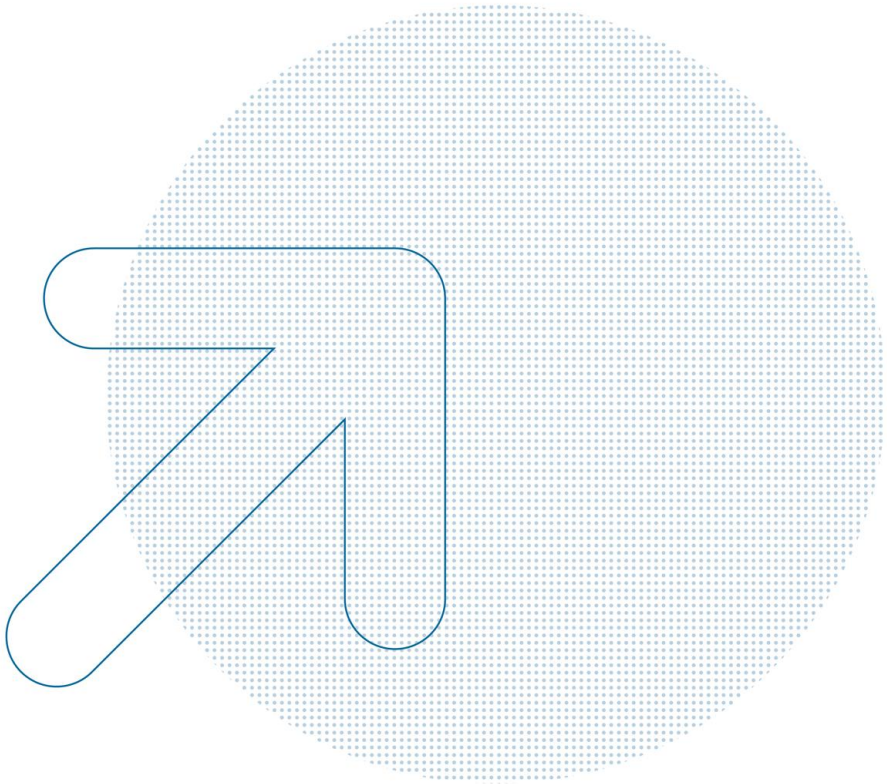
WIK-Consult • Bericht

Studie für die Bundesnetzagentur



Umsetzung des Data Act in Deutschland

Abschlussbericht

Autoren:
Christian Märkel, Marina Happ, Dagmar Gesmann-Nuissl, Serpil Taş,
Martin Lundborg, Lukas Wiewiorra

Bad Honnef, 11.07.2025

WIK CONSULT

Impressum

WIK-Consult GmbH
Rhöndorfer Str. 68
53604 Bad Honnef
Deutschland
Tel.: +49 2224 9225-0
Fax: +49 2224 9225-63
E-Mail: info@wik-consult.com
www.wik-consult.com

Vertretungs- und zeichnungsberechtigte Personen

Geschäftsführung	Dr. Cara Schwarz-Schilling (Vorsitzende der Geschäftsführung)
	Alex Kalevi Dieke (Kaufmännischer Geschäftsführer)
Prokuristen	Prof. Dr. Bernd Sörries
	Dr. Christian Wernick
	Dr. Lukas Wiewiorra
Vorsitzender des Aufsichtsrates	Dr. Thomas Solbach
Handelsregister	Amtsgericht Siegburg, HRB 7043
Steuer-Nr.	222/5751/0926
Umsatzsteueridentifikations-Nr.	DE 329 763 261

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

EXECUTIVE SUMMARY [DE]

Untersucht wurden die im Data Act enthaltenen Regelungen zum B2B- und B2C-Sharing (im Wesentlichen Kapitel II – IV des Data Act), mit den folgenden drei Schwerpunkten:

- Eine anschauliche Darstellung und Aufbereitung der Ausgestaltung der Regeln im Data Act entlang der Datenwertschöpfungskette (d.h. in Bezug auf Datenzugang und -bereitstellung sowie Datennutzung und -weitergabe) (Teil I).
- Eine empirische Identifizierung der für den Data Act relevantesten Sektoren in Deutschland sowie eine Analyse relevanter Anbieter in diesen Sektoren (Teil II).
- Eine tiefergehende Analyse der Anwendungsherausforderungen bezüglich Datenschutzrecht und Geschäftsgeheimnisse (Teil III).

