zu erstellen. Der andere Use Case diskutiert den proprietären Datenraumansatz von Fitbit im sekundären Gesundheitsmarkt. Der Vergleich der beiden Ansätze zeigt die unterschiedliche Ausgestaltung der Datenbehandlung durch die beiden Ansätze sowie die Auswirkungen auf die Datengeber und -nutzer.

1. Einführung

1.1 Zielstellung der Studie

In einer zunehmend digitalisierten Welt werden Daten zu einem zentralen Treiber für Forschung, Innovation und wirtschaftliche Wertschöpfung. Wurden in der Vergangenheit Daten vor allem für einzelne spezifische Anwendungen gesammelt, schaffen Datenräume heute die Chance, Daten unterschiedlicher Anwendungen und Domänen miteinander zu kombinieren. So schafft in der medizinischen Forschung der Austausch von Daten die Grundlage für die Entwicklung neuer Behandlungsmethoden. In der Klimaforschung wird es durch den Zugang zu umfangreichen Klima- und Biodiversitätsdaten ermöglicht, Aussagen zu Klimaveränderungen und deren Auswirkungen auf die Artenvielfalt zu treffen. Diese Beispiele deuten an, welche weiteren Chancen sich aus der Verknüpfung von Daten verschiedener Anwendungen und Domänen ergeben können.

Auch im privaten Lebensbereich sind immer mehr Daten vorhanden. Anwendungen wie die Einzelraumtemperatursteuerung, die mit der verstärkten Nutzung von Photovoltaikanlagen einhergehenden Energiemanagementsysteme, die wachsenden Anwendungen für die Sicherheit und den Schutz von Bewohnerinnen und Bewohnern in Gebäuden sowie deren digitale Anbindung an die Gebäudeumwelt generieren immer mehr Daten. Dies gilt umso mehr vor dem Hintergrund der dazu verwendeten IoT-Technologien, deren globale Anwendungszahl sich zudem von heute bis 2033 nochmals mehr als verdoppeln soll (Vailshery, 2024).

Die wachsende Menge an Daten liefert Chancen sowohl für Unternehmen wie auch Private. Für die Wettbewerbsfähigkeit von Unternehmen, insbesondere KMU, spielt die zunehmende Möglichkeit umfangreicher Datenanalysen eine entscheidende Rolle, etwa um Entscheidungsprozesse zu verbessern, innovative Produkte und Dienstleistungen zu entwickeln oder effizientere Geschäftsprozesse zu gestalten. Da der Trend immer stärker weg von singulären Anwendungen hin zu einer anwendungsübergreifenden Zusammenarbeit geht, besteht im Verknüpfen der Daten der eigenen Anwendung mit Daten anderer Anwendungen – innerhalb der eigenen Domäne oder domänenübergreifend – ein großes **Innovationspotenzial** (Denga, 2023; Lauf et al., 2023). Für private Datengeber und –nutzer eröffnen die steigenden Datenmengen neue Nutzungsmöglichkeiten, z.B. im Bereich des Komforts, der Energieoptimierung wie aber auch des Verbleibs von Menschen mit Hilfsbedürfnis in den angestammten Lebensumwelten.

Damit die Daten aus den unterschiedlichen Anwendungsdomänen für neue Geschäftsmodelle genutzt werden können, müssen sie für die Beteiligten verfügbar gemacht werden. Dies kann über sogenannte Datenräume erfolgen, in denen der Zugang zu Daten unterschiedlicher Anwendungen geregelt ist. Mit der Schaffung eines Datenraums auf Basis semantischer Modelle, die eine semantische Programmierung zulassen, lassen sich Daten aus unterschiedlichen Quellen und Formaten integrieren und miteinander verknüpfen. Semantische Technologien bieten dabei im Gegensatz

zu traditionellen Standards eine höhere Flexibilität, um auf neue Technologien und Anforderungen zu reagieren.

Der Datenaustausch in einem solchen Datenraum erfordert aber auch ständige Abfragen, ob die jeweils erforderlichen Informationen verfügbar sind und die jeweiligen Zugriffsrechte vorliegen. Auch rechtliche Unsicherheiten und fehlendes Vertrauen seitens Datengebern und -nutzern stellen in der praktischen Umsetzung des Datenaustausches Herausforderungen dar. Denkbar ist deshalb die Einrichtung einer unabhängigen Instanz, die beim Datenaustausch als **neutraler und vertrauenswürdiger Intermediär zwischen Datengebenden und Datennutzenden** fungiert und in ihrer Funktion die Verantwortung für die sichere und rechtskonforme Vermittlung von Daten übernimmt: Ein solcher Intermediär kann helfen, Vertrauen auf Seiten der Datengebenden aufzubauen und rechtliche Unsicherheiten bei Datennutzenden zu minimieren, indem er Anreize für das Datenteilen aufzeigt und dabei rechtskonforme Richtlinien und Standards für die Datennutzung etabliert und überwacht (Baars et al., 2022). Hierbei unterliegen die Aktivitäten der Intermediäre zahlreichen regulatorischen Anforderungen. Gesetze auf nationaler und europäischer Ebene (insb. die DSGVO und der Data Governance Act) regeln die Anforderungen an das Datensammeln, die Datenzugänge, die Datenspeicherung wie auch die Weiterverarbeitung von Daten.

Als eine Form eines Intermediärs hat das Konzept von **Datentreuhändern** und die Erforschung und Erprobung möglicher Datentreuhandmodelle in den vergangenen Jahren stark an Bedeutung gewonnen (Micheli et al., 2023). Dabei entwickelt sich dieses Konzept immer stärker zu einem politischen Leitbild, das die Teilhabe von Datengebenden und die Umsetzung von Datenschutz hervorhebt und sich damit als Gegenmodell zu den großen Plattformen versteht, denen vorgeworfen wird Datenmacht anzusammeln und diese für ihre eigenen Zwecke zu nutzen (Specht-Riemenschneider, 2023). Sowohl über Förder- als auch Regulierungsmaßnahmen werden aktuell Bestrebungen verfolgt, um die Schaffung von Datentreuhanddiensten in einem europäischen Verständnis zu unterstützen.

Vor dem Hintergrund der enormen Potenziale des Datenteilens wird im Rahmen des Technologieprogramms *SmartLivingNEXT – Künstliche Intelligenz für nachhaltige Lebens- und Wohnumgebungen* des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) aktuell ein KI-basiertes Ökosystem entwickelt, das den oben beschriebenen rechtskonformen Zugang zu Daten deutlich erleichtern und damit die Entwicklung intelligenter und nachhaltiger Lebensumgebungen effizienter, schneller und kostengünstiger gestalten soll. Ziel ist es, dass Daten künftig unabhängig von der jeweils verbauten Gebäudetechnik verfügbar sind, alle Systemwelten abdecken und dabei gleichzeitig vor unautorisierten Zugriffen geschützt werden (Schulz-Dieterich et al., 2024). Dabei liegt der Fokus auf Daten von Anwendungen aus den Bereichen Energie und Assistenz, die im SmartLivingNEXT-Dataspace – unabhängig von ihrem Speicherort oder ihrer Herkunft – über einen standardisierten Zugang bereitgestellt, semantisch beschrieben und mit anderen Daten verknüpft werden können. Im Zentrum des Programms steht die Entwicklung der Kerntechnologie wie einer Governance-Struktur für den Betrieb des Datenraums und den Aufbau des Innovationsökosystems. Diese Technologie wird mithilfe eigener Anwendungen erprobt. Ergänzend dazu

schaffen angebundene Forschungs- und Entwicklungsprojekte weitere Anwendungen, deren Daten im SmartLivingNEXT-Ökosystem zusammengeführt werden.

Der sichere und effiziente Austausch von Daten schafft in dem Vorhaben die Grundlage für eine vernetzte und nachhaltige Lebensweise, die den Alltag von Menschen verbessert und gleichzeitig zur Lösung globaler Herausforderungen beiträgt. Beispielsweise können Daten über Energieverbrauch und -erzeugung geteilt werden, um Energiemanagementsysteme zu entwickeln, die den Energieverbrauch optimieren und Kosten senken. Ein weiteres Beispiel ist die Ausstattung von Wohnungen hilfebedürftiger Menschen mit unterschiedlichen Technologien aus dem Bereich Ambient Assisted Living (AAL), der Angehörigen und medizinischem Personal einen niedrigschwelligen Zugriff auf relevante Gesundheitsdaten erlaubt und damit zu einem selbstbestimmteren Leben im Alter beitragen soll.

Im Rahmen der Begleitforschung von SmartLivingNEXT soll die vorliegende Kurzstudie in Ergänzung zu den projektspezifischen Geschäftsmodellarbeiten der Ludwig-Maximilians-Universität in München das Potenzial und die Hürden von Datentreuhändern beleuchten. Die Kurzstudie zielt darauf ab, auf einer projektübergreifenden Basis die Anforderungen für die Etablierung von nachhaltigen Geschäftsmodellen von Datentreuhändern vor dem Hintergrund der Regulierungsansätze, denen auch das Smart Living-Ökosystem unterliegt, zu erörtern und diese für die beteiligten Akteure im SmartLivingNEXT-Technologieprogramm ebenso wie für die Fachöffentlichkeit verständlich aufzubereiten. Eine Übertragung auf zukünftige Projekte im Smart Living-Bereich soll ermöglicht werden. Die folgenden zentralen Fragestellungen gilt es dabei zu erörtern:

- Welche **Anforderungen** stellen sich an Datentreuhänder?
- Welche unterschiedlichen **Funktionen** können Datentreuhänder erfüllen?
- Welche **Regulierungsansätze** bestimmen die Ausgestaltung eines Datentreuhandmodells?
- Welche generischen Ansätze für **Geschäftsmodelle** ergeben sich vor dem Hintergrund der Regulierung für Datentreuhänder, die in der Arbeitsgruppe *Marktkonformität & Datenökonomie* des Leitprojekts von SmartLivingNEXT verwendet werden können?

Grundlage der Studie ist eine umfassende Literaturrecherche zum aktuellen Forschungsstand sowie Fachgespräche mit Vertreterinnen und Vertretern aus

Industrie, Wohnungswirtschaft und Gesundheit.[1] Aufbauend auf einer Diskussion über das Rollenverständnis eines Datentreuhänders einschließlich seiner Anforderungen und Funktionen (Kapitel 2) werden die geltenden rechtlichen Rahmenbedingungen (Kapitel 3) sowie mögliche Geschäftsmodelle näher beleuchtet (Kapitel 4). Auf Grundlage dessen soll in Kapitel 5 ein Rahmenwerk für Datentreuhänder im Smart Living erschlossen werden, das den bisherigen Literatur- und Rechtsstand zusammenführt. Anhand dieses Rahmenwerks sollen in einer abschließenden Analyse die technischen, wirtschaftlichen und rechtlichen Grundlagen eines proprietären und eines öffentlichen Datentreuhandmodells zum Teilen von Gesundheitsdaten gegenübergestellt werden (Kapitel 6). Das abschließende 7. Kapitel soll ein Fazit über die Anforderungen, Herausforderungen und Lösungsansätze von Datentreuhändern ziehen sowie einen Ausblick liefern, wie die hier gewonnenen Erkenntnisse auf aktuelle und zukünftige Projekte im Smart Living-Bereich übertragen werden können.

1.2 Methodischer Ansatz

Zur Erstellung dieser Studie wurde ein methodischer Ansatz gewählt, der auf drei Säulen basiert. Zunächst wurde eine umfassende Literaturstudie durchgeführt, bei der relevante Quellen zum Thema identifiziert und anhand eines festgelegten Rasters ausgewertet wurden. Dieses Raster orientierte sich an den drei Perspektiven der Studie: 1. Funktionen von Datentreuhändern, 2. rechtliche Rahmenbedingungen für Datentreuhänder und 3. Geschäftsmodelle für Datentreuhänder. Neben der Literaturauswertung wurden Interviews mit insgesamt drei Expertinnen und Experten geführt. Ziel war es, die Anforderungen an die Erfüllung der drei Perspektiven aus ihrer Sicht zu ermiiteln. In diesen Gesprächen wurden insbesondere die Hypothesen, die aus der Literaturrecherche abgeleitet wurden, thematisiert und weiter vertieft. Schließlich wurden drittens Projekte außerhalb des Anwendungsbereichs von Smart Living erhoben und hinsichtlich ihrer Ausrichtungen auf die drei Perspektiven analysiert.

Durch diesen Methodenmix konnte eine solide Grundlage für die in der Studie gewonnenen Erkenntnisse geschafften werden.

[1] Die Fachgespräche fanden überwiegend in den Organisationen Wirtschaftsinitiative Smart Living e.V. und Smart Living Hessen Cluster statt.

2. Anforderungen an und Funktionen von Datentreuhändern

Trotz des eingangs erläuterten Potenzials, das aus dem Teilen von Daten entstehen kann, bleibt die globale Datennutzung weit hinter ihrem Potenzial zurück. Täglich werden weltweit über 400 Millionen Terrabyte an Daten erzeugt. Das Datenvolumen hat sich dabei seit 2010 exponentiell von 2 auf 120 Zettabyte erhöht, Schätzungen zufolge wurden 90% der weltweit verfügbaren Daten zwischen 2022 und 2024 erzeugt (Duarte, 2024). Dabei bleiben 80 Prozent der Industriedaten jedoch ungenutzt (Jussen et al., 2023). Insbesondere Europa schöpft das Potenzial der Datenwirtschaft nicht voll aus und droht, im Vergleich zu Asien und den USA in der Entwicklung seiner Datenwirtschaft zurückzufallen. Auch unter den deutschen Unternehmen nutzen nur vier von zehn das Teilen von Daten zur Ausgestaltung ihres Geschäftsmodells (Schönwerth, 2024). Lediglich sechs Prozent schöpfen tatsächlich das Potenzial der verfügbaren Daten aus, obgleich bis 2025 mehr als die Hälfte der von der Bitkom befragten Unternehmen datengetriebene Geschäftsmodelle einsetzen möchten (ebd.). Auch im Smart Living gibt es noch erhebliches ungenutztes Potenzial in der Nutzung von generierten Daten, insbesondere wenn es um deren anwendungs- und domänenübergreifende Verknüpfung geht (Chataut et al., 2023).

Ein wesentlicher Grund für das ungenutzte Potenzial von Daten liegt darin, dass viele potenzielle Datengebende und -nutzende die mit dem Datenteilen verbundenen Risiken stärker gewichten als den potenziellen Nutzen (**Wert-Risiko-Dilemma**) (Kreutzer et al., 2024c; Opriel et al., 2021; Otto et al., 2020). Ein wichtiger Aspekt ist die **Vertrauensdimension**: Viele Unternehmen fürchten, dass ihre Daten missbraucht oder nicht sicher verwaltet werden könnten, was das Vertrauen in den Umgang mit sensiblen Informationen erheblich beeinträchtigt. Hinzu kommt eine **unternehmenskulturelle Komponente**, da Unternehmen befürchten, dass Wettbewerber vom Datenteilen stärker profitieren und ihre eigene Marktposition geschwächt wird. Auch die **Sicherheitsdimension** und die Angst vor Datenlecks und Cyberangriffen spielen eine Rolle. Unternehmen fürchten den potenziellen Schaden, der durch den Verlust oder Missbrauch von Daten entstehen könnte. Zudem wirken sich **technische Faktoren**, wie die hohen Kosten der Datenverarbeitung und die oftmals fehlenden digitalen Kompetenzen innerhalb der Organisation negativ auf die Bereitschaft aus, in datengestützte Prozesse zu investieren.

Neben den Hürden auf der Unternehmensseite bestehen auch Hürden auf der Seite privater Nutzer. So haben bspw. Mietende, nicht zuletzt wegen der fehlenden Selbstbestimmung des Verbauens von Smart Living-Technologien durch Mietende in Mietwohnungen, Befürchtungen, dass die Vermieter über die Auswertung von Daten Zugang zu persönlichen Informationen der Mietenden erlangen, was jüngst bei einem großen Wohnungsunternehmen zu erheblichen auch rechtlichen Konsequenzen führte (Moering and Wendt, 2024).

In einer zunehmend datengetriebenen Welt können Datentreuhänder helfen, dieses Wert-Risiko-Dilemma aufzulösen, sodass potenzielle Datengebende und -nutzende einen entscheidend größeren Mehrwert im Teilen von Daten angesichts von

(Compliance)-Risiken und Kosten sehen. Wie das Modell eines Datentreuhänders dabei organisatorisch, rechtlich und technisch ausgestaltet ist, ist in der Praxis häufig noch unklar und hängt vor allem von den jeweiligen Anwendungsfeldern und seinen spezifischen Anforderungen ab. Obwohl es keine ‚one-size-fits-all'-Lösung eines Datentreuhandmodells gibt, zeichnet sich nunmehr ein Grundkonsens in der Literatur über die wesentlichen Anforderungen an Datentreuhänder und deren primäre Funktionen ab, was eine praktische Übertragung in die jeweiligen Anwendungsfelder ermöglicht (Kreutzer et al., 2024b). Im Folgenden gehen wir daher zunächst auf die diversen Anforderungen und Funktionen und die diesen zugrundeliegenden technischen Prämissen ein, bevor daraus Implikationen für den Anwendungsbereich Smart Living abgeleitet werden.

2.1 Begriffsverständnis

2.1.1 Aufgabenportfolio eines Datentreuhänders

Trotz der wachsenden Aufmerksamkeit in Politik und Wissenschaft für das Konzept von Datentreuhändern fehlt es aktuell noch an einer allgemein anerkannten Definition. Es erscheint daher notwendig, zunächst ein Verständnis darüber zu entwickeln, was den Kern eines Datentreuhänders ausmacht. Ausgehend von dem angesprochenen Wert-Risiko-Dilemma beim Datenteilen besteht die **zentrale Aufgabe** eines Datentreuhänders darin, Datengebende[2] und -nutzende durch die Bereitstellung von Diensten dabei zu unterstützen, den Nutzen so weit zu steigern und die Kosten und Risiken so weit zu senken, dass das Teilen von Daten für alle Beteiligten lohnenswert erscheint (Kreutzer et al., 2024b). Konkrete **Ziele** eines Datentreuhänders können sich dabei je nach Anwendungsfall unterscheiden (Blankertz, 2020): Beispielsweise können Datentreuhänder in erster Linie zum Schutz und zur Stärkung der Datenhoheit und Partizipation von Datengebern etabliert werden, indem sie deren Mitwirkung an der wirtschaftlichen Nutzung ihrer Daten fördern und einen transparenten sowie sicheren Datenaustausch sicherstellen. In anderen Datentreuhandmodellen liegt die Motivation in einer möglichst breiten Verfügbarkeit von Daten, um Innovation und Wettbewerb in Wissenschaft und Wirtschaft durch weitreichende Nutzung voranzutreiben. Wiederum verstehen sich andere Datentreuhänder in erster Linie als Unterstützer eines gesunden Wettbewerbs, die die Datenmacht großer Plattformbetreiber beschränken und fairere Marktbedingungen schaffen. Ausgehend von den

[2] Zu Datengebenden zählen einerseits betroffene Personen, die ihre eigenen personenbezogenen Daten bereitstellen, und andererseits Dateninhabende, wie Unternehmen, öffentliche Institutionen oder Forschungseinrichtungen, die Daten mit der Einwilligung der betroffenen Personen zur Verfügung stellen können.

angesprochenen unterschiedlichen Zielvorstellungen bzw. Rollenverständnissen lassen sich drei **Grundmerkmale** ableiten, die Datentreuhänder in jedem Fall erfüllen müssen (Blankertz and Specht, 2021):

- Funktion der **Datenzugangsmittlung**, darüber hinaus möglicherweise auch Datenverwaltung, -durchleitung und/oder -aufbereitung zum Nutzen einer anderen Partei (oder mehrerer);
- Erfüllung **rechtlicher Anforderungen** (allgemeiner Art als auch spezifische Vereinbarungen zwischen beteiligten Parteien);
- Erfüllung anwendungsabhägiger **Vertrauens-/Neutralitätsanforderungen**

Basierend auf diesen drei Merkmalen, die die unterschiedlichen Ausgestaltungsmöglichkeiten von Datentreuhandmodellen auf ihren kleinsten gemeinsamen Nenner runterbrechen, verstehen wir **Datentreuhänder – als betreibende Stelle eines Datentreuhandmodells – als eine unabhängige Vertrauensinstanz, die schützenswerte Daten zwischen Datengebern und Datennutzern unter Wahrung der Interessen beider Seiten digital auf sichere und gesetzeskonforme Weise vermittelt** (Bundesdruckerei, 2024; Feth and Rauch, 2024; Kreutzer et al., 2024a). Je nach Anwendungsfeld und Zielvorstellung eines Datentreuhänders ergibt sich dann eine große Breite an möglichen, kontext-gebundenen Definitionen, aus denen sich weitere kontextspezifische Funktionen und Anforderungen ableiten lassen. Die folgende Abbildung 1 veranschaulicht die Beziehungen der involvierten Akteure und den dabei entstehenden Fluss von Daten:

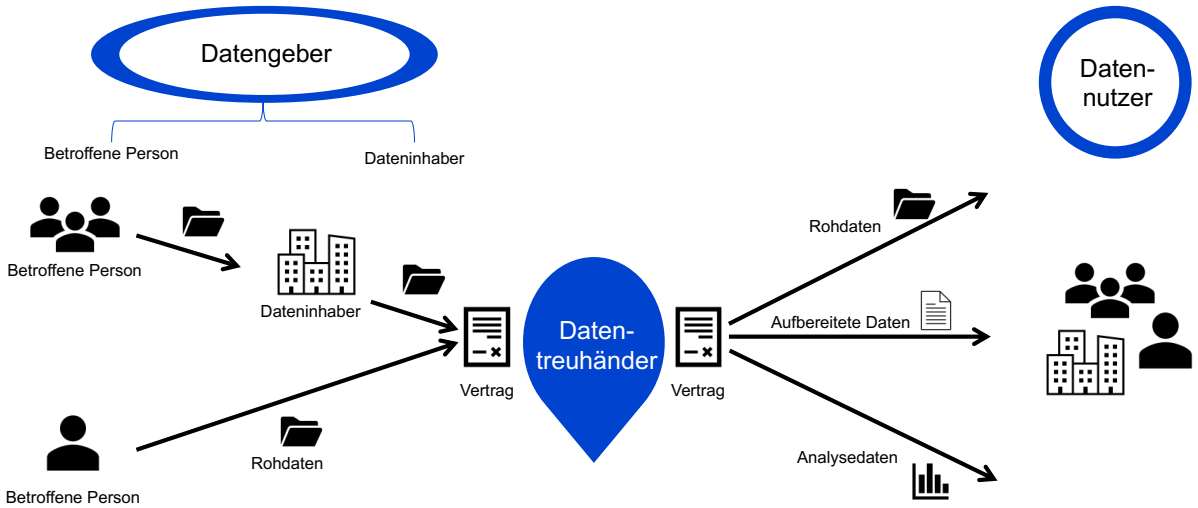


Abbildung 1 Übersicht über den Datenfluss und die involvierten Akteure. Eigene Darstellung (Technopolis Group).

2.1.2 Datentreuhänder versus Datenintermediär

Neben vielfältigen Definitionen ist die Fachliteratur auch geprägt von einem unklaren Begriffsverhältnis zwischen den Konzepten des Datentreuhänders und des Datenintermediärs. Eine Auslegung, wie sie von Micheli et al. (2023) vertreten wird, suggeriert eine de facto Deckungsgleichheit der Begriffe. Demnach ist ein Datentreuhänder lediglich als möglicher rechtlicher Rahmen eines Datenintermediärs zu betrachten. Im Gegensatz dazu sieht eine andere Auslegung Datentreuhänder als eine besondere Form des Datenintermediärs.[3] Nach Richter (2023) etwa haben Datentreuhänder als Untergruppe des Datenintermediärs die treuhänderische Pflicht, im Interesse von Datengebern und -nutzern zu handeln. Datenschutz ist für Datentreuhänder eine zentrale Bedeutung, während dies nicht für alle Datenintermediäre gelten muss. Carovano und Finck (2023) ergänzen, dass Datentreuhänder durch eine Spannbreite von Beteiligungs- und Befugnisoptionen sowie möglicher Zusatzleistungen gekennzeichnet sind. Diese Spezialisierungen führen schließlich vom Datenintermediär, der die Grundanforderungen des neutralen Datenteilens erfüllt, hin zum vertrauenswürdigen Datentreuhänder. Für den Zweck dieser Studie soll dem differenzierenden Pfad gefolgt werden, demzufolge **Datentreuhänder eine Sonderform des Datenintermediärs** darstellen, wie von Carovano und Finck (2023) und Richter (2023) vertreten.

Der Diskussionsspielraum rund um die Begrifflichkeit des Datentreuhänders beweist die Vielzahl an möglichen Formen zur Ausgestaltung seiner zentralen Aufgabe einer vertrauensvollen, rechtskonformen und sicheren Vermittlung von Daten, die sich je nach Domäne und Anwendungsbeispiel stark unterscheiden können. In welcher Form und Intensität Datentreuhänder diese Aufgabe übernehmen können, wird im Folgenden anhand verschiedener Dimensionen beleuchtet.

2.2 Anforderungen an den technischen Umgang mit Daten

Aus technischer Sicht müssen Datentreuhänder im Wesentlichen drei Anforderungen erfüllen, hierzu zählen die Sicherstellung von **Datensouveränität** und **Dateninteroperabilität** sowie die Ermöglichung von **Datenwertschöpfung** durch Qualitätssicherung und Verwaltung von Daten (DSSC, 2024; Lindner and Straub, 2023). Daraus resultiert ein großes Spektrum an möglichen Formen ebenso wie an zugehöriger technischer Infrastruktur (Appelt et al., 2023).

[3] Daneben gibt es andere organisatorische Strukturen oder funktionale Beziehungen im Hinblick auf das Datenteilen, wie Datenräume, Datentreuhand, Datenmarktplätze oder Datenkooperationen.

2.2.1 Datensouveränität

Im Mittelpunkt der Gewährleistung von Datensouveränität, also der selbstbestimmten Kontrolle von Datengebenden über die Erhebung, Speicherung und Nutzung ihrer Daten, stehen Entscheidungen über die Art der Datenhaltung, das Identitätsmanagement, Regelungen zu Berechtigungen und Zugängen sowie die Nachvollziehbarkeit von Datenflüssen. Diese Aspekte werden im Folgenden näher beleuchtet

Eine zentrale Frage ist die nach der **Art der Datenhaltung**, also wie die Daten vom Datengebenden zum Datennutzenden gelangen. Möglich sind eine zentrale sowie dezentrale Speicherung der Daten. Bei einer *zentralen Datenhaltung* werden die Daten von den Datengebenden in ein zentrales digitales System des Datentreuhänders eingespeist, dort „auf Vorrat" verwaltet und nach festgelegten Regeln weitergeben. Im Gegensatz dazu verbleiben die Daten bei einem dezentralen Datentreuhänder in ihren Ursprungssystemen, und der Datentreuhänder übernimmt lediglich die Vermittlung der Daten, wobei der Datentreuhänder hier entweder als Broker agiert und als zentrale Stelle (*Routing*) Daten beim Datengebenden bei Bedarf anfragt, an den Datennutzenden durchreicht und anschließend wieder löscht oder als Vermittlungsstelle den direkten Datenaustausch zwischen Datengebenden und -nutzenden ermöglicht (*Peer-to-Peer*). Auch hybride Formen sind möglich. Während eine zentrale Form der Datenhaltung vor allem die Interoperabilität von Daten begünstigt und es Datentreuhändern leichter macht, datenverarbeitende Funktionen zu realisieren, fördern dezentrale Formen aufgrund der lokalen Kontrollkomponente die Datensouveränität der Datengebenden sowie die Resilienz gegenüber potenziellen Sicherheitslücken (Feth and Rauch, 2024; Kreutzer et al., 2024c). Dezentrale Formen gelten deshalb nicht nur als sicherer, sondern auch als demokratischer und sind nach aktuellem Stand der Forschung die gängigere Variante (Küfeoğlu et al., 2022; Stefanija et al., 2023). Letztlich sind aber die jeweiligen spezifischen Anforderungen des Anwendungsfalls bei der Frage entscheidend, welche Art der Datenhaltung zu bevorzugen ist.

Im Gegensatz zu der Art der Datenhaltung ist das **Berechtigungs- und Zugriffs-management**, durch das Daten vor unberechtigtem Zugriff geschützt und für berechtigte Nutzende verfügbar gemacht werden, in Datenaustauschmodellen recht einheitlich geregelt und wird durch die Zusammenarbeit zweier technischer Bausteine umgesetzt (Kreutzer et al., 2024c):

Die **Access-Control-Komponente** (AC) legt die Autorisierungsregeln für den Zugriff auf spezifische Daten fest. Nach erfolgreicher Authentifizierung erhält der Nutzende nur Zugriff auf Daten, die seinen individuellen Berechtigungen entsprechen. Die Daten-nutzung kann dabei gezielt beschränkt oder freigegeben werden, beispielsweise auf bestimmte Nutzergruppen oder Verwendungszwecke, auf den Eintritt bestimmter Ereignisse, oder auf ein definiertes Zeitintervall oder eine festgelegte Nutzungsanzahl.

Konkret lassen sich verschiedene Modelle der Zugriffskontrolle unterscheiden, wobei die letzteren beiden Modelle nach aktuellem Stand bevorzugt Verwendung finden (Lindner and Straub, 2023):

- *Discretionary Access Control* (DAC): Individuelle Festlegung von Zugriffsrechten auf Basis der Identität jedes Akteurs
- *Mandatory Access Control* (MAC): Systembestimmte, auf Regeln und Entscheidungen basierende Festlegung von Zugriffsrechten (Kategorisierungen, Labels, Code-Wörter)
- *Role-Based Access Control* (RBAC): Festlegung von Zugriffsrechten auf Basis von Benutzerrollen oder Gruppen (Abgeschwächtes DAC-Modell)
- *Attribute-based Access Control* (ABAC): Festlegung von Zugriffsrechten auf Basis einer Kombination von Attributen (des Nutzers, der Daten, des Nutzungszwecks, der Umgebung)

Über die **Identity-Management-Komponente** (IDM) erfolgt eine Prüfung der Identität der Datennutzenden und ihrer Zugriffsrechte (Kreutzer et al., 2024c). Hierfür müssen sich alle Datennutzende zunächst beim IDM registrieren und erhalten daraufhin einen Global-Unique-Identifier (GUID), der ihre Identität authentifiziert. Der IDM teilt dem AC bei jedem Zugriffsversuch mit, ob die Datennutzenden im entsprechenden Fall auf die Daten zugreifen dürfen.

Der Datentreuhänder muss aber Berechtigung und Zugriff nicht nur bei Erhalt der Daten kontrollieren, sondern auch sicherstellen, dass Datennutzende die Daten der Datengebenden nach Erhalt nicht zweckentfremden. Vor allem bei personenbezogenen, sensiblen Daten, wie sie beispielsweise im Gesundheitsbereich geteilt werden, ist diese laufende Kontrolle zur Einhaltung der Datensouveränität essenziell. Der Datentreuhänder ist in diesem Rahmen für die **Aufzeichnung und Überwachung** zuständig und muss geeignete Instrumente und Prozesse zur übersichtlichen Darstellung von Datennutzungsanfragen und geteilten Freigaben gewährleisten, sodass Datengebende jederzeit wissen, wer ihre Daten zu welchem Zweck nutzt.

Auch können Datentreuhänder technische Methoden zur Pseudonymisierung oder Anonymisierung von Daten einsetzen, um die Datensouveränität von Datengebenden zu stärken und eine Nutzungskontrolle zu gewährleisten. Durch Datenanonymisierung werden die Daten auf eine Weise verändert, dass eine Rückführung zu Datengebenden nur noch mit einem unverhältnismäßig großen Aufwand möglich ist. Bei der Pseudonymisierung von Daten wird der Schlüssel (oder zusätzliche Informationen), der die Rückführung auf die ursprüngliche Identität ermöglicht, separat und besonders geschützt aufbewahrt, z.B. durch restriktivere Zugriffsrechte oder zusätzliche Verschlüsselung. Solange der Schlüssel vorhanden ist, bleibt bei einer Pseudonymisierung die Verbindung zu einer spezifischen Person also grundsätzlich möglich.

2.2.2 Dateninteroperabilität

Ebenfalls auf der technischen Ebene wird die Grundlage für eine Interoperabilität von Daten gelegt, die in diesem Kontext als „Fähigkeit technischer Systeme sowie deren Nutzerinnen und Nutzer (…), Daten einfach und effektiv auszutauschen und aus den

geteilten Daten einen Mehrwert zu generieren“ (Lindner and Straub, 2023) verstanden werden soll. Die heterogenen Schnittstellen, unterschiedliche Datenmodelle und Datengewinnungsmethoden erschweren diese Interoperabilität und damit den Datenaustausch.

Das Referenzarchitekturmodell der International Data Space Association (**IDS-Referenzarchitektur**) soll eine einheitliche, technische und organisatorische Grundlage für den sicheren und souveränen Datenaustausch zwischen verschiedenen Akteuren in einem Datenraum schaffen und hat sich in der praktischen Erprobung von Datentreuhandmodellen als bewährter Referenzrahmen etabliert (Kreutzer et al., 2024b). Neben einem allgemeinen Governance-Modell und einer Implementierungsstrategie für Datenräume definiert es auch technische Standards, die die Interoperabilität sicherstellen sollen. Daraus ergeben sich gemeinsame Schnittstellen, standardisierte Datenformate und Kommunikationsprotokolle. Kurz gesagt, es werden gemeinsame Ontologien geschaffen, die es ermöglichen, dass unterschiedliche IT-Systeme nahtlos miteinander kommunizieren können (Kreutzer et al., 2024a). Vor allem die domänenübergreifende Interoperabilität von Daten erweist sich in der Praxis allerdings noch als Herausforderung.

2.2.3 Datenwertschöpfung

Ein zentraler Zweck eines Datenraums besteht darin, durch den Austausch von Daten einen Mehrwert für die verschiedenen Akteure des Datenraums zu schaffen. Um dieses Ziel zu erreichen, müssen diese über die verfügbaren Daten, Dienste und Angebote im Datenraum informiert sein, verstehen, wie sie auf diese zugreifen und sie nutzen können, und in der Lage sein, Beziehungen einzugehen, die den ordnungsgemäßen Austausch von Daten beinhalten (DSSC, 2024). Um direkte Mehrwerte zu ermöglichen, können Datentreuhänder Datengebenden und -nutzenden weitere technische Bausteine bereitstellen. Beispielsweise können sie Softwarelösungen anbieten, über die Datengebenden einfach festlegen können, wie ihre Daten genutzt werden dürfen. In Verbindung mit einem Monitoring der Nutzung von bereitgestellten Daten können Datentreuhänder für die Akteure des Ökosystems so übersichtliche Dashboards bereitstellen sowie Abrechnungs- und Streitschlichtungsmechanismen umzusetzen (Lindner and Straub, 2023). Über Metadatenkataloge oder aktive Matching-Protokolle können Datentreuhänder außerdem die Identifikation von relevanten Daten für Datennutzende erleichtern und ein aktives Matchmaking zwischen Datengebenden und -nutzenden erzielen (Lindner and Straub, 2023). Schließlich können Datentreuhänder auch datenbasierte Analysedienste bereitstellen, die je nach Bedarf statistische Auswertungen durch die Neukombination von Rohdaten oder maschinelles Lernen beinhalten und zu einer datengestützten Entscheidungsfindung von Datennutzern beitragen (Lindner and Straub, 2023).