TEIL I: Data Sharing gemäß Data Act: Zielsetzung, Anwendungsbereich & Ablauf

Der Data Act hat im Bereich des Data Sharing die Intention, die Mehrfachnutzung der Daten, die durch die Nutzung von vernetzten Produkten und verbundenen Diensten generiert werden, zu ermöglichen. Eine Analyse der im Data Act festgelegten Regelungen zum Data Sharing entlang der Datenwertschöpfungskette zeigt, dass die Mehrfachnutzung der Daten über eine Stärkung der Position des Nutzers erreicht werden soll. Dies gilt für alle Schritte des Datenzugangs, der Datenbereitstellung, der Datennutzung sowie der Datenweitergabe.

Für Nutzer vernetzter Produkte und verbundener Dienste werden Datenzugangsrechte geschaffen, und dadurch die Verfügungsrechte über die Nutzung der Daten bei ihnen konzentriert. Damit soll die gegenwärtige de facto-Kontrolle über die von vernetzten Produkten und verbundenen Diensten generierten Daten durch den Dateninhaber bzw. Hersteller aufgebrochen werden. Die Rechtfertigung für diese Nutzerzentrierung im Data Act wird darin gesehen, dass zur Datengenerierung sowohl der Hersteller / Dateninhaber (durch die Konzeption des Produkts / Dienstes) als auch der Nutzer (durch die Nutzung des Produkts / Dienstes) beitragen. Da die Daten durch den Dateninhaber erfasst werden und dieser somit eine stärkere Ausgangsposition innehat, werden die Nutzer durch den Data Act in ihren Rechten gestärkt. Dies führt zu einem ausgeglicheneren Machtverhältnis zwischen Nutzer und Dateninhaber.

Der Anwendungsbereich des Data Act umfasst sowohl personenbezogene sowie nicht-personenbezogene Daten, wobei für personenbezogene Daten ein Regelungsvorrang der DSGVO besteht. Unter den Data Act fallen Rohdaten und vorverarbeitete Daten inklusive der zugehörigen Metadaten. Informationen, die aus den Produktdaten geschlussfolgert oder abgeleitet sind (bspw. durch Sensorfusion), fallen hingegen nicht unter den Data Act und müssen demnach nicht mit dem Nutzer bzw. einer Drittpartei geteilt werden. Im Einzelfall kann es jedoch schwierig sein, eine klare Grenze zwischen dem reinen Datum und einer daraus abgeleiteten Information zu ziehen (siehe hierzu auch Teil III).

TEIL II: Empirische Sektor- und Anbieteranalyse

Der Data Act als horizontale Regulierung ist grundsätzlich für alle Wirtschaftszweige gemäß gängiger Klassifikationssysteme; NACE, WZ 2008) von Bedeutung. Durch die Analyse in der vorliegenden Studie kann jedoch gezeigt werden, dass insbesondere 11 Sektoren in ihrer Relevanz für den Data Act hervorstechen. Insgesamt kann auf Basis der European Data Market Study davon ausgegangen werden, dass in Deutschland bis zu 50.000 Unternehmen vom DA betroffen sind.