2.2.4 Implikationen technischer Ausgestaltungsmöglichkeiten

Die verschiedenen technischen Ansätze zur Erfüllung der Anforderungen an Datentreuhänder verdeutlichen die vielfältigen Gestaltungsoptionen, die für die Implementierung eines Datentreuhänders zur Verfügung stehen. Wie ein Datentreu-

handmodell technisch gestaltet ist, d.h. welche technischen Bausteine zur Verfügung gestellt werden, hängt dabei von der Frage ab, welche Leistungen der Datentreuhänder aus funktioneller Sicht erfüllen soll. Hier unterscheiden wir allgemein zwischen drei Kerndimensionen:

Im ersten Modell, einer rein **technischen Plattformbereitstellung**, stellt der Datentreuhänder die *technische Verfügbarkeit von Daten* sicher. Dabei muss ein Datentreuhänder neben der Bereitstellung einer technischen Infrastruktur zur Vermittlung von Daten einige grundlegende Funktionen erfüllen. Durch diese Funktionen geht seine Rolle über die eines rein passiven Infrastrukturanbieters hinaus, wodurch bereits dieses Modell eine Sonderform des Datenintermediärs (wie wir ihn in Abschnitt 2.1.2 beschreiben) darstellt. Im Sinne einer *Nutzerverwaltung* müssen Datentreuhänder in diesem Modell bereits umfassende Prozesse und Schnittstellen für das Aufnehmen (Onboarding) und Verlassen (Offboarding) von Datengebenden und -nutzenden schaffen (Feth and Rauch, 2024). Hierzu zählt auch die Verwaltung und Durchsetzung von *Zugriffsrechten* sowie ein durchgängiges Einwilligungsmanagement; auch müssen den beteiligten Akteuren die jeweiligen Nutzungsbedingungen jederzeit *nachvollziehbar* gemacht werden (Protokollierung). Neben der Entgegennahme und Weitervermittlung von Daten gehört zur Aufgabe der Datenverwaltung auch die Möglichkeit, Daten bei Bedarf zu *löschen*. Auch hierfür müssen in diesem Modell bereits Prozesse und Schnittstellen geschaffen werden. Schließlich muss ein Datentreuhänder hier auch schon technische und organisatorische Maßnahmen zur *Datensicherheit* schaffen, um Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Nachweisbarkeit zu gewährleisten. Im Sinne einer *Funktionsberatung* muss der Datentreuhänder dabei in diesem Modell sicherstellen, dass alle beteiligten Akteure mit den angebotenen Funktionen vertraut sind. Beispiele hierfür sind Datenplattformen wie „dropbox“.

Das zweite Modell umfasst Funktionen der **Datenaufbereitung,** um die Nutzbarkeit von Daten sicherzustellen. Zusätzlich zu den oben beschriebenen Funktionen bieten Datentreuhänder hier Leistungen zur Datenbereinigung und Qualitätssicherung an. Zu solchen Leistungen können die Standardisierung von heterogenen Datenformaten zählen, die Konvertierung, Pseudonymisierung oder Anonymisierung von Rohdaten und Maßnahmen zur Gewährleistung von Korrektheit, Aktualität und Integrität von Daten. Zusätzlich zur Funktionsberatung kommt im zweiten Modell eine *methodische Beratung* durch den Datentreuhänder hinzu. Exemplarisch handelt es sich hierbei um Aktivitäten, wie sie das Bundesamt für Statistik wahrnimmt, das nicht nur die Daten auf die Plattform einfließen lässt, sondern auch ihre Qualität prüft und ggfl. die Entscheidung trifft, ob spezielle Daten auf der Plattform aufgenommen werden.

Im dritten, ambitioniertesten Modell eines Datentreuhänders steht neben der reinen Vermittlung und Nutzbarmachung von Daten die **Datenweiterverarbeitung bzw. -veredelung** im Vordergrund. Solche Dienste umfassen die Datenauswertung und die Verknüpfung von Daten aus verschiedenen Datenquellen, um neue Kombinationen von Daten weiterzugeben. Der Datentreuhänder ist deshalb in diesem Modell zusätzlich zu einer funktionalen und methodischen Beratung auch *inhaltlich beratend* tätig. Ein Beispiel für dieses Modell ist Statista, die einerseits eine technische

Datenplattform darstellen, aber die dort verfügbaren Daten auch für eigene Mehrwertdienste nutzen.

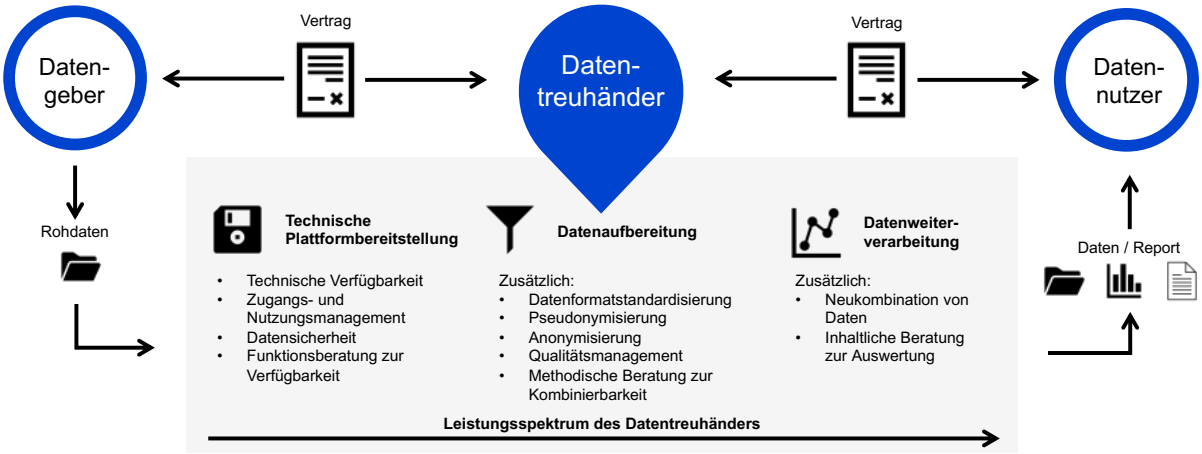


Abbildung 2 Leistungsspektrum des Datentreuhänders. Eigene Darstellung (Technopolis Group).

2.3 Zwischenfazit

Bisher wurden die allgemeinen Anforderungen von Datengebenden und Datennutzenden an Datentreuhänder sowie die möglichen technischen Maßnahmen zur Erfüllung dieser Anforderungen diskutiert. Es wurde ausgeführt, dass die Funktionen von Datentreuhändern in Datenökosystemen flexibel sind und maßgeblich durch den spezifischen Anwendungsfall bestimmt werden. Trotz dieser Variabilität lassen sich einige Kerndimensionen und Funktionen identifizieren, die allen Datentreuhändern gemein sind. Dabei besteht ihre zentrale Aufgabe darin, das Wert-Risiko-Dilemma des Datenteilens aufzulösen, indem wahrgenommene Kosten und Risiken reduziert und die generelle Nützlichkeit und das Vertrauen ins Datenteilen erhöht werden. Hierzu müssen Datentreuhänder als Vermittler zwischen Datengebenden und -nutzenden einen sicheren und rechtskonformen Datenaustausch gewährleisten und Vertrauens- und Neutralitätsanforderungen erfüllen. Die Entscheidung für die Konzeption und technische Umsetzung eines Datentreuhandmodells folgt dabei individuellen Kontextfaktoren des entsprechenden Anwendungsfalls.

Auch in der Ausgestaltung einzelner Funktionen können Datentreuhänder variieren. Dass ein Datentreuhänder beispielsweise für die Qualitätssicherung der zu vermittelten Daten zuständig ist, kann bedeuten, dass er die Datensätze „nur“ auf fehlende Bestandteile prüft. In einem umfangreicheren Ansatz der Qualitätssicherung nimmt er eine logische Prüfung vor und kontrolliert, ob die Datensätze schlüssig sind. Auf der umfassendsten Stufe der Qualitätssicherung könnte der Datentreuhänder nach dem Entdecken von Unregelmäßigkeiten auf den Datengeber zurückkommen, um gemeinsam mit ihm Auffälligkeiten in den Datensätzen zu klären und zu beheben. Diese unterschiedlichen Ansätze zeigen, dass die Rolle und die Aufgaben eines Datentreuhänders flexibel und anpassungsfähig sein müssen, um den spezifischen Anforderungen des jeweiligen Anwendungsfalls gerecht zu werden.

Die bisherigen Ausführungen der technischen Ausprägungen sagen noch nichts zu ihren rechtlichen und wirtschaftlichen Ausgestaltungen aus. Die vielfältigen Erwartungen an Datentreuhänder sind an zahlreiche Regulierungsmaßnahmen geknüpft, die in den letzten Jahren auf nationaler und europäischer Ebene aufgekommen sind. Diese Regulierungen sollen einen Rahmen liefern, der festlegt, welche Anforderungen aus rechtlicher Sicht an Datentreuhänder gestellt werden und welche der angesprochenen technischen Maßnahmen und Ausgestaltungen von Datentreuhändern rechtskonform umsetzbar sind. Die gesetzlichen Vorgaben an Datentreuhänder und wie diese ihre technische und organisatorische Umsetzung beeinflussen, wird im Folgenden untersucht.

3. Rechtliche Rahmenbedingungen

Dem steten technologischen Wandel steht das Ideal einer transparenten und kontrollierbaren Verteilung von Rechten wie Interessen von Datengebenden und -nehmenden gegenüber. Die Europäische Union hat in den letzten Jahren diverse Regulierungen eingeführt, mit dem Ziel den Europäischen Datenbinnenmarkt zu strukturieren und fairer sowie sicherer zu gestalten. Diese Maßnahmen markieren einen Übergang von nationalen Regelungen einzelner Mitgliedsstaaten hin zu einer Regulierung direkt durch die Europäische Union (Geminn et al., 2023). Dabei ergänzen bestehende nationale Regelungen weiterhin die neuen europäischen Rechtsakte. Zentral steht dabei die **Datenschutz-Grundverordnung (DSGVO)**, die seit 2018 den Schutz personenbezogener Daten und die Rechte von Bürgerinnen und Bürgern stärkt. Ergänzend wurden im Rahmen der Europäischen Datenstrategie der **Data Governance Act (DGA)** und der Digital Markets Act (DMA) eingeführt, um fairen Wettbewerb zu gewährleisten, den Zugang zu Daten zu verbessern und die Nutzung von Daten zu fördern. Der **Data Act (DA)** zielt darauf ab, die Datenverfügbarkeit zwischen Akteuren zu regeln und klare Verantwortlichkeiten für den Datenzugang und die -nutzung zu definieren. Diese Regulierungen sind Teil der Strategie der EU, ein harmonisiertes und transparentes Datenökosystem zu schaffen, das die digitale Souveränität stärkt und globale Standards setzt (Europäische Kommission, 2023).

Die Bestrebungen der EU, einen Europäischen Datenbinnenmarkt zu gestalten, sind noch von diversen offenen Fragen rund um das Datenteilen geprägt. So fehlen in vielen Unternehmen und Organisationen noch das Bewusstsein und die Werkzeuge, um auf die rechtlichen Entwicklungen der letzten Jahre zu reagieren (Dobler et al., 2023; Micheli et al., 2023). Daher soll an dieser Stelle der Schwerpunkt auf den oben angesprochenen relevanten Regulierungen des Datenbinnenmarktes und den Implikationen für die Ausgestaltung von Datentreuhändern liegen. Eine detaillierte Sachstandsanalyse zur Rechtslage rund um Data Governance in Deutschland ist bei Geminn et al. (2023) nachzulesen.

Darüber hinaus sind beim Datenteilen auch **weitere gesetzliche Regelungen** zu berücksichtigen, etwa zum Schutz von Geschäftsgeheimnissen, zur IT-Sicherheit sowie spezielle Vorschriften zum Schutz individuell schützenswerter Daten, auf die diese Studie jedoch nicht näher eingehen wird. Neben den gesetzlichen Regulierungen finden sich am Markt auch de-facto Standards. So wirken einige Grundsätze des Datenteilens wie die **FAIR-Prinzipien** als freiwillige Standards auf die Vereinheitlichung der Strukturen hin. Die FAIR-Prinzipien gehen zurück auf eine sektorübergreifende Initiative zur geteilten Nutzung von Daten im Jahr 2014 (Wilkinson et al., 2016). FAIR steht dabei für *Findable*, *Accessible*, *Interoperable and Reusable* (auffindbar, zugänglich, interoperabel und wiederverwendbar). Seitdem hat sich ein Ökosystem darum mit entsprechenden Metriken und Werkzeugen sowie angepasster Infrastruktur und Workflow entwickelt (Rainey et al., 2023).

3.1 Datenschutzgrundverordnung (DSGVO)

Die seit dem 25. Mai 2018 geltende **DSGVO** ist die erste Regelung zur Verarbeitung personenbezogener Daten, die unmittelbar und einheitlich in allen EU-Mitgliedsstaaten gilt, ohne dass sie in nationales Recht umgesetzt werden muss (Wadephul, 2022). Ihr Ziel, den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sicherzustellen und gleichzeitig den freien Verkehr solcher Daten innerhalb der EU zu ermöglichen, sollte eine Balance zwischen privaten und wirtschaftlichen Interessen schaffen.

Artikel 5 der DSGVO definiert **Verarbeitungsgrundsätze**, denen jede Datenverarbeitungstätigkeit entsprechen muss, die in den Anwendungsbereich der DSGVO fällt, und legt damit den Grundstein für Datensouveränität, also die Kontrolle der Verarbeitung, Erhebung und Speicherung von personenbezogenen Daten. Artikel 5 folgend dürfen Daten nur auf rechtmäßiger Grundlage und in verständlicher Weise verarbeitet werden. Der Grundsatz der Zweckbindung fordert, dass Daten nur für vorher festgelegte, eindeutige und legitime Zwecke verwendet werden. Nach dem Prinzip der Datenminimierung dürfen nur so viele Daten erhoben werden, wie für den jeweiligen Zweck erforderlich sind. Der Grundsatz der Richtigkeit verpflichtet zur Aktualisierung unrichtiger Daten. Daten dürfen gemäß der Speicherbegrenzung nur so lange gespeichert werden, wie es für die Zwecke nötig ist. Schließlich verlangen die Integrität und Vertraulichkeit, dass Daten durch geeignete Sicherheitsmaßnahmen vor unbefugtem Zugriff geschützt werden.

Grundsätzlich unterliegt jede Verarbeitung personenbezogener Daten nach DSGVO einem Verbot mit Erlaubnisvorbehalt. Die DSGVO erlaubt die Verarbeitung personenbezogener Daten nur, wenn mindestens eine der **Rechtsgrundlagen** aus Artikel 6 DSGVO erfüllt ist. Dazu zählt insbesondere die Einwilligung der betroffenen Person, die freiwillig, informiert und jederzeit widerrufbar sein muss. Daten dürfen auch verarbeitet werden, wenn dies zur Erfüllung eines Vertrags oder vorvertraglicher Maßnahmen erforderlich ist oder zur Erfüllung einer rechtlichen Verpflichtung dient. Weiterhin ist die Verarbeitung legitim, wenn sie dem Schutz lebenswichtiger Interessen einer Person dient, im öffentlichen Interesse liegt oder im Rahmen der Ausübung öffentlicher Gewalt erfolgt. Schließlich kann auch ein berechtigtes Interesse des Verantwortlichen oder eines Dritten die Verarbeitung rechtfertigen, sofern die Grundrechte der betroffenen Person nicht überwiegen. Für sensible Daten, bspw. Gesundheitsdaten, gelten zusätzliche Schutzvorgaben aus Artikel 9.

Weiterhin sollen die in der DSGVO definierten **Betroffenenrechte** in den Artikeln 12 bis 22 und 34 Transparenz, Kontrolle und die aktive Mitbestimmung der Betroffenen fördern, wie ihre Daten verarbeitet und genutzt werden. Dazu gehören das Recht auf Information und Auskunft, um Transparenz über die Verarbeitung zu schaffen, sowie das Recht auf Berichtigung und Löschung, um unrichtige oder unnötige Daten korrigieren bzw. entfernen zu lassen. Mit dem Recht auf Datenübertragbarkeit stellt die DSGVO das Fundament zum Datenteilen mittels Nutzungs- und Zugriffsfreigabe dar (Grünewald and Pallas, 2021). Hiernach können Datengebende ihre Daten nahtlos von einem Anbieter zu einem anderen zu migrieren. Das Widerspruchsrecht und der

Schutz vor automatisierten Entscheidungen stärken weiterhin die Selbstbestimmung der betroffenen Personen.

Die DSGVO ist auf alle Einrichtungen anwendbar, die für die Verarbeitung verantwortlich sind („**Verantwortliche**“, engl. „Controller“) oder personenbezogene Daten verarbeiten („**Auftragsverarbeiter**“). Als „Verantwortlicher“ gilt dabei gemäß Art. 4 Nr. 7 DSGVO diejenige Person, die allein oder gemeinsam mit anderen „über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“; als „Auftragsverarbeiter“ gemäß Art. 4 Nr. 8 DSGVO gelten hingegen Personen, „die personenbezogene Daten im Auftrag des Verantwortlichen“ verarbeiten und dabei deren Weisungen unterliegen (Art. 29 DSGVO). In aktuellen Diskussionen herrscht noch Unklarheit darüber, wann sich ein Datentreuhänder hier als Verantwortlicher und wann als Auftragsverarbeiter einzuordnen hat (Brauneck and Schmalhorst, 2024). Vieles spricht dafür, diese Einordnung anhand der konkreten Ausgestaltung des Datentreuhänders und seinen übernommenen Funktionen festzumachen: Nimmt der Datentreuhänder eine passive Rolle ein und vermittelt Daten auf Anweisung des Datengebenden, würde er demnach datenschutzrechtlich als Auftragsverarbeiter gelten; agiert er aktiv (im Interesse von und damit gemeinsam mit Datengebenden und/oder -nutzenden), könnte er als (ggf. gemeinsamer) Verantwortlicher eingeordnet werden, da er zwar nicht den Zweck, aber zumindest die Mittel (mit-)bestimmt und die Verarbeitung damit nur unter Mitwirkung des Datentreuhänders möglich ist.

Die DSGVO legt sowohl für Verantwortliche als auch für Auftragsverarbeiter spezifische Pflichten fest, um den Schutz personenbezogener Daten sicherzustellen. Verantwortliche sind verpflichtet, die Einhaltung der DSGVO-Grundsätze nachzuweisen (Art. 5 Abs. 2 DSGVO), Betroffenenrechte wie Auskunft, Berichtigung und Löschung zu gewährleisten (Art. 15-22 DSGVO) sowie bei sehr risikoträchtigen Verarbeitungsvorgängen Datenschutz-Folgenabschätzungen durchzuführen (Art. 35 Abs. 3 DSGVO) und Datenschutzverletzungen binnen 72 Stunden zu melden (Art. 35 DSGVO). Sie müssen zudem die Datenschutzkonformität der Auftragsverarbeiter sicherstellen, u.a. durch eine Auftragsverarbeitungsvereinbarung (Art. 28 DSGVO), für geeignete technische und organisatorische Maßnahmen zur Gestaltung (Privacy-by-Design) (Art. 25 DSGVO) sowie Umsetzung von Datensicherheit sorgen (Art. 32 DSGVO) und personenbezogene Daten löschen, wenn diese nicht mehr benötigt werden oder Betroffene ihr Recht auf Löschung geltend machen (Art. 17 DSGVO). Auftragsverarbeiter hingegen verarbeiten Daten ausschließlich auf Weisung des Verantwortlichen und sind zur Unterstützung des Verantwortlichen bei der Erfüllung seiner Pflichten und zur Meldung von Datenschutzverletzungen (Art. 28 Abs. 3 DSGVO) sowie zur Umsetzung von Sicherheitsmaßnahmen verpflichtet (Art. 32 DSGVO). Auch müssen sie ein Verzeichnis über die im Auftrag durchgeführten Verarbeitungstätigkeiten führen (Art. 30 Abs. 2 DSGVO) und nach Beendigung des Auftragsverhältnisses personenbezogene Daten auf Weisung des Verantwortlichen löschen oder zurückgeben (Art. 28 Abs. 3 DSGVO). Beide Parteien müssen eng mit den Datenschutzbehörden kooperieren (Art. 31 DSGVO) und einen Datenschutzbeauftragten benennen, wenn dies nach Art der Datenverarbeitung erforderlich ist (Art. 37 DSGVO).

Implikationen für Datentreuhänder

Die DSGVO bietet sowohl eine rechtliche Grundlage als auch einen komplexen Rahmen für die Etablierung von Datentreuhändern. Insbesondere der Artikel 6, der die Rechtsgrundlagen der Datenverarbeitung regelt, schafft eine Basis, auf der Datentreuhänder ihre Rolle sicher ausfüllen können. Die in Artikel 5 definierten Grundprinzipien wie Zweckbindung, Transparenz und Datenminimierung stärken zudem das Vertrauen der Betroffenen und fördern die Etablierung von Treuhandmodellen. Auch das Verlangen von hohen Sicherheits- wie auch Qualitätsstandards und der Einhaltung von Privacy-by-Design-Bestimmungen (Datenschutz durch Technikgestaltung) macht die Etablierung von Datentreuhändern attraktiv, die diese Bestimmungen umsetzen (z.B. über Pseudonymisierung, Verschlüsselung oder Authentifizierungsmaßnahmen).

3.2 Data Governance Act

Der **DGA** wurde geschaffen, um einen harmonisierten Rahmen für den Datenaustausch innerhalb der EU zu schaffen und dadurch die Bedingungen für die gemeinsame Datennutzung im Binnenmarkt zu verbessern (DGA Erwägungsgrund 3). Als Teil des Vorhabens der Europäischen Datenstrategie verfolgt der DGA dabei das Ziel, die Datenwirtschaft rechtlich neu zu vermessen (Hennemann, 2022) und dabei die Dominanz großer Plattformbetreiber stärker einzuschränken. Auf der DSGVO aufbauend sollen durch die Regulierung von Datenräumen ein *level playing field* für die ganzheitliche Datenwirtschaft gestaltet, das Vertrauen in Datenintermediäre und das Datenteilen verbessert und Anreize für die Entwicklung neuer datengetriebener Dienste geschaffen werden (Hennemann, 2022). Diese seit Ende 2023 gültige Verordnung greift das in Kapitel 2 beschriebene Konzept des Datentreuhänders auf, definiert und verwendet jedoch den Begriff des Datenvermittlungsdienstes. Aktuell herrscht deshalb noch große Unklarheit darüber, welche Datentreuhanddienste unter die Vorgaben des DGA fallen; der hier verwendete Begriff des Datenvermittlungsdienstes wird aus der englischen Fassung des ‚data intermediary' übersetzt, wobei dieser nicht mit unserem Verständnis des Datenintermediärs, also eines die Daten „nur" vermittelnden Intermediärs, gleichzusetzen ist, der von uns als Oberkategorie eines Datentreuhänders definiert wurde (s. Abschnitt 2.1.2).

Für Datenvermittlungsdienste sieht der DGA ein konstitutives Anmeldeverfahren vor und definiert zudem Bedingungen für die Diensterbringung sowie eine behördliche Aufsichtsstruktur zur Überwachung der Einhaltung der durch den DGA vorgesehenen Pflichten. Für bereits existierende Datenvermittlungsdienste besteht für die Anmeldung eine Übergangsfrist bis zum 24. September 2025 (DGA Art. 37).

3.3.1 Begriffsbestimmung

Als Datenvermittlungsdienst betrachtet der DGA im Wesentlichen einen Dienst, „mit dem durch technische, rechtliche oder sonstige Mittel Geschäftsbeziehungen zwischen einer unbestimmten Anzahl von betroffenen Personen oder Dateninhabenden einerseits und Datennutzenden andererseits hergestellt werden sollen, um die gemeinsame Datennutzung, auch für die Zwecke der Ausübung der

Rechte betroffener Personen in Bezug auf personenbezogene Daten, zu ermöglichen“ (DGA Art. 2/11). Diese Definition eines Datenvermittlungsdienstes, die die Bereitstellung von technischen, rechtlichen ODER sonstigen Mittel zur Herstellung von Geschäftsbeziehungen für eine gemeinsame Datennutzung umfasst, ist zunächst sehr weit gefasst. Von zentraler Bedeutung ist dabei erstens die Herstellung einer geschäftlichen Beziehung für den Datenaustausch sowie zweitens, dass dies zwischen einer unbestimmten Anzahl an Datengebenden und Datennutzenden geschieht. Artikel 2/11 weiter folgend sind hingegen nicht als Datenvermittlungsdienste zu betrachten (a) Dienste zur Datenaufwertung und -veredelung, um deren Wert erheblich zu steigern, sowie Lizensierung für die Nutzung dieser Daten, ohne dass diese Geschäftsbeziehungen zwischen Datengebenden und -nutzenden herstellen; (b) Dienste mit Schwerpunkt auf Vermittlung urheberrechtlich geschützter Inhalte; (c) geschlossene Datenpools und (d) staatliche Intermediärstätigkeiten ohne die Herstellung von Geschäftsbeziehungen. Ob ein Datentreuhanddienst in den Anwendungsbereich des DGA fällt, hängt also insbesondere davon ab, ob er aktiv in den Austausch oder die Übermittlung von Daten zwischen Dritten eingreifen und Geschäftsbeziehungen zwischen Datengebenden und -nutzenden herstellt. Reine technische Infrastruktur-Anbieter, wie z.B. Cloud-Speicher- oder Hosting-Dienste, die nur den Platz oder die Infrastruktur für die Speicherung und gemeinsame Datennutzung bieten, geschlossene Datenräume und Kooperationen ohne die offene Vermittlung von Daten an externe Akteure und Dienste, auf denen Unternehmen bspw. sensible Daten sicher hinterlegen, ohne dass andere Nutzende darauf zugreifen können sind also davon ausgeschlossen.

3.3.2 Bedingungen für die Erbringung von Datenvermittlungsdiensten

Weiter formuliert der DGA Anforderungen, die Datenvermittlungsdienste befolgen müssen, insbesondere bezüglich Transparenz, Neutralität und Interessenskonflikten (DGA Art. 12). Ein zentraler Aspekt des DGA ist das Verbot zur Datennutzung eines Datenvermittlungsdienstes für eigene **Zwecke**, das auf die in Artikel 12 verankerte Neutralitätspflicht zurückgeht. Demzufolge dürfen die Daten einzig für den Zweck verwendet werden, sie den Datennutzern zur Verfügung zu stellen (DGA Art. 12 lit. a)), sowie dürfen die gesammelten Metadaten nur der Erbringung bzw. (Weiter-)Entwicklung des Datenvermittlungsdienstes dienen, bspw. zur Aufdeckung von Betrug und Cyberangriffen (Art. 12 lit. c)). Für den Datenvermittlungsdienst bedeutet dies, dass eine strikte Trennung zwischen den Kernaufgaben der Datenvermittlung und etwaigen Zusatzaktivitäten des Treuhänders notwendig ist. Es dürfen keine eigenen Analysen oder Produkte auf Basis der bereitgestellten Daten erstellt werden, und die Preisgestaltung muss vollständig unabhängig von der Nutzung zusätzlicher Dienste erfolgen (Art. 12 lit. b)). Dies erfordert sowohl organisatorische als auch technische Maßnahmen, um diese Neutralität sicherzustellen.

Ein weiterer zentraler Aspekt ist die Gewährleistung der **Interoperabilität und Standardisierung** (Art. 12 lit. d, i). Datenvermittlungsdienste müssen Daten grundsätzlich in dem vom Datengebenden bereitgestellten Format weiterleiten. Standardisierungen oder Umwandlungen dürfen nur erfolgen, wenn sie zur Verbesserung der Interoperabilität beitragen, wenn der Datennutzende dies verlangt, oder

wenn dies durch Unionsrecht vorgeschrieben ist oder der Harmonisierung mit internationalen und europäischen Datennormen dient. Für Datentreuhänder bedeutet dies, dass die technische Infrastruktur eine flexible Unterstützung verschiedener Formate bieten und die Einhaltung offener Standards des jeweiligen Sektors sicherstellen muss. Zudem ist sicherzustellen, dass Datengebende der Umwandlung widersprechen können, sofern diese nicht zwingend vorgeschrieben ist.

Zusätzliche Werkzeuge und Dienste, wie eine vorübergehende Speicherung, Pflege, Konvertierung, Anonymisierung oder Pseudonymisierung von Daten sind ebenfalls an strikte Bedingungen geknüpft (Art. 12 lit. e). Solche Dienstleistungen dürfen nur mit ausdrücklicher Zustimmung der Datengebenden erfolgen und müssen vorrangig der Erleichterung des Datenaustauschs dienen. Für die Praxis der Datentreuhänder ergibt sich daraus die Notwendigkeit, klare Mechanismen zur Einholung und Verwaltung von Zustimmungen zu implementieren. Auch müssen diese Dienste modular und separat vom Kernangebot bereitgestellt werden, um die Neutralität des Vermittlungsdienstes zu gewährleisten.

Die Sicherstellung von **Datensouveränität und Transparenz** ist ein weiterer Eckpfeiler der Anforderungen aus Art. 12. Datentreuhänder müssen ihren Service sowohl für Datengebende als auch -nutzende auf Grundlage fairer, transparenter und nichtdiskriminierender Bedingungen anbieten (Art. 12 lit. f). Gleichzeitig sind sie verpflichtet, die betroffenen Personen vor der Einwilligung in den Datenaustausch umfassend und in klar verständlicher Sprache über die beabsichtigte Nutzung der Daten zu informieren (Art. 12 lit. m). Um dies zu gewährleisten, sollte der Datentreuhänder eine benutzerfreundliche Oberfläche bieten, über die Datengebende ihre Einwilligungen verwalten, widerrufen und Einblick in die Protokolle der Vermittlungsaktivitäten erhalten können. Im Falle unbefugter Zugriffe oder rechtswidriger Nutzung von personenbezogenen Daten sind Anbietende von Datenvermittlungsdiensten außerdem verpflichtet, diese unverzüglich zu melden (Art. 12 lit. k). Dies erfordert robuste Monitoring- und Alarmierungssysteme sowie klare Medeprozesse. Ergänzend dazu verpflichtet der DGA (Art. 12 lit n) die Anbieter dazu, den Datengebern Werkzeuge zur Verfügung zu stellen, mit denen sie ihre Einwilligungen zur Datenverarbeitung jederzeit erteilen oder widerrufen können. Diese Funktionalitäten müssen leicht zugänglich und transparent gestaltet sein, um die Kontrolle der Datengebenden über ihre Daten zu stärken. Schließlich schreibt Art. 12 lit. o die Protokollierung aller Datenvermittlungstätigkeiten vor, um die Nachvollziehbarkeit und Rechenschaftspflicht sicherzustellen. Diese Protokolle dienen nicht nur der internen Qualitätssicherung, sondern sind auch essenziell, um Datengebende im Falle von Sicherheitsvorfällen effektiv informieren zu können. Insgesamt implizieren diese Anforderungen, dass Datentreuhänder ein integriertes System schaffen müssen, das sowohl präventiv den Schutz von Daten gewährleistet als auch reaktiv Transparenz und schnelle Maßnahmen im Falle von rechtswidrigen Vorfällen ermöglicht.

Schließlich müssen Datentreuhänder ein hohes **Sicherheitsniveau** gewährleisten, um die Verarbeitung, Speicherung und Übermittlung von Daten zu schützen (Art. 12 lit. l). Maßnahmen zur Prävention von Betrug und Missbrauch (Art. 12 lit. g) sowie die Verhinderung rechtswidriger Datenübertragungen (Art. 12 lit. j) sind ebenfalls

vorgeschrieben. Für die technische Umsetzung sind daher robuste Sicherheitsmaßnahmen wie Verschlüsselung, Zugriffsmanagement und regelmäßige Audits unabdingbar.

3.3.3 Implikationen für Datentreuhänder

Insgesamt bilden die Anforderungen aus Art. 12 DGA die Grundlage für die rechtliche und organisatorische Ausgestaltung eines Datentreuhänders. Sie definieren die gesetzlichen Rahmenbedingungen, die alle Kernfunktionen eines Datentreuhänders – von der Datenverwaltung über die Sicherheit bis hin zur Gewährleistung von Transparenz und Neutralität – regeln.

Allerdings stellt die Umsetzung des DGA die Entwicklung von Datenvermittlungsdiensten auch vor erhebliche Herausforderungen. Insbesondere in Bezug auf tragfähige Geschäftsmodelle sind deutliche Rechtsunsicherheiten entstanden, da der DGA die Nutzung der vermittelten Daten für eigene kommerzielle Zwecke weitgehend untersagt. Kritisiert wird dabei vor allem die „Idealisierung einer vollständig neutralen und gemeinnützigen Datentreuhand“ (Blankertz and Specht-Riemenschneider, 2021): Das grundlegende Verbot, eigene Interessen zu verfolgen, nimmt jegliche Anreize, solche Organisationen aufzubauen, da vor allem Angebote über die reine Datenvermittlung hinaus eine Basis für tragfähige Geschäftsmodelle bieten würden. Um Interessenskonflikte zu vermeiden, müsste deshalb eine strikte Trennung zwischen Diensten zur gemeinsamen Datennutzung und darüberhinausgehenden datenverarbeitenden Diensten vorgenommen werden. Auch müsste garantiert werden, dass Nutzer den Vermittlungsdienst auch ohne die Nutzung weiterer Dienste in Anspruch nehmen können. Zusammenfassend ist zum aktuellen Zeitpunkt festzustellen, dass die strikten Regulierungen und Verpflichtungen sowie das Verbot eigener kommerzieller Interessen den Handlungsspielraum von Datenvermittlungsdiensten stark einschränken.

3.3 Data Act

Die jüngste Ergänzung der Europäischen Datenstrategie ist die am 11. Januar 2024 in Kraft getretene „Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung“, kurz **Datenverordnung** oder **Data Act** (DA)**.** Der Data Act wird nach einer 20-monatigen Übergangsfrist am 12.09.2025 EU-weit anwendbares Recht werden. Wie auch der DGA wirken die Vorschriften im Data Act ergänzend zu denen der DSGVO. Der Data Act soll den „Zugang zu industriellen Daten, sowohl personenbezogenen als auch nicht personenbezogenen, für alle Akteure in der Datenwirtschaft” (Dobler et al. 2023) ermöglichen. Ziel ist also, den Zugang zu Daten zu erleichtern, deren Nutzung zu fördern und gleichzeitig die Rechte der Nutzer von digitalen Produkten und Diensten zu schützen. Die Verpflichtung zu Datenverträgen für den Datenaustausch und die erhöhte Datenverfügbarkeit sollen sich dabei insbesondere zum Vorteil von KMU auswirken (Dobler et al. 2023; Bernal, 2024; Voigt and Von Dem Bussche, 2024). Der DA enthält Regelungen zu:

- der **Pflicht der Zugänglichmachung** von Produktdaten und verbundenen Dienstdaten für den Nutzer (Art. 3);

- Rechten und Pflichten von Nutzern und Dateninhabern in Bezug auf den **Zugang zu sowie die Nutzung und die Bereitstellung** von Produktdaten und verbundenen Dienstdaten (Art. 4);
- dem Recht des Nutzers auf **Weitergabe von Daten an Dritte** (Art. 5).

Artikel 3 bezieht sich auf die Verpflichtung, dass Anbieter von Produkten und Dienstleistungen dem Nutzer sämtliche relevante Produktdaten sowie damit verbundene Dienstdaten zugänglich machen müssen. Es handelt sich dabei um eine Transparenzpflicht gegenüber dem Nutzer, die sicherstellt, dass keine wichtigen Informationen vorenthalten werden.

Artikel 4 geht einen Schritt weiter und gewährt den Nutzenden das Recht, auf diese Produkt- und Dienstdaten zuzugreifen. Es geht nicht nur darum, dass die Daten zugänglich gemacht werden müssen (wie in Artikel 3), sondern auch darum, dass Nutzende diese ohne unangemessene Hürden oder Einschränkungen selbst abrufen oder verwenden können muss.

Artikel 5 räumt Nutzenden das Recht ein, die Produktdaten und Dienstdaten an Dritte weiterzugeben. Das bedeutet, dass Nutzende diese Daten nicht nur für den eigenen Gebrauch nutzen kann, sondern sie auch an andere, zum Beispiel Dienstleister oder Partner, weiterleiten darf. Diese Bestimmung fördert die Flexibilität und die Möglichkeit für Nutzende, die gewonnenen Daten für verschiedene Zwecke zu verwenden, wie etwa für die Integration in andere Systeme oder für den Vergleich mit anderen Angeboten.

Indem die Verordnung Nutzenden von Geräten ein Zugangsrecht zu den durch ihre Nutzung erzeugten Daten gewährt, adressiert der Data Act insbesondere Daten, die im Zusammenhang mit smarten, vernetzten Geräten im IoT generiert werden. Die dort generierten Daten werden aufgrund des Designs der Geräte in der Regel beim Hersteller gespeichert, sodass dieser bisher faktisch die vollständige Kontrolle über die Daten besaß. Dieses Monopol bedeutet auch, dass Dritte nur eingeschränkte Möglichkeiten haben, diese Daten für innovative Zwecke zu nutzen (Kathuria, 2024). Es ist somit das Ziel des DA, dass die bei IoT-Herstellern vermuteten „Datenschätze“ erschlossen weren können, indem Nutzende von IoT-Geräten das Recht eingeräumt wird, auf die durch diese Geräte erzeugten Daten zuzugreifen (Voigt and Von Dem Bussche, 2024).