- Eine hohe IoT-Durchdringung ist insbesondere im verarbeitenden Gewerbe zu verzeichnen, insbesondere in den Bereichen Industrielles IoT als auch im Bereich Automotive IoT.
- Darüber hinaus sticht der IKT-Sektor in seiner Relevanz für den Data Act hervor, hier insbesondere im Bereich Consumer IoT.
- Im Bereich des öffentlichen Sektors ist vor allem der Bereich Smart City von Bedeutung. Dieser weist im Hinblick auf die IoT-Verbindungen eine der höchsten prognostizierten Wachstumsraten im Zeitraum von 2024-28 auf. Damit gehört der Smart City-Sektor zu einem der wichtigsten Segmente im IoT-Markt und hat somit auch für den Data Act eine besondere Bedeutung.
- Auch der Gesundheitssektor zeigt eine hohe Relevanz, was u.a. daran abgelesen werden kann, dass der Medizinbereich den höchsten Umsatzanteil im deutschen Robotik-Markt erzielt.
- Neben den bisher genannten Branchen kann gezeigt werden, dass auch den Sektoren Verkehr und Lagerei, Energie(versorgung), Handel & Instandhaltung und Reparatur von Kfz sowie dem Bereich Landwirtschaft. Forstwirtschaft und Fischerei eine besondere Bedeutung im Hinblick auf den Data Act zukommt.

Zusammenfassend sind die identifizierten Sektoren in Tabelle 1 aufgeführt:

Tabelle 1: Vom Data Act besonders stark betroffene Branchen

Industrielles IoT **Automotive IoT** **Sonstiges verarbeitende Gewerbe**	Verarbeitendes Gewerbe
Consumer IoT **Sonstiger IKT-Sektor**	Information und Kommunikation
Smart City	Öffentlicher Sektor
Energie(-versorgung)	
Gesundheits- und Sozialwesen	
Verkehr und Lagerei	
Handel; Instandhaltung und Reparatur von Kfz	
Landwirtschaft, Forstwirtschaft und Fischerei	

Quelle: Eigene Darstellung.

Neben den Sektoren wurden im Zuge der Anbieteranalyse auch eine Stichprobe von 500 als potentiell relevant eingeschätzten Unternehmen in diesen Sektoren näher untersucht. Dabei wurden relevante Unternehmen identifiziert, die sich in den 11 ermittelten Sektoren bewegen. Hierzu wurde sowohl auf qualitative als auch quantitative Indikatoren zurückgegriffen.

- Die Analyse zeigt, dass die Relevanz im Kontext des DA für ca. ein Drittel der Unternehmen in der betrachteten Stichprobe bereits mit öffentlich verfügbaren Informationen nachgewiesen werden konnte.
- Mehr als die Hälfte dieser Unternehmen sind dem IKT-Sektor zuzuordnen.
- Mehr als ein Drittel dieser Unternehmen fallen in den Bereich des verarbeitenden Gewerbes.

Die Anbieteranalyse untermauert damit die besonders hervorgehobene Rolle dieser beiden Sektoren für die Relevanz des Data Act. Ca. 80% der identifizierten Unternehmen sind hauptsächlich im Business-to-Business-Umfeld (B2B) unterwegs.

TEIL III: Ausgewählte Anwendungsherausforderungen des Data Act

In der Studie wurden tiefergehenden Analysen zu zwei Anwendungsherausforderungen durchgeführt. Zum einen wurde das Überschneiden der Anwendungsbereiche von Data Act und DSGVO für personenbezogene Daten analysiert. Zum anderen wurde der Umgang mit Geschäftsgeheimnissen im Data Act und das daraus folgende Spannungsfeld zwischen der Gewährung des Datenzugangs und dem Aufrechterhalten von Innovationsanreizen näher betrachtet.