Implikationen für Datentreuhänder

Der Data Act hat weitreichende Implikationen für die Rolle und Ausgestaltung von Datentreuhändern, da diese eine zentrale Position zwischen Nutzenden und Herstellern von vernetzten Geräten und Dienstleistungen einnehmen können (Kathuria, 2024). Zudem sind sie dafür verantwortlich, eine einfache und sichere Datenweitergabe an Dritte zu ermöglichen. Dabei spielen Datentreuhänder eine Schlüsselrolle in der Gewährleistung von Transparenz, Sicherheit und Datenschutz, da sie als vertrauens-würdige Dritte fungieren, die den Austausch und die Nutzung der Daten gemäß den Wünschen der Nutzenden überwachen und koordinieren. Diese Verantwortung erfordert den Aufbau robuster technischer Infrastruktur, klare

vertragliche Vereinbarungen und die Einhaltung der rechtlichen Anforderungen und Vorschriften, die durch den Data Act aufgestellt werden.

3.4 Zwischenfazit

Datentreuhänder agieren in einem hochsensiblen Umfeld, in dem der sichere und transparente Umgang mit Daten eine zentrale Rolle spielt. Rechtliche Rahmenbedingungen sollen eine Grundlage dafür schaffen, das Vertrauen zwischen Akteuren des Datenaustauschs zu fördern. Vorschriften dazu, robuste Systeme für Zugriffsmanagement, Dokumentation oder Datenverschlüsselung entwickeln zu müssen, sollen dazu beitragen, die Kontrolle über personenbezogene Daten in die Hände der betroffenen Personen zurückzugeben. Die Regulierung von Datentreuhändern hat aber auch tiefgreifende Auswirkungen auf die Entwicklung von Geschäftsmodellen in diesem Bereich: Eine der größten Herausforderungen für Datentreuhänder besteht in der Balance zwischen dem Schutz der Privatsphäre und der Schaffung von Mehrwert durch Daten. Denn die Regulierungen beeinflussen sowohl die wirtschaftlichen Rahmenbedingungen als auch die Art und Weise, wie Datentreuhänder ihre Leistungen anbieten und Vertrauen bei Datengebenden und -nutzenden aufbauen können. Aktuelle Regulierungsvorhaben werden deshalb von Rechtsexpertinnen und -experten als hinderlich wahrgenommen, weil sie den Handlungsspielraum von Unternehmen und Organisationen einschränken, als Datentreuhänder aktiv zu werden (Blankertz and Specht-Riemenschneider, 2021). Flankierende Maßnahmen wie Aufsichtsstrukturen, Zertifizierung und Akkreditierung von Datentreuhändern könnten solche Risiken minimieren (Blankertz et al., 2020; Pavel et al., 2022). Für den langfristigen Erfolg müssen Datentreuhänder innovative Ansätze finden, um Datenschutz und wirtschaftliche Nutzung von Daten zu verbinden. Derzeit ist noch unklar, ob die neuen Regulierungsversuche der Europäischen Union tatsächlich einen Schub für die europäische Datenökonomie bedeuten oder die Pflichten nicht eher als „erdrosselnd“ wahrgenommen werden (Hennemann, 2022).

4. Geschäftsmodelle

Kapitel 2 stellt verschiedene Modelle zur Ausgestaltung eines Datentreuhänders aus technischer Perspektive dar. Das dritte Kapitel diskutiert rechtliche Rahmenbedingungen, die bei der weiteren organisatorischen Ausgestaltung eines Datentreuhänders zu berücksichtigen sind. In diesem Kapitel beleuchten wir schließlich die Schlüsselkomponenten, die die wirtschaftliche Tragfähigkeit gewährleisten und damit für einen nachhaltigen, skalierbaren und zielgerichteten Betrieb eines Datentreuhänders essenziell sind (nach DSSC, 2024). Hierbei geht es in dem Kapitel primär um die grundlegenden Überlegungen zu Geschäftsmodellen in Datenräumen. Spezifische Überlegungen dazu für die Smart Living Community werden in der Arbeitsgruppe *Marktkonformität & Datenökonomie* des Leitprojekts von SmartLivingNEXT bearbeitet.

Zu den wesentlichen Schlüsselkomponenten für die erfolgreiche Etablierung eines Geschäftsmodells zählt zunächst die klare Definition des **Wertversprechens**, das die Vorteile der Datennutzung für alle beteiligten Akteure verdeutlicht. Dieses umfasst die in Kapitel 2.2 diskutierten Funktionen, die der Datentreuhänder im Ökosystem einnimmt. Ebenso essenziell ist die präzise Identifikation dieser Akteure, die als **Zielgruppen** des Datentreuhänders fungieren, und ihrer spezifischen Bedürfnisse: Dazu zählen sowohl Datengebende als auch Datennutzende, die je nach Anwendungsfall Unternehmen, Privatpersonen, Behörden und/oder wissenschaftliche Einrichtungen umfassen können. Ein weiterer zentraler Aspekt ist die Sicherstellung der **finanziellen Tragfähigkeit**, sei es durch öffentliche Fördermittel oder durch privatwirtschaftliche Einnahmen. Diese Einnahmen müssen eng an die spezifische Kostenstruktur des Datentreuhänders angepasst werden, um die finanzielle Grundlage für die übernommenen Funktionen nachhaltig zu sichern. Um Vertrauen zu schaffen, muss der Datentreuhänder in seinem Geschäftsmodell schließlich eine klare und transparente **Governance-Struktur** etablieren, die festlegt, wie der Datentreuhänder strukturiert, organisiert und geführt wird. Dabei ist vor allem zu beachten, dass sie das Vertrauen der Stakeholder fördert, mit der verfügbaren Finanzierung vereinbar ist und die rechtlichen Anforderungen erfüllt.

4.1 Governance

Lipovetskaja et al. (2024) haben in ihrer Analyse auf Grundlage öffentlicher Daten weltweit insgesamt 34 Datentreuhänder in drei Finanzierungsmodellen klassifiziert: Die von **privaten Akteuren** betriebenen Datentreuhänder können entweder gewinnorientiert (*for-profit-Modell*) oder ohne Gewinnerzielungsabsicht (*non-profit-Modell*) agieren; in einem Modell **staatlicher Trägerschaft** werden die Kosten und Investitionen durch staatliche Förderung und Subventionen getragen, das heißt über eine Umlegung auf steuerzahlende Personen oder Organisationen (Lipovetskaja et al., 2024; Stachon et al., 2023). Die Analyse ergab eine gute Hälfte der Datentreuhändermodelle in privater und die andere knappe Hälfte in staatlicher Trägerschaft. Unter den privat getragenen Modellen sind dabei etwa doppelt so viele for- wie non-profit ausgerichtet.

Hinsichtlich der Organisationsform kristallisieren sich in der Landschaft bestehender Datentreuhandmodelle drei Modelle heraus (Blankertz et al., 2020; Hardinges et al., 2019): In **institutionellen Modellen** ist der Datentreuhänder beispielsweise bei einer Behörde oder einer Hochschule angesiedelt. Solche Modelle werden in der Regel in staatlicher Trägerschaft oder unter staatlicher Aufsicht (Gebühren, Steuern) ohne Gewinnerzielungsabsicht organisiert. In rein **mitgliedsorientierten Modellen** werden die Dienste des Datentreuhänders über einen Verband oder Verein getragen, diese sind also immer privat organisiert, können aber sowohl non- als auch for-profit agieren. In **Unternehmensmodellen** werden Dienste immer von privaten Akteuren und mit Gewinnerzielungsabsicht angeboten.

Wie in Bezug auf die technischen Ausgestaltungsmöglichkeiten hängt auch die Wahl des passenden Organisations- und Finanzierungsmodells von verschiedenen Faktoren ab, die sich je nach Anwendungsdomäne unterscheiden.

4.2 Funktionen

Die Ausgestaltung des Geschäftsmodells und die Entscheidung der Finanzierung ist unter anderem abhängig von den **Funktionen**, die der Datentreuhänder in seinem Datenökosystem einnimmt. Die in Kapitel 2.2.4 gegenübergestellten Modelle (1) *technische Plattformbereitstellung*, (2) *Datenaufbereitung* und (3) *Datenweiterverarbeitung bzw. -veredelung* veranschaulichen das Leistungsspektrum von Datentreuhändern und bestimmen die Kosten und Aufwände für den Betrieb der Datentreuhandstelle sowie die Potenziale für Monetarisierung und Skalierung. Je mehr Funktionen der Datentreuhänder anbietet, desto vielfältiger sind die Möglichkeiten, Gebühren auf seine Dienstleistungen zu erheben.

4.3 Finanzierungs- und Bepreisungsansätze

Nachhaltige Finanzierungsmodelle für Datentreuhänder stellen, vor allem im C2B-Kontext, eine große Herausforderung dar. Insbesondere im Anfangsstadium sind **externe Anschubfinanzierungen** durch die öffentliche Hand oder Dritte häufig essenziell, um die Entwicklung und Etablierung von Datentreuhändern abzusichern (Schneider, 2022). Allerdings muss der Staat für eine öffentliche Finanzierung, die eine Umverteilung der Kosten auf das Kollektiv bedeutet, eine Begründung vorlegen (Kreutzer et al., 2024c).

Bei einer **internen Finanzierung** besteht aktuell noch die größte Herausforderung in der Frage zur Bestimmung des den Gewinn beeinflussenden Werts von Daten. Nach Krotova et al. (2019) ist eine ökonomische Bewertung von Daten anhand von drei verschiedenen Ansätzen möglich: Bei der *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 und setzt bereits einen aktiven Markt für den Datenhandel voraus. Die *kostenorientierte* Methode beschreibt einen Ansatz, der den Wert anhand der Kosten berechnet, die für die Erhebung, Verarbeitung und Vermittlung von Daten entstehen. Die *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 in der Wertzuschreibung bei den Datengebenden und Datennutzenden besteht.

Wenn Daten im Rahmen von Ökosystemen oder zwischen verschiedenen Akteuren geteilt werden, bemisst sich der tatsächliche Wert von Daten an deren Austausch und Verknüpfung, sodass hier die nutzerorientierte Methode zur ökonomischen Bewertung am geeignetsten scheint. Dieser potenzielle Nutzen ist allerdings vorab schwer zu bestimmen. Weiterhin ist der Wert von Daten in hohem Maße kontextabhängig und subjektiv (Otto et al. 2022).

In der Diskussion um die Monetarisierung von Daten kristallisierten sich verschiedene Ansätze heraus. Hier lässt sich zwischen Pay-per-use-Modellen (nach Datenvolumen oder nach Anzahl Transaktionen), Abonnementmodellen und Mitgliedschaften unterscheiden (Lindner and Straub, 2023; Otto et al., 2022). Auch gibt es Ansätze, die Datentransaktionen unentgeltlich, dafür aber hierauf aufsattelnde Mehrwertdienste kommerziell anzubieten. Auch Mischformen sind denkbar, etwa in Form einer Mitgliederpauschale oder aber eines pay-per-use-Ansatzes für einzelne Datenprodukte.

Kritisch betrachtet wird ein vom Datenvolumen oder von der Anzahl an Datenzugriffen abhängiger Finanzierungsansatz, da solche Ansätze Anreize dafür geben, mehr Daten an mehr Datennutzer zu „verkaufen“ als nötig, was das Missbrauchspotenzial erhöht (Blankertz and Specht-Riemenschneider, 2021). Abzuwarten bleibt außerdem, inwieweit die Finanzierung über weitere Mehrwertdienste aus europäischer regulatorischer Sicht erlaubt ist.

4.4 Neutralitätsanforderungen

Es wird häufig angenommen, dass Datentreuhänder in staatlicher Trägerschaft und in non-profit-Ausgestaltung die Anforderungen an **Neutralität** besser erfüllen, da sie für Interessenskonflikte weniger anfällig sind. Die Annahme, dass es für die Akzeptanz des Datentreuhänders am besten wäre, wenn sein Betrieb langfristig von einer staatlichen Stelle oder einer privaten non-profit-Organisation übernommen würde, ist insbesondere in Anwendungsdomänen zu beobachten, die mit sensiblen Daten (z.B. im Gesundheitsbereich) umgehen (Kreutzer et al., 2024b). Dieser wahrgenommene Spannungsbogen zwischen Gewinnmotiv von Datentreuhändern und der Wahrung

von Neutralität ist aber bisher nicht abschließend empirisch geklärt, da auch private Anbieter in einem Wettbewerbsmarkt Anreize haben, sensibel mit Daten umzugehen.[4]

Forderungen nach einem „neutralen“ Geschäftsmodell im Sinne von einem Ausschluss eines Gewinnmotivs und einer vertikalen Integration von Daten schließen Datentreuhandmodelle aus, die Daten zum Beispiel in wertschöpfungssteigernder Kombination mit Daten anderer Dienste nutzbar machen und/oder Dienste zur Analyse und Veredelung von Daten anbieten. Je weniger der Datentreuhänder etwas „mit den Daten macht“, desto unkritischer wird er üblicherweise wahrgenommen (Blankertz and Specht, 2021). Eine solche Restriktion entspricht allerdings nicht der Realität bestehender Datentreuhandmodelle und führt zur Frage, welche Anreize für die Entwicklung strikt neutraler Datentreuhandmodelle noch bestehen (Blankertz and Specht-Riemenschneider, 2021). Denn die Vermittlung, Verwaltung und ggf. Aufbereitung von Daten sowie Wartungsleistungen des Datentreuhänders sind mit Aufwand und Kosten verbunden. Zusätzliche, stärker analytische Dienstleistungen könnten die Kosten und Investitionen finanzieren und skalierbar machen. Die Annahme, dass die Bevorzugung von Datentreuhandmodellen, die weniger mit den Daten machen, Missbrauch und Interessenskonflikte vermeidet, birgt auch das Risiko Geschäftsmodelle zu verhindern, die in stärkerem Umfang Mehrwert aus Daten generieren und zum Gewinn neuer Erkenntnisse beitragen (Blankertz and Specht-Riemenschneider, 2021). Auch ist die Annahme zu hinterfragen, dass staatlich betriebene Datentreuhänder den Anforderungen an Neutralität pauschal besser gerecht werden. Machtkonzentrationen beim Staat und damit einhergehende Missbrauchspotenziale müssen hier ebenfalls bedacht werden (Lindner and Straub, 2023). Im Zentrum der Diskussion um die Neutralität des Datentreuhänders sollte entsprechend die Frage nach der Transparenz und Beeinflussung der Nutzung der Daten durch die Datengebenden stehen und nicht so sehr die wirtschaftliche Aufstellung des Datentreuhänders.

4.5 Zwischenfazit

Die Wahl der in 4.1 beschriebenen Organisationsformen für einen Datentreuhänder hängt also stark vom jeweiligen Anwendungsfall ab. Institutionelle Modelle erscheinen besonders dann sinnvoll, wenn eine starke öffentliche Unterstützung erforderlich oder ein staatliches Eingreifen sogar wünschenswert ist, etwa in Märkten mit geringer Wettbewerbsintensität oder hoher Marktmacht einzelner Akteure. Mitgliedsorientierte Modelle bieten sich aufgrund ihres hohen Koordinationsaufwands eher für bereits gut

[4] So verpflichtet sich bspw. das amerikanische Unternehmen Apple den Inhalt der Zugriffe auf die Gesundheitsdaten in der APP Health selber nicht einsehen zu können (O.V., 2024, Apple Platform Security).

etablierte Netzwerke an. Unternehmensmodelle sind ideal, wenn eine hohe Agilität und eine schnelle Anpassung an Markterfordernisse notwendig sind, beispielsweise in dynamischen Märkten, in denen Innovationen und Monetarisierungspotenziale im Vordergrund stehen, jedoch können die hohen Anfangsinvestitionen und rechtliche Unsicherheiten eine Herausforderung darstellen.

Die zögerlichen Entwicklungen bei der Etablierung tragfähiger Geschäftsmodelle zeigen, dass insbesondere rechtliche Unsicherheiten noch ein großes Hemmnis darstellen. Besonders die im DGA verankerten Neutralitätsanforderungen und der damit verbundene Ausschluss von Abhängigkeiten zwischen Datentreuhändern und Datengebern wie -nutzern, direkten Anbindungen an Wertschöpfungsketten oder anderweitige vertikale Integration bergen Unklarheiten darüber, welche Leistungen Datentreuhänder anbieten und in Rechnung stellen dürfen. Je mehr diese Leistungen über eine reine Vermittlung von Daten (die ggf. noch eine Weiterverarbeitung im Sinne der Datensouveränität und -interoperabilität umfasst) hinausgehen, desto größer werden diese Unklarheiten. Nach aktueller Auslegung der Rechtsakte scheint es deshalb notwendig, Mehrwertdienste nicht durch den Datentreuhänder selbst anzubieten, sondern in einer gesonderten juristischen Person zu organisieren, um Verstöße insbesondere gegen die Anforderungen des DGA zu vermeiden. In dem Fall würde die Datentreuhändertätigkeit also auf zwei juristische Personen aufgeteilt sein: die eine wäre für die technische Verfügbarmachung und ggf. Weiterverarbeitung von Daten (Datenbereinigung, Qualitätssicherung) zuständig, die zweite für auf den Daten aufsattelnde Mehrwertdienste (Neukombination und Analyse von Daten).

Die aktuellen Diskussionen weisen auf eine enge Verknüpfung zwischen dem Vertrauen von Datengebenden in die Datentreuhandstelle einerseits und der Ausgestaltung des Geschäftsmodells und des darin definierten Finanzierungsansatzes andererseits hin. Dabei zeigen sich verschiedene Risikoprofile von Datengebern, die sich folgerichtig in ihrer Bereitschaft, ihre Daten zu monetarisieren, unterscheiden. In der Ausgestaltung seines Geschäfts- und Finanzierungsmodells bietet es sich deshalb an, dass der Datentreuhänder diese unterschiedlichen Risikoprofile bei der Ausgestaltung seiner Funktionen sowie seines Finanzierungsansatzes berücksichtigt. Hierbei können Datengebende zunächst selbst entscheiden, welche Daten sie bereit sind, weiterzugeben. Beide Marktseiten, Datengebende wie auch Datennutzende, können dann aus einer Art Produktportfolio gemäß ihren ökonomischen Präferenzen wählen. So kann zum Beispiel ein Datengebender, der sich für einen sehr restriktiven Umgang mit seinen Daten entscheidet, ein Datennutzungsprodukt anbieten, das nur einen sehr geringen Zugang zu seinen privaten Daten und ihren Details ermöglicht. Damit einher geht auch eine geringe Verzinsung der Datenbereitstellung. Ein anderer Datengebender ist für einen höheren Ertrag bereit einen deutlich umfassenderen Zugang und höhere Detaillierungsgrade zu akzeptieren. Im Extremfall kann jemand vollständigen Zugang zu all seinen Daten ermöglichen, was dann durch den Datennutzenden mit hohen Renditen zu entgelten ist. Je nach Risikobereitschaft des Datengebenden könnte der Datentreuhänder also verschiedene Datenpakete verwalten und darauf aufbauend verschiedene Dienste anbieten, die mit gesteigerter Risikobereitschaft des Datengebenden auf dem in Kapitel 2.2.4 angesprochenen Leistungsspektrum immer weiter nach rechts wandern.

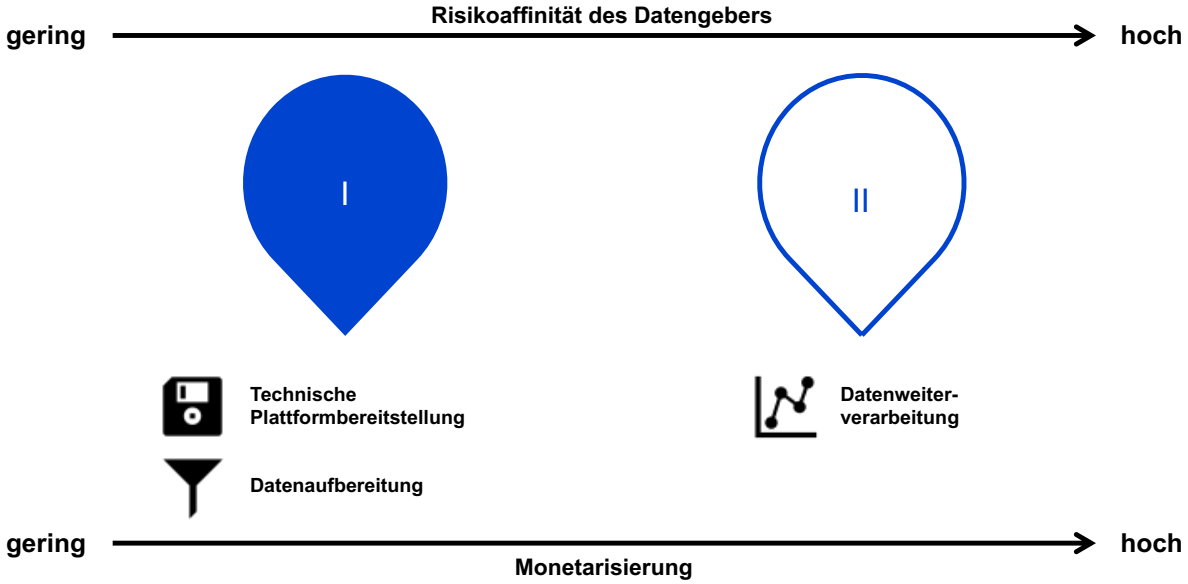


Abbildung 3 Zusammenhänge zwischen Risikoprofilen der Datengebenden, Leistungen des Datentreuhänders und der Ausgestaltung des Geschäftsmodells. Eigene Darstellung (Technopolis Group).

Die obige folgende Abbildung stellt diese Zusammenhänge grafisch dar: Die linke Instanz stellt die technische Verfügbarkeit sicher und bereitet Daten ggf. noch weiter auf. Datengebende mit geringerer Risikobereitschaft würden ihre Daten nur dieser Instanz zur Verfügung stellen, erhalten hierfür im Gegenzug aber auch einen geringeren monetären Betrag. Weitergehende Mehrwertdienste können in einer zweiten Instanz organisiert sein – die hier weiterverarbeiteten Daten stammen von risikoaffineren Datengebenden und werden höher bepreist, da durch die Mehrwertdienste ein höherer Nutzen zu erwarten ist.

5. Klassifikation von Datentreuhandmodellen

Die bisherigen Kapitel haben die diversen Anforderungen und Rahmenbedingungen bei der Ausgestaltung von Datentreuhändern aus technischer, rechtlicher und wirtschaftlicher Sicht beleuchtet. Das folgende Kapitel soll diese unterschiedlichen Ausgestaltungsmöglichkeiten abschließend zusammenfassen.

In der Literatur existieren unterschiedliche Ansätze zur Klassifikation von Datentreuhändern, die auf verschiedenen Unterscheidungsmerkmalen basieren. Blankertz et al. (2020) kategorisieren Datentreuhandmodelle etwa anhand ihrer Zielgruppe, also ob die Datengebenden Unternehmen oder Privatpersonen sind. Blankertz und Specht-Riemenschneider (2021) verwenden als Klassifikationskriterien die Art der Datenspeicherung und die Unterscheidung zwischen verpflichtender und freiwilliger Nutzung. Arlinghaus et al. (2021) gliedern Datentreuhänder nach ihrem Geschäftsmodell und ihrer Zugehörigkeit zum staatlichen oder privatwirtschaftlichen Bereich. Augsberg und Buchheim (2022) betonen die dauerhafte Speicherung von Daten sowie den Verbleib der Rechte als Unterscheidungsmerkmale. Feth & Rauch (2024) differenzieren zwischen Modellen, je nachdem, ob Rohdaten oder verarbeitete Daten vermittelt werden und ob der Zugang durch den Datentreuhänder oder die Datengebenden bestimmt wird. Kreutzer et al. (2024b) schließlich klassifizieren Modelle nach der Ausprägung der Zugangsberechtigung sowie den Compliance-Risiken.

Aus diesen Kategorisierungen wird ersichtlich, wie differenziert sich Datentreuhandmodelle betrachten lassen. Je nach Erkenntnisinteresse sind dabei ggf. verschiedene Kriterien von Bedeutung. Nachfolgend werden auf der Grundlage der bisherigen Diskussion die für das Erkenntnisinteresse dieser Studie relevanten Kriterien zusammengefasst. Entscheidend für die Wahl **technischer** Bausteine ist zunächst die Frage, welche Leistungen der Datentreuhänder aus technischer Sicht erfüllen soll: Ist er „nur“ dafür zuständig, Rohdaten technisch verfügbar zu machen oder bereitet er diese auf bzw. analysiert sie ggf. noch? Wie gelangen außerdem die Daten vom Gebenden zum Nutzenden: werden sie zentral beim Datentreuhänder gespeichert oder übernimmt der Datentreuhänder lediglich die Vermittlung der Daten, als zentraler Router oder Matchmaker (Peer-to-Peer)? Ausgehend von diesen Fragen entscheidet sich, was der Datentreuhänder mit den Daten macht. Mögliche Datenbehandlungsschritte sind die Standardisierung von Datenformaten, eine Qualitätsprüfung, Maßnahmen zu Anonymisierung, Pseudonymisierung und/oder Verschlüsselung sowie weitergehende Datenanalysen.

Welche **rechtlichen** Rahmenbedingungen für den Datentreuhänder gelten, hängt zunächst von der Art von Daten ab, die geteilt werden, und welche Schutzgründe diese haben: Hier kann unterschieden werden zwischen personenbezogenen Daten, Geschäftsgeheimnissen und/oder individuell schützenswerten Daten. Datentreuhänder, die personenbezogene Daten vermitteln, müssen sich zusätzlich an die Vorgaben der DSGVO halten. Je nachdem, ob sie dabei eine passive (an Fremdanweisungen gebunden) oder aktive Rolle (eigenverantwortlich handelnd) einnehmen, müssen sie dabei die Vorgaben von Auftragsverarbeitern oder

Verantwortlichen nach DSGVO einhalten. Der Datentreuhänder muss dafür sorgen, dass Nutzer nur Zugriff auf Daten erhalten, die ihren individuellen Berechtigungen entsprechen. Der Zugriff und die Nutzung von Daten kann dabei über verschiedene Modelle autorisiert werden, konkret nach Ermessen, obligatorisch, rollen- oder merkmalsbasiert.

Die technischen und rechtlichen Entscheidungen bestimmen wiederum die **geschäftliche** Ausgestaltung des Datentreuhänders. Weitere Kriterien, die für die Entwicklung eines Geschäftsmodells relevant sind, sind ob die Daten innerhalb einer Anwendungsdomäne oder domänenübergreifend geteilt werden sollen sowie in welchem Verhältnis Datengebende und -nutzende zueinanderstehen. Für welches Geschäftsmodell (mit oder ohne Gewinnorientierungsabsicht) und welche Organisationsform sich ein Datentreuhänder letztlich also entscheiden sollte und wie er die Vermittlung von Daten bestenfalls monetarisiert, hängt also von diversen Dimensionen ab, die sich je nach Anwendungsfall unterscheiden.

	Dimension	Ausprägungen					
Technische Ebene	**Daten**	Rohdaten		Aufbereitete Daten		Analysedaten	
	Datenhosting	Zentrale Datenhaltung		Zentraler Router		Peer-to-Peer	
	Datenbehandlung	Datenformat-standardisierung	Qualitätsprüfung	Anonymisierung	Pseudonymi-sierung	Verschlüsselung	Datenanalysen
Rechtliche Ebene	**Schutzgründe**	Personenbezogene Daten		Geschäftsgeheimnisse		Individuell schützenswerte Daten	
	Rollenverständnis DT	Auftragsverarbeiter			Verantwortlicher		
	Zugriffs- und Nutzungsverwaltung	Nach Ermessen	Obligatorisch		Rollenbasiert		merkmalsbasiert
Geschäftliche Ebene	**Domäne**	Eine Domäne			Domänenübergreifend		
	Datengeber	Unternehmen	Privatperson		Verwaltung/Behörde		Wissenschaft
	Datennutzer	Unternehmen	Privatperson		Verwaltung/Behörde		Wissenschaft
	Geschäftsmodell	Non-profit			For-profit		
	Organisationsform	Institutionelles Modell		Mitgliedsorientiertes Modell		Unternehmensmodell	
	Bepreisungsansatz	Pay-per-use nach Datenvolumen	Pay-per-use nach Anzahl Transaktionen	Abomodell	Mitgliedschaften	Gebühren für weitere Dienstleistungen	

Abbildung 4 Klassifikation von Datentreuhändern. Eigene Darstellung (Technopolis Group)

Abbildung 4 fasst die zentralen Dimensionen aus technischer, rechtlicher und wirtschaftlicher Sicht und ihre unterschiedlichen Ausprägungen zusammen. Diese Klassifikation kann als Grundlage und Orientierung für die Entwicklung von Datentreuhändern dienen.

6. Use Cases

Um die unterschiedlichen Ansätze von Datentreuhandmodellen zu analysieren, werden im Folgenden die Ansätze eines proprietären und eines öffentlichen Datentreuhänders im sekundären Gesundheitsmarkt gegenübergestellt. Dabei handelt es sich um Health-x dataLOFT (BMWK, Charité) und Device Connect for Fitbit (Google). Diese werden entlang ihrer technischen, wirtschaftlichen und rechtlichen Rahmenbedingungen aufgeschlüsselt. Relevante Informationen wurden über öffentlich verfügbare Informationen sowie Interviews gewonnen.

6.1 Health-X dataLOFT

Seit 2021 fördert das BMWK das Forschungsvorhaben Health-X dataLoft, das darauf abzielt, Bürger:innen in den Mittelpunkt der Bereitstellung, Nutzung und Kontrolle ihrer eigenen Gesundheitsdaten zu stellen. Dabei soll ein einheitlicher Markt für digitale Gesundheitsdienste geschaffen und das Potenzial der Gesundheitsdatenökonomie umfassend ausgeschöpft werden (Hussein et al., 2023; Kari et al., 2023). Der Vorstand des Konsortiums aus Industrie, Wissenschaft und Forschung obliegt dem Berlin Health Institute der Charité. Gesundheitsdaten aus dem ersten und zweiten Gesundheitsmarkt sollen in einem offenen, föderierten und rechtssicheren Datenraum mit Gaia-X-Technologie für verschiedene Szenarien in Forschung, Prävention und Versorgung nutzbar gemacht werden. Mögliche Anwendungsfelder umfassen bisher selbstbestimmte Alltagsgesundheit, klinische Begleitung, personalisierte Gesundheitsdienste, sowie die Sekundärnutzung von Daten (BIH 2024b). Health-X dataLOFT fördert als Gaia-X-Projekt die Vernetzung der Dateninfrastruktur für ein digitales europäisches Ökosystem und unterstützt so die Implementierung des EHDS, der einen einheitlichen europäischen Rahmen für den sicheren und gemeinwohlorientierten Austausch von Gesundheitsdaten schafft (Gersch et al., 2023).

6.1.1 Technische Grundlagen

Der Health-X dataLOFT ist als transparente, cloud-basierte Plattform konzipiert, die selbst keine Daten speichert, sondern lediglich eine sichere Verarbeitungsumgebung bereitstellt, und sich so bewusst von Big-Tech-Unternehmen abgrenzt (BIH, 2024b; Gersch et al., 2023; Reiberg et al., 2024). Die Datentreuhandstelle CenTrust der Bundesdruckerei übernimmt als neutrale und herstellerunabhängige Lösung die Datenverwaltung und stellt hierfür eine gesicherte und anwendungsoffene Infrastruktur bereit (Bundesdruckerei, 2024). Der Datentreuhandstelle auf dieser Ebene kommt dabei vorrangig eine vermittelnde Rolle zu, die die Daten verschlüsselt an den jeweiligen Anwendungsfall weiterleitet.

Um die Souveränität der Bürger und Bürgerinnen und Patienten und Patientinnen über ihre eigenen Daten sicherzustellen, bietet dataLOFT ein personalisiertes Datenraumkonzept. Diese Datenraumstruktur basiert auf rollenbasierten Zugriffsrechten und einem ID-Management-Service. So wird die sichere und eigenständige Verwaltung persönlicher Daten gewährleistet, während gleichzeitig die Verbindung zwischen primärem und sekundärem Gesundheitssektor gestärkt wird.

Dies schließt den Zugriff auf die elektronische Patientenakte (ePA) ein, deren Inhalte auf Wunsch der Patientinnen und Patienten auch für neue medizinische Portale nutzbar gemacht werden können (BIH, 2024b; Gieß et al., 2023).

Als technische Grundlage für die dataLOFT-Infrastruktur dient die European Data Space Association (EDA E.V.), die eine flexible Basis für eine Vielzahl von Use Cases schafft. Zwischen der zentralen Infrastruktur und den spezifischen Anwendungsfällen agieren dezentrale Datentreuhänder, die durch unterschiedliche Geschäftsmodelle anpassungsfähig und vielseitig einsetzbar sind. Dadurch kann dataLOFT auf unterschiedliche Anforderungen eingehen und den dezentralen Charakter des Systems wahren.

Ein wesentlicher Bestandteil des dataLOFT ist die Data Wallet App. Sie ermöglicht Patientinnen und Patienten eine selbstbestimmte Nutzung und Steuerung ihrer Gesundheitsdaten. Auf Basis des Gaia-X-konformen Technologie-Stacks unterstützt die Data Wallet nicht nur den Zugriff auf persönliche Daten, sondern erlaubt den betroffenen Personen auch, ihre Daten gezielt den Anbietenden auf der Plattform zugänglich zu machen, wenn Bedarf besteht. Diese App dient zugleich als zentrales Steuerungsinstrument, das prozessbasierte Interaktionen und die Integration verschiedener Datenbereiche ermöglicht (Appelt et al., 2023).

6.1.2 Rechtliche Grundlagen

Bis 2025 sollen EU-Mitgliedstaaten gesetzliche Grundlagen schaffen, um den digitalen Gesundheitsmarkt zu fördern und das Potenzial der Gesundheitsdatenwirtschaft auszuschöpfen. In diesem Kontext entwickelt Health-X dataLOFT auf Basis von Gaia-X einen nationalen Gesundheitsdatenspeicher, der perspektivisch auch auf europäischer Ebene eingesetzt werden könnte. Das Projekt, das als Gaia-X-konformer Datenraum gestaltet wird, orientiert sich dabei an den EHDS-Vorgaben und strebt danach, die Anforderungen des Data Governance Acts zu erfüllen. Besonders hervorzuheben ist, dass in diesem Modell Bürgerinnen und Bürger als zentrale Datenquelle dienen, was zusätzliche rechtliche Anforderungen erfordert. Health-X dataLOFT schafft deshalb gezielte Beteiligungsmöglichkeiten und sorgt für Transparenz über die Nutzung der Daten. Betroffene Personen können gezielt ihre Einwilligung für bestimmte Nutzungszwecke erteilen und werden über die tatsächliche Weiterverwendung informiert (Appelt et al., 2023).

In Deutschland wurde die Gematik GmbH als nationale Agentur für Digitale Medizin eingerichtet, die für die Telematikinfrastruktur (TI) im Gesundheitsbereich nach §306 SGB V zuständig ist. Damit baut die Gematik die digitale Infrastruktur für das deutsche Gesundheitswesen auf. Health-X dataLOFT integriert die rechtsverbindlichen Standards und Lösungen der Gematik für die TI. Die Gematik ist durch das Digitalagenturgesetz verpflichtet, den Aufbau und sicheren Betrieb dieser kritischen Infrastruktur zu gewährleisten und die Stabilität der Systeme abzusichern (BIH, 2024b).

6.1.3 Wirtschaftliche Grundlagen

Als datentreuhänderisches Modell bietet Health-X dataLOFT derzeit kostenfreie Basisdienste an. Für Drittanbieter sind jedoch individuell anpassbare B2B-Dienste,

etwa als "White-Label-Lösungen," geplant (BIH, 2024a). Health-X dataLOFT legt dabei den Fokus auf partizipative Datenräume, die offen und diskriminierungsfrei gestaltet sind und alle Akteure einbeziehen, die sich an gemeinsame Vorgaben halten.

Zur Verwaltung dieser Infrastruktur wählt Health-X die Form eines gemeinnützigen Vereins, um auf Infrastrukturebene keine Gewinnerzielungsabsicht zu verfolgen. Die verschiedenen Use Cases müssen jedoch eigenständig die Balance zwischen kommerzieller und gemeinwohlorientierter Datennutzung wahren. Ein zentrales Ziel ist dabei die datenschutzkonforme Sekundärnutzung im Rahmen des European Health Data Space (EHDS), wodurch Health-X sowohl wirtschaftlich nutzbare als auch gemeinwohlorientierte Daten fördert (Appelt et al., 2023).

Health-X konzentriert sich dabei auf die Entwicklung datenbasierter Geschäftsmodelle für die deutsch-europäische Gesundheitsindustrie, insbesondere für Gerätehersteller, Service-Provider und klinische Versorger (BIH, 2024a). Hierbei stehen Patientinnen und Patienten im Zentrum der Gestaltung, etwa durch Beteiligungsmöglichkeiten (Appelt et al., 2023). Zur Vergütung der Datennutzung werden drei Modelle diskutiert: Datentausch, der Zugang zu Diensten und eine monetäre Vergütung. Eine weitere Option besteht darin, dass Daten freiwillig für Forschungszwecke zur Verfügung gestellt werden, wobei die betroffenen Personen ihre Kontrolle über die Daten behalten (Jussen et al., 2024).

6.2 Device Connect for Fitbit

Das amerikanische Technologieunternehmen Fitbit ist bereits seit 2009 auf dem sekundären Gesundheitsmarkt aktiv – 2021 wurde das Unternehmen von Google akquiriert. Mittlerweile ermitteln Fitbit-Anwendungen wie Fitnesswatches und Smarttracker bis zu 91 Messwerte, die der präventiven und diagnostischen Nutzung im zweiten Gesundheitsmarkt dienen (Modrall, 2021).

Device Connect for Fitbit (DCF) ist eine seit September 2022 verfügbare Anwendung, die bei erfolgter Einwilligung das Telemonitoring von Patientinnen und Patienten erlaubt. Google verspricht, durch DCF Unternehmen des Gesundheitswesens und der Biowissenschaften mithilfe beschleunigter Analysen und tieferer Einblicke bei der Verbesserung der Gesundheitsversorgung zu unterstützen. Die Anwendung soll Gesundheitsorganisationen die Möglichkeit bieten, das Verhalten und die Gesundheitsentwicklung von Patientinnen und Patienten auch außerhalb klinischer Einrichtungen besser zu verstehen und Betreuung, Forschung sowie die Versorgung

gezielter zu optimieren (Lynch and Mcdonough, 2022).[5] Seit April 2024 können die Daten zudem über das Google Home System ausgelesen werden (Davies, 2024); eine automatische Einspeisung in e-Krankenakten zur unmittelbaren Verwendung im ersten Gesundheitssektor soll zurzeit erörtert werden (Kumar et al., 2024). Praxisrelevante Einblicke in DCF werden über das Pilotprojekt ME-TIME des Haga Ziekenhuis in Den Haag in Kooperation mit Fitbit und Google Cloud gewonnen, die mittels DCF eine neue Studie zur Früherkennung und Prävention von Gefäßerkrankungen durchführen (Kennedy, 2022). Die über einen Fitbit Tracker gesammelten Daten zum Aktivitätsniveau der Patientinnen und Patienten werden mit weiteren zuvor erhobenen klinischen Informationen verglichen, um potenzielle Muster oder Auffälligkeiten zu identifizieren, die auf bestimmte Herz-Kreislauf-Erkrankungen hinweisen könnten.

6.2.1 Technische Grundlagen

Der gesamte Prozess der Erhebung, Verarbeitung und Speicherung von Fitbit-Daten wird ausschließlich von Fitbit selbst verwaltet und ist organisatorisch und technisch von Google getrennt (Google, 2024). Diese strukturelle Trennung wurde implementiert, um den Wettbewerb zu schützen und geht auf die Entscheidung der EU-Kommission M.9660 (No. 139/2004) zurück, insbesondere auf die sogenannte "Ads Commitment"-Regelung (DG COMP, 2020). Zur Verwaltung der Daten verwendet Fitbit die Plattform Fitabase, die cloudbasiert und auf Industriestandards ausgerichtet ist.

Die Datenspeicherung erfolgt sowohl lokal auf dem Gerät und zugehörigen Anwendungen (Web-Interface, eWallet) sowie in der Cloud, sofern die Gerätsynchronisierung aktiviert ist (Almogbil 2024). Ehe die Daten auf die Cloud gelangen, werden sie nach einer gerätbasierten Verschlüsselung durch einen github-basierten Open-Source Daten-Connector gefiltert; Dies beinhaltet die Normalisierung und Standardisierung der Daten (Lynch and Mcdonough, 2022; Zwanenburg, 2022). Die in Fitabase gespeicherten Daten werden zudem anonymisiert, um die Privatsphäre der Gerätnutzenden zu schützen (fitabase, 2024; Mozilla, 2022). Dabei kommen auch Verschlüsselungsmethoden zum Einsatz, insbesondere der Advanced Encryption Standard (AES) und der Extended Tiny Encryption Algorithm (XTEA) (Al-Sabaawi et al., 2024). Eine standardisierte Registrierungs- und Einwilligungs-App ermöglicht Patientinnen und Patienten, ihre Datenzugriffsrechte und die Verwendung ihrer Daten transparent zu verwalten. Von der Cloud aus können die Daten (nach datenspe-

[5] Diese neue Lösung soll vor allem in den folgenden Anwendungsbereichen wertvolle Einblicke bieten: Vor- und Nachbehandlung von Patientinnen und Patienten, Management chronischer Erkrankungen wie Diabetes, präventive Programme zur Bevölkerungsgesundheit, Zulieferung von Lifestyle-Daten für klinische Forschung, sowie verbesserte Chancengleichheit im Gesundheitsbereich durch die Verknüpfung mit demographischen Daten (Lynch and Mcdonough, 2022).

zifischen Einverständnis durch die Gerätnutzenden) an Datennutzende weitergegeben werden (Zwanenburg, 2022). Erst dann können Datennutzende mittels der Fitbit Web API auf die freigegebenen Gesundheitsdaten zugreifen (Kennedy, 2022). Angeboten wird außerdem die Datenaufbereitung, -analyse und -veredelung durch Google-Tools wie BigQuery und andere, z.B. Looker, AutoML Tables und Vertex AI (Lynch and Mcdonough, 2022).

6.2.2 Rechtliche Grundlagen

Die Übernahme von Fitbit durch Google wurde durch die Europäische Kommission hinsichtlich der EU-Fusionskontrollverordnung umfassend geprüft. Bedenken bestanden darin, dass Google durch den Kauf (i) Zugriff auf eine umfangreiche Gesundheits- und Fitnessdatenbank der Nutzer erlangen und (ii) Fitbits Technologie für den Ausbau eigener Datenbanken nutzen könnte. Dies könnte Googles Position im Bereich personalisierte Werbung stärken und den Wettbewerb behindern. Zudem könnte Google den Zugang zur Fitbit-Web-API für andere Anbieter im Bereich digitaler Gesundheit einschränken, was besonders für Start-ups in der wachsenden europäischen Gesundheitsbranche nachteilig wäre. Auch wurde befürchtet, dass Google die Interoperabilität von Wearables mit Android-Geräten beschränken könnte. Die Kommission stellte jedoch fest, dass der europäische Markt für digitale Gesundheit noch im Aufbau ist und Fitbit im Smartwatch-Bereich nur einen kleinen Marktanteil besitzt. Zudem wird Google zur Einhaltung der DSGVO verpflichtet, um Gerätnutzenden volle Kontrolle über ihre Gesundheitsdaten zu garantieren.

Um die wettbewerbsrechtlichen Bedenken der Kommission auszuräumen, hat Google ferner folgende Zusagen gemacht:

1. **Werbung**: Google wird Fitbit-Gesundheitsdaten im EWR nicht für Werbezwekke verwenden. Diese Daten werden technisch von den anderen Google-Daten isoliert gespeichert, und Nutzer im EWR können wählen, ob sie ihre Fitbit-Daten für andere Google-Dienste freigeben möchten.
2. **Zugang zur Fitbit-API:** Google stellt sicher, dass Entwickler weiterhin auf die Fitbit-API zugreifen können, um auf Gesundheitsdaten mit Zustimmung der Gerätinhaber zu nutzen – ohne Gebühren.
3. **Android-Interoperabilität:** Google garantiert OEMs weiterhin kostenlosen Zugang zu Android-Schnittstellen, die die Interoperabilität von Wearables sichern, und verpflichtet sich, zukünftige Updates ebenfalls im Android Open Source Project (AOSP) zu veröffentlichen. Diskriminierende Nutzereinschränkungen für Wearables anderer Anbieter sind untersagt.

Diese Verpflichtungen gelten zehn Jahre, mit einer möglichen Verlängerung um weitere zehn Jahre für den Werbebereich. Ein unabhängiger Treuhänder überwacht die Einhaltung der Vorgaben (Europäische Kommission, 2020).

Fitbit verfügt zudem über eine eigene Datenschutzrichtlinie, die unabhängig von Google operiert und spezifische Schutzmaßnahmen vorschreibt (Mozilla, 2022). Demnach sind alle Weitergaben von personenbezogenen Daten nur mit ausdrücklicher Zustimmung der betroffenen Personen zulässig, ausgenommen in Fällen

gesetzlicher Verpflichtungen (Mozilla, 2022). Fitbit legt zudem großen Wert auf die sorgfältige Auswahl und Kontrolle von Drittanbietern, denen in Einzelfällen Zugriff auf Daten gewährt wird; diese Sorgfaltspflicht ist auch in den allgemeinen Lieferantenbedingungen fest verankert (Fitbit, 2021). Die aktive Freigabe bzw. Einwilligung zur Datennutzung durch Dritte erfolgt durch die DCF-Nutzenden mittels einer gemeinsamen Freigabeapp (Lynch and Mcdonough, 2022).

Seit August 2023 sieht sich Fitbit in Österreich, Italien und den Niederlanden allerdings einem Rechtsstreit gegenüber, der in Folge von Beschwerden wegen unzureichender Widerrufsmöglichkeiten bei Datenübermittlungen in Drittstaaten außerhalb der EU entfachte. Da betroffenen Nutzern keine Möglichkeit eingeräumt wurde, solchen Datenübermittlungen zu widersprechen, sehen die Kläger dies als Verstoß gegen die DSGVO-Vorgaben zur Datensouveränität und dem Recht auf Widerruf (noyb, 2023).

Auf den Kooperationsfall mit dem Haga Krankenhaus bezogen, erhielten die lokalen Sicherheits- und Datenschutzbeauftragten des Krankenhauses die Genehmigung zur Durchführung der Studie nach einer umfassenden Datenschutz-Folgenabschätzung, die zudem vom Ethikkomitee bestätigt wurde. Die Datenschutz-Folgenabschätzung beschreibt einen Datenmanagementplan, der den Anforderungen der europäischen Datenschutz-Grundverordnung (DSGVO) entspricht. Zum Schutz der Probandinnen und Probanden werden alle Daten pseudonymisiert; nur die Forschenden haben Zugang zu den Sensordaten, während nur der Forschungsleiter Zugriff auf persönliche Daten (z. B. Namen und Kontaktdaten) hat. Alle Beteiligten haben entsprechende Verarbeitungsvereinbarungen unterzeichnet. Die Speicherung der Daten erfolgt auf Google-Servern innerhalb der Niederlande, sodass die Daten nicht das Land verlassen und damit den niederländischen Vorschriften entsprechen (Naseri et al., 2023).

6.2.3 Wirtschaftliche Grundlagen

Das Geschäftsmodell von Google Device Connect for Fitbit basiert auf dem Ansatz von Software-as-a-Service (SaaS), welches dem Unternehmen ermöglicht, Gesundheitsdaten-Services zentralisiert über die Cloud anzubieten. Bei diesem Modell bleibt Google Eigentümer und Betreiber der zugrundeliegenden Software und Infrastruktur, während Kunden (bspw. Krankenhäuser und Forschungsinstitute) über ein Abonnement auf die benötigten Services zugreifen können, ohne selbst eigene Software installieren oder warten zu müssen. Die Verwaltung erfolgt vollständig cloudbasiert, was eine hohe Skalierbarkeit und Kosteneffizienz sicherstellt.

Durch die Einbindung der SaaS-Lösung bietet Google den Institutionen eine Vielzahl von Funktionen zur Analyse und Nutzung von Fitbit-Daten, die Google laufend an Marktnachfragen und Kundenbedürfnisse anpasst. Damit unterstützt das Modell einen schnellen und effizienten Einstieg in den Service (Onboarding), ermöglicht gleichzeitig regelmäßige Innovationen und erleichtert Multi-Tenant-Fähigkeit sowie Compliance, wie beispielsweise die Einhaltung der Datenschutzgrundverordnung (DSGVO). Das Google Device Connect Modell fördert die Monetarisierung der Dienste durch ein nutzungsbasiertes Lizenzmodell, was institutionelle Partner dazu befähigt, Gesundheitsdaten sicher und effizient für die Entwicklung von Gesundheitslösungen und

personalisierten Patientenservices einzusetzen, ohne eigene Server und spezialisierte IT-Ressourcen betreiben zu müssen.

Als proprietäres Datentreuhandmodell ist Fitbit zwar gewinnorientiert, fitabase jedoch ob der Forschungszentrierung nicht. Bis zum Merger stand der Datenzugriff Drittnutzern zudem entgeltfrei zur Verfügung (DG COMP, 2020). Seitdem bestehe eine umfassende Kooperation mit Drittanbietern, es erfolge aber kein Verkauf (Mozilla, 2022). Für DCF erfolgen jegliche Preisauskünfte nur auf Anfrage. Es bestehen Kooperation mit bluevector.ai, CitiusTech, Deloitte, und Omnigen (Lynch and Mcdonough, 2022).

6.3 Vergleich der beiden Use Cases

Technische Rahmenbedingungen: Health-X dataLOFT basiert auf einem dezentralen, Gaia-X-konformen Modell, das Daten nicht speichert, sondern ausschließlich als Vermittler agiert. Die Datenweiterleitung erfolgt sicher und verschlüsselt, wobei der Fokus auf dezentraler Datenspeicherung liegt. Die Rohdaten werden in ihrer Originalform belassen, ohne dass sie vorab aufbereitet oder analysiert werden. Die Plattform unterstützt Rollen- und ID-basierte Zugriffskontrollen, die es Nutzer und Nutzerinnen ermöglichen, ihre Gesundheitsdaten individuell zu verwalten und freizugeben. Im Gegensatz dazu verfolgt DCF einen zentralisierten Ansatz, bei dem Daten sowohl lokal als auch cloudbasiert gespeichert und zudem anonymisiert, normalisiert und standardisiert werden. Fitbit setzt auf eine Kombination aus zentraler Datenhaltung und Analysefunktionalitäten, was über eine Integration mit Tools wie Google BigQuery und AutoML erfolgt. Beide Modelle setzen auf Maßnahmen zur Verschlüsselung, um Datensicherheit zu gewährleisten.

Rechtliche Rahmenbedingungen: Health-X dataLOFT ist an die Vorgaben der DSGVO und EHDS-Richtlinien gebunden und bietet Nutzern und Nutzerinnen eine aktive Kontrolle über ihre personenbezogenen Daten. DCF hingegen unterliegt einer stärker regulierten Umgebung aufgrund der Übernahme durch Google. Es ist verpflichtet, Gesundheitsdaten von Werbedaten zu trennen und den API-Zugang für Drittentwickler zu gewährleisten. Beide Systeme stellen sicher, dass der Zugriff auf Daten ausschließlich autorisierten Nutzern und Nutzerinnen entsprechend ihrer Berechtigungen erlaubt ist.

Wirtschaftliche Rahmenbedingungen: Health-X verfolgt ein gemeinnütziges Geschäftsmodell, das auf die Förderung datenbasierter Geschäftsmodelle abzielt, ohne primär profitorientiert zu sein. Einnahmen generiert die Plattform durch optionalen Zugriff auf B2B-Dienste und White-Label-Lösungen. Das Modell orientiert sich an einer institutionellen Struktur, wie sie in Abbildung 4 beschrieben wird, und bindet Patient:innen aktiv in die Datenökonomie ein, beispielsweise durch Vergütungen oder die freiwillige Teilnahme an Forschungsprojekten. Im Gegensatz dazu verfolgt DCF ein gewinnorientiertes SaaS-Modell mit einer klaren Monetarisierungsstrategie, die sich an Unternehmen und Gesundheitsinstitutionen richtet. Die Skalierbarkeit und Effizienz des Systems werden durch die Integration in Google-Dienste erhöht, wobei der Fokus auf Abonnements und Pay-per-use-Ansätzen liegt.

7. Fazit und Ausblick

Wir befinden uns noch am Anfang des Datenzeitalters, in dem Menschen täglich Unmengen an Daten erzeugen. Bisher werden diese Daten jedoch noch viel zu wenig genutzt, und die „Datenmacht“ ist asymmetrisch verteilt, konzentriert sich auf einige wenige Akteure, vor allem auf große Tech-Unternehmen. Dies führt dazu, dass der Nutzen der Daten nicht allen zugutekommt. Zudem entfalten individuelle Daten oft nur aggregiert mit anderen Daten ihren vollen Nutzen. Als Gegenmodell hierzu ermöglichen dezentrale Datenräume mit etablierten semantischen Standards es, Daten aus verschiedenen Quellen und Anwendungen zu integrieren und miteinander zu verknüpfen. Semantische Technologien fördern die Interoperabilität und erleichtern auf technischer Ebene den Datenaustausch zwischen verschiedenen Anwendungen und Domänen. Datentreuhänder sind in einer solchen Form des Datenteilens als neutrale und vertrauenswürdige Intermediäre zwischen Datengebenden und -nutzenden notwendig, um sicherzustellen, dass die Daten nur für die vorgesehenen Zwecke verwendet und die Interessen aller Beteiligten geschützt werden. Sie sorgen für die Einhaltung von Sicherheits- und Qualitätsstandards, schaffen mehr Kontrolle und Transparenz über den Umgang mit Daten und steigern gleichzeitig die Verwertung von Daten. Datentreuhänder bieten damit eine vielversprechende Lösung, um die asymmetrische Verteilung der „Datenmacht“ zu überwinden und den Nutzen von Daten breiter zu streuen.

Durch ihre vielfältigen Funktionen, flexiblen organisatorischen Ansätze und nachhaltigen Finanzierungsmodelle können sie auch im Smart Living-Sektor einen wesentlichen Beitrag zur Entwicklung intelligenter und nachhaltiger Lebensumgebungen leisten. Denn vor dem Hintergrund der Konkurrenz der privaten Anbieter im zweiten Gesundheitsmarkt und Smart Living-Markt wird es entscheidend sein zu ergründen, wie die Vermittlung, Aufbereitung und Weiterverarbeitung von Daten rechtskonform erfolgt. Insbesondere die Einhaltung der Datenschutzgrundverordnung (DSGVO) und des Data Governance Acts (DGA) muss dabei sichergestellt sein. Datentreuhänder müssen dabei als neutrale und vertrauenswürdige Intermediäre agieren, die die Interessen von Datengebern und -nutzern wahren und hohe Sicherheits- und Qualitätsstandards einhalten.

Literaturverzeichnis

Al-Sabaawi, A., Al-Dulaimi, K., Zhao, Y., Simpson, L., 2024. Investigating data storage security and retrieval for Fitbit wearable devices. Health Technol. 14, 695–708. https://doi.org/10.1007/s12553-024-00885-0

Appelt, D., Kraemer, P., Reiberg, A., Smolén, A., 2023. Datentreuhänder, Datenvermittlungsdienste und Gaia-X. White Paper 2/2023 Version 2.0.

Arlinghaus, T., Kus, K., Kajüter, P., Teuteberg, F., 2021. Datentreuhandstellen gestalten: Status quo und Perspektiven für Geschäftsmodelle. HMD 58, 565–579. https://doi.org/10.1365/s40702-021-00727-x

Augsberg, S., Buchheim, J., 2022. Transaktionsbasierte Datentreuhand. JZ 77, 1139. https://doi.org/10.1628/jz-2022-0368

Baars, H., Weber, P., Tank, A., 2022. Institutionalizing Analytic Data Sharing in SME Ecosystems – A Role-Based Perspective.

BIH, 2024a. Use Cases [WWW Document]. health-X dataLOFT. URL https://www.health-x.org/use-cases (accessed 8.28.24).

BIH, 2024b. Plattform [WWW Document]. health-X dataLOFT. URL https://www.health-x.org/plattform (accessed 8.28.24).

Blankertz, A., 2020. Designing Data Trusts Why We Need to Test Consumer Data Trusts Now.

Blankertz, A., Specht, Prof.Dr.L., 2021. Wie eine Regulierung für Datentreuhänder aussehen sollte.

Blankertz, A., Specht-Riemenschneider, L., 2021. Wie eine Regulierung für Datentreuhänder aussehen sollte.

Blankertz, A., von Braunkohl, P., Kuzew, P., Richter, F., Richter, H., Schallbruch, M., 2020. Datentreuhandmodelle. Themenpapier.

Brauneck, A., Schmalhorst, L., 2024. Die Datentreuhand in der medizinischen Forschung - eine Untersuchung aus juristischer Perspektive, in: Buchholtz, G., Hering, L. (Eds.), Digital Health Und Recht. DUNCKER UND HUMBLOT. https://doi.org/10.3790/978-3-428-58889-3

Bundesdruckerei, 2024. Datentreuhänder: Sicherer Datenschutz nach DSGVO [WWW Document]. bdr. URL https://www.bundesdruckerei-gmbh.de/de/loesungen/datentreuhaender (accessed 8.28.24).

Carovano, G., Finck, M., 2023. Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy. Computer Law & Security Review 50, 105830. https://doi.org/10.1016/j.clsr.2023.105830

Chataut, R., Phoummalayvane, A., Akl, R., 2023. Unleashing the Power of IoT: A Comprehensive Review of IoT Applications and Future Prospects in Healthcare, Agriculture, Smart Homes, Smart Cities, and Industry 4.0. Sensors 23, 7194. https://doi.org/10.3390/s23167194

Davies, R., 2024. A new Google Home feature reads out your daily Fitbit stats with Google Assistant – but it should've been here three years ago. TechRadar. URL https://www.techradar.com/health-fitness/fitness-trackers/a-new-google-home-feature-reads-out-your-daily-fitbit-stats-with-google-assistant-but-it-shouldve-been-here-three-years-ago (accessed 8.27.24).

Denga, M., 2023. Die Corporate Governance von Datenintermediären. Zeitschrift für Unternehmens- und Gesellschaftsrecht 52, 611–671. https://doi.org/10.1515/zgr-2023-0022

DG COMP, 2020. Declaring a Concentration to be Compatible with the Internal Market and the EEA Agreement.

Dobler, M., Strittmatter, M., Treiterer, M., Meyer, J., Meierhofer, J., Benedech, R., Vogt, H., Kugler, P., 2023. Data Sharing Framework für KMU. Abschlussbericht 05/2023. Konstanz, Dornbirn, St. Gallen, Winterthur.

DSSC, 2024. Data Spaces Blueprint v1.5: Technical Building Blocks [WWW Document]. Data Spaces Support Centre. URL https://dssc.eu/space/bv15e/766066850/Technical+Building+Blocks (accessed 12.5.24).

Duarte, F., 2024. Amount of Data Created Daily. Exploding Topics. URL https://explodingtopics.com/blog/data-generated-per-day (accessed 9.25.24).

Europäische Kommission, 2023. Europäische Datenstrategie [WWW Document]. Europäische Kommission. URL https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de (accessed 11.21.24).

Europäische Kommission, 2020. Pressemitteilung. Fusionskontrolle: Kommission genehmigt Übernahme von Fitbit durch Google unter Auflagen [WWW Document]. European Commission. URL https://ec.europa.eu/commission/presscorner/detail/de/ip_20_2484 (accessed 11.7.24).

Feth, D., Rauch, B., 2024. Datentreuhänder in der Praxis. Datenschutz Datensich 48, 103–109. https://doi.org/10.1007/s11623-023-1889-3

fitabase, 2024. Pricing - Fitabase [WWW Document]. Fitabase. URL https://www.fitabase.com/how-it-works/pricing/ (accessed 10.18.24).

Fitbit, 2021. Fitbit Lieferantenbedingungen [WWW Document]. Google Fitbit. URL https://www.fitbit.com/global/de/legal/supplierterms (accessed 8.28.24).

Geminn, C.L., Johannes, P.C., Müller, J.K.M., Nebel, M., 2023. Data Governance in Germany – An Introduction. https://doi.org/10.17170/KOBRA-202304127800

Gersch, M., Schurig, T., Kari, A., 2023. Europäische Datenräume als öffentliche Güter und Wettbewerbsvorteil: 10 Jahre zu spät oder gerade noch rechtzeitig?! WINGbusiness 3, 26–31.

Gieß, A., Möller, F., Schoormann, T., Otto, B., 2023. Design Options for Data Spaces, in: ECIS 2023 Research Papers. Presented at the European Conference on Information Systems, Kristiansand (NO).

Google, 2024. Welche Daten Fitbit für Nutzer von Google-Konten erhebt - -Hilfe [WWW Document]. Google Support. URL https://support.google.com/product-documentation/answer/14811751?hl=de (accessed 8.28.24).

Grünewald, E., Pallas, F., 2021. Datensouveränität für Verbraucher:innen: Technische Ansätze durch KI-basierte Transparenz und Auskunft im Kontext der DSGVO. Presented at the Alexander Boden, Timo Jakobi, Gunnar Stevens, Christian Bala (Hgg.): Verbraucherdatenschutz - Technik und Regulation zur Unterstützung des Individuums, pp. 1–17. https://doi.org/10.18418/978-3-96043-095-7_02

Hardinges, J., Wells, P., Blandford, A., Tennison, J., Scott, A., 2019. Data trusts: lessons from three pilots.

Hennemann, M., 2022. Die Regulierung von Datenintermediären. Der Entwurf des Data Governance Act.

Hussein, R., Scherdel, L., Nicolet, F., Martin-Sanchez, F., 2023. Towards the European Health Data Space (EHDS) ecosystem: A survey research on future health data scenarios. International Journal of Medical Informatics 170, 104949. https://doi.org/10.1016/j.ijmedinf.2022.104949

Jussen, I., Möller, F., Schweihoff, J., Gieß, A., Giussani, G., Otto, B., 2024. Issues in inter-organizational data sharing: Findings from practice and research challenges. Data & Knowledge Engineering 150, 102280. https://doi.org/10.1016/j.datak.2024.102280

Jussen, I., Schweihoff, J., Dahms, V., Möller, F., Otto, B., 2023. Data Sharing Fundamentals: Definition and Characteristics.

Kari, A., Schurig, T., Gersch, M., 2023. European Health Data Space (EHDS), Gaia-X and Health-X dataLOFT.

Kathuria, V., 2024. Comparative Assessment of Non-Personal Data Access Frameworks. SSRN Journal. https://doi.org/10.2139/ssrn.4746707

Kennedy, S., 2022. Google, Fitbit Launch Data-Driven Remote Patient Monitoring Solution | TechTarget [WWW Document]. Healthtech Analytics. URL https://www.techtarget.com/healthtechanalytics/news/366590617/Google-Fitbit-Launch-Data-Driven-Remote-Patient-Monitoring-Solution (accessed 8.27.24).

Kreutzer, S., Heimer, Prof.Dr.T., Bauer, F., Rabe, L., Blind, Prof.Dr.K., Martin, Dr.N., Grafenstein, Prof.Dr.M. von, Streblow, Prof.Dr.R., Du, J., Schölzel, J., 2024a. Wissenschaftliche Begleitforschung von Pilotprojekten zur Entwicklung und praktischen Erprobung von Datentreuhandmodellen in den Bereichen Forschung und Wirtschaft. Kurzpapier.

Kreutzer, S., Heimer, Prof.Dr.T., Nachtigall, H., Pschorn, L., Bauer, F., Blind, Prof.Dr.K., Martin, Dr.N., Grafenstein, Prof.Dr.M. von, Streblow, Prof.Dr.R., Du, J., Schölzel, J., 2024b. Wissenschaftliche Begleitung und Vernetzung der Projekte zur Entwicklung und praktischen Erprobung von Datentreuhandmodellen in den Bereichen Forschung und Wirtschaft. Bericht zu Arbeitspaket 1.2: Anforderungen und Umsetzungshemmnisse für Datentreuhandmodelle.

Kreutzer, S., Heimer, Prof.Dr.T., Nachtigall, H., Pschorn, L., Waiblinger, F., Blind, Prof.Dr.K., Martin, Dr.N., Horvat, Dr.D., Grafenstein, Prof.Dr.M. von, Schweinberg, M., Streblow, Prof.Dr.R., Du, J., Schölzel, J., 2024c. Wissenschaftliche Begleitung und Vernetzung der Projekte zur Entwicklung und praktischen Erprobung von Datentreuhandmodellen in den Bereichen Forschung und Wirtschaft. Arbeitspaket 1.1 Bestandsaufnahme.

Krotova, A., Rusche, C., Spiekermann, M., 2019. Die ökonomische Bewertung von Daten: Verfahren, Beispiele und Anwendungen = The economic evaluation of data: procedures, examples and applications, IW-Analysen. Institut der deutschen Wirtschaft Köln Medien GmbH, Köln.

Küfeoğlu, S., Açıkgöz, E., Taşcı, Y.E., Arslan, T.Y., Priesmann, J., Praktiknjo, A., 2022. Designing the Business Ecosystem of a Decentralised Energy Datahub. Energies 15, 650. https://doi.org/10.3390/en15020650

Kumar, P.C., Zimmer, M., Vitak, J., 2024. A Roadmap for Applying the Contextual Integrity Framework in Qualitative Privacy Research. Proc. ACM Hum.-Comput. Interact. 8, 1–29. https://doi.org/10.1145/3653710

Lauf, F., Scheider, S., Friese, J., Kilz, S., Radic, M., Burmann, A., 2023. Exploring Design Characteristics of Data Trustees in Healthcare - Taxonomy and Archetypes. ECIS 2023 Research Papers.

Lindner, M., Straub, S., 2023. Datentreuhänderschaft. Status Quo und Entwicklungsperspektiven.

Lipovetskaja, A., Ciftci, S.A., Schweihoff, J., Janiesch, C., Möller, F., 2024. Business Model Types for Data Trustees. Presented at the 19th International Conference on Wirtschaftsinformatik, Würzburg.

Lynch, A.H., Mcdonough, A., 2022. Device Connect for Fitbit, powered by Google Cloud. Google Cloud Blog. URL https://cloud.google.com/blog/topics/healthcare-life-sciences/device-connect-for-fitbit-powered-by-google-cloud (accessed 8.27.24).

Micheli, M., Farrell, Eimear, Carballa-Smichowski, B., Posada-Sánchez, M., Signorelli, S., Vespe, M., 2023. Mapping the landscape of data intermediaries: emerging models for more inclusive data governance. EU Publications Office, LU.

Modrall, J., 2021. Google/Fitbit - The EU Commission Misses a Step. Kluwer Competition Law Blog. URL https://competitionlawblog.kluwercompetitionlaw.com/2021/06/17/google-fitbit-the-eu-commission-misses-a-step/ (accessed 8.27.24).

Moering, J., Wendt, F., 2024. Mieter fühlen sich überwacht: Ärger um Rauchmelder in Vonovia-Wohnungen eskaliert [WWW Document]. hessenschau.de. URL https://www.hessenschau.de/wirtschaft/aerger-um-neue-rauchmelder-in-vonovia-wohnungen-eskaliert-v1,vonovia-aerger-um-rauchmelder-100.html (accessed 12.5.24).

Mozilla, 2022. Fitbit. Leitfaden zu Datenschutz und -sicherheit. Mozilla. URL https://foundation.mozilla.org/de/privacynotincluded/fitbit/ (accessed 8.27.24).

Naseri, A., Tax, D., Van Der Harst, P., Reinders, M., Van Der Bilt, I., 2023. Data-efficient machine learning methods in the ME-TIME study: Rationale and design of a longitudinal study to detect atrial fibrillation and heart failure from wearables. Cardiovascular Digital Health Journal 4, 165–172. https://doi.org/10.1016/j.cvdhj.2023.09.001

noyb, 2023. Deine Fitbit ist nutzlos – außer du akzeptierst illegale Datentransfers [WWW Document]. noyb. URL https://noyb.eu/de/your-fitbit-useless-unless-you-consent-unlawful-data-sharing (accessed 8.27.24).

Opriel, S., Möller, F., Burkhardt, U., Otto, B., 2021. Requirements for Usage Control based Exchange of Sensitive Data in Automotive Supply Chains. Presented at the Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2021.051

Otto, B., Ten Hompel, M., Wrobel, S. (Eds.), 2022. Designing Data Spaces: The Ecosystem Approach to Competitive Advantage. Springer International Publishing, Cham. https://doi.org/10.1007/978-3-030-93975-5

Otto, Prof.Dr.-Ing.B., Mohr, Prof.Dr.N., Roggendorf, Dr.M., Guggenberger, T., 2020. Data sharing in industrial ecosystems: Driving value across entire production lines. Dortmund, Düsseldorf, Berlin.

Pavel, V., Kind, C., Strait, A., Reeve, O., Peppin, A., Szymielewicz, K., Veale, M., MacDonald, R., Lynskey, O., Coyle, D., Nemitz, P., 2022. Rethinking data and rebalancing digital power (Report). Ada Lovelace Institute, London, UK.

Rainey, L., Lutomski, J.E., Broeders, M.J., 2023. FAIR data sharing: An international perspective on why medical researchers are lagging behind. Big Data & Society 10, 205395172311710. https://doi.org/10.1177/20539517231171052

Reiberg, A., Niebel, C., Schmitz, A.-R., 2024. Governance von Datenräumen: Akteure, Strukturen und Phasen der Datenraum-Governance, in: Friedewald, M., Roßnagel, A., Geminn, C.L., Karaboga, M., Schindler, S. (Eds.), Data Sharing – Datenkapitalismus by Default? Nomos Verlagsgesellschaft mbH & Co. KG, pp. 49–74. https://doi.org/10.5771/9783748940173-49

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 International 72, 458–470. https://doi.org/10.1093/grurint/ikad014

Schneider, I., 2022. Datentreuhandschaft durch Intermediäre. Chancen, Herausforderungen und Implikationen.

Schönwerth, D., 2024. Deutsche Unternehmen nutzen ihre Daten kaum [WWW Document]. Bitkom e.V. URL https://www.bitkom.org/Presse/Presseinformation/Datenoekonomie-Deutschland-2024 (accessed 9.25.24).

Schulz-Dieterich, A., Alberternst, S., Ebersberger, L., Galen, A., Güney, S., Hoffmann, Dr.H., Kremer, Dr.M., Mackensen, M., Milojkovic, F., Ta, D.P., Weißkirchen, E., 2024. Systemkonzept ForeSightNEXT, 1.00. ed, SmartLivingNEXT. SmartLivingNEXT Projektbüro Forschungsvereinigung Elektrotechnik beim ZVEI e.v., Frankfurt.

Specht-Riemenschneider, L., Kerber, W., 2022. Datentreuhänder - ein problemlösungsorientierter Ansatz = Designing data trustees - a purpose-based approach. Berlin Konrad-Adenauer-Stiftung e. V. 2022.

Stachon, M., Guggenberger, T., Möller, F., Tomczyk, M., 2023. Understanding Data Trusts. Presented at the Thirty-first European Conference on Information Systems (ECIS 2023), Kristiansand (Norway).

Stefanija, A.P., Buelens, B., Goesaert, E., Lenaerts, T., Pierson, J., Van den Bussche, J., 2023. Toward a Solid Acceptance of the Decentralized Web of Personal Data: Societal and Technological Convergence. Commun. ACM 67, 43–46. https://doi.org/10.1145/3624555

Vailshery, L.S., 2024. Number of IoT Connections Worldwide 2022-2033 [WWW Document]. Statista. URL https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (accessed 10.18.24).

Wadephul, C., 2022. Datensouveränität durch Datenintermediäre? Eine Kritik am Beispiel der Datenschutzgrundverordnung (DSGVO) und dem Versuch einer risikobasierten Regulierung von KI und automatisierten Entscheidungssystemen (AES).

Wilkinson, M.D., Dumontier, M., Aalbersberg, Ij.J., Appleton, G., Axton, M., Baak, A., Blomberg, N., Boiten, J.-W., da Silva Santos, L.B., Bourne, P.E., Bouwman, J., Brookes, A.J., Clark, T., Crosas, M., Dillo, I., Dumon, O., Edmunds, S., Evelo, C.T., Finkers, R., Gonzalez-Beltran, A., Gray, A.J.G., Groth, P., Goble, C., Grethe, J.S., Heringa, J., 't Hoen, P.A.C., Hooft, R., Kuhn, T., Kok, R., Kok, J., Lusher, S.J., Martone, M.E., Mons, A., Packer, A.L., Persson, B., Rocca-Serra, P., Roos, M., van Schaik, R., Sansone, S.-A., Schultes, E., Sengstag, T., Slater, T., Strawn, G., Swertz, M.A., Thompson, M., van der Lei, J., van Mulligen, E., Velterop, J., Waagmeester, A., Wittenburg, P., Wolstencroft, K., Zhao, J., Mons, B., 2016. The FAIR Guiding Principles for scientific data management and stewardship. Sci Data 3, 160018. https://doi.org/10.1038/sdata.2016.18

Zwanenburg, E., 2022. Google Cloud, Fitbit, Haga collaborate on pilot heart study. Google Cloud Blog. URL https://cloud.google.com/blog/topics/healthcare-life-sciences/google-cloud-fitbit-haga-collaborate-on-pilot-heart-study (accessed 8.28.24).