Mit Blick auf das Überschneiden der Anwendungsbereiche von Data Act und DSGVO zeigt sich, dass sich insbesondere für den Dateninhaber eine Dilemmasituation ergeben kann. Um die widerstreitenden Interessen der beiden Rechtsakte zu versöhnen, bedarf es zur Weitergabe personenbezogener Daten einer Legitimationsgrundlage. Sofern Nutzer und betroffene Personen identisch sind, kann bereits das Datenherausgabeverlangen als Einwilligung i.S. des Art. 6 DSGVO und damit als Legitimationsgrundlage angesehen werden. Anderes gilt jedoch, wenn Nutzer und betroffene Personen verschieden sind. In dieser Konstellation bedarf es der Synchronisierung von Data Act und DSGVO über Rechtfertigungstatbestände. Neben dem Erfüllen eines „berechtigten Interesses“ (Art. 6 (1 lit. f) DSGVO), das hohe Anforderungen an den notwendigen Abwägungsprozess stellt, kann ein Datenvertrag zwischen Dateninhaber und Nutzer helfen. Er kann die Interessen aller Beteiligten (Nutzer, Dateninhaber, Betroffener und Datenempfänger) aufnehmen und austarieren sowie die Verantwortlichkeiten zur Sicherstellung der datenschutzrechtlichen Anforderungen festlegen.

Der Gesetzgeber hat bei der prinzipiellen Inklusion von Geschäftsgeheimnissen in die Datenzugangsansprüche der Datenempfänger versucht, mögliche Schlupflöcher für Dateninhaber zum Umgehen des Data Sharing zu schließen. Über technische und organisatorische Maßnahmen (TOMs), welche vom Dateninhaber zum Schutz der Daten

gegenüber dem Nutzer eingefordert werden können, wird beabsichtigt, die Interessen der Dateninhaber und Nutzer bzw. Datenempfänger beim Vorliegen von Geschäftsgeheimnissen auszutarieren. Beim Dateninhaber verbleiben jedoch Ermessensspielräume im Hinblick auf die Deklaration von Geschäftsgeheimnissen sowie die Einforderung von TOMs zum Schutz dieser. Diese Ermessensspielräume entstehen insbesondere dadurch, dass der Dateninhaber aufgrund der Vertraulichkeit der Geschäftsgeheimnisse einen Informationsvorsprung gegenüber den Nutzern bzw. Datenempfängern (und der Aufsichtsbehörde) hat. Aus diesen Informationsasymmetrien resultiert für den Dateninhaber ein zweifacher Anreiz zum „Overclaiming“: Sowohl im Hinblick auf das Vorliegen eines Geschäftsgeheimnisses selbst als auch in einem weiteren Schritt im Hinblick auf das Einfordern von TOMs.

Dieses Overclaiming steht der Intention des Data Act entgegen und ist mit Einbußen des vom Data Act ausgehenden Wohlfahrtspotenzials verbunden. Der Gesetzgeber sollte daher für diese Overclaiming-Problematik sensibilisiert sein und wenn nötig, geeignete Gegenmaßnahmen ergreifen. Insbesondere für kleine und mittlere Unternehmen könnte es z. B. zielführend sein, diese bei der Implementierung von TOMs zu unterstützen, um so die Transaktionskosten der Inanspruchnahme der Datenzugangsrechte zu senken und Overclaiming als Strategie für den Dateninhaber unattraktiver zu machen.

EXECUTIVE SUMMARY [EN]

The regulations on B2B and B2C data sharing contained in the Data Act (essentially Chapters II - IV of the Data Act) were examined, with the following three focal points:

- A clear presentation and preparation of the structure of the rules in the Data Act along the data value chain (i.e. in relation to data access and data provision as well as data use and data transfer) (Part I)
- An empirical identification of the most relevant sectors for the Data Act in Germany and an analysis of relevant providers in these sectors (Part II).
- An in-depth analysis of the application challenges regarding data protection law and trade secrets (Part III).

PART I: Data sharing in accordance with the Data Act: Objectives, scope of application & procedure

The intention of the Data Act in the area of data sharing is to enable the multiple use of data generated through the use of connected products and related services. An analysis of the Data Act's regulations on data sharing along the data value chain shows that the multiple use of data is to be achieved by strengthening the position of the user. This applies to all steps of data access, data provision, data use and data transfer.

Data access rights are created for users of connected products and related services, thereby concentrating the rights of disposal over the use of the data with them. This is intended to break up the current de facto control over the data generated by connected products and related services by the data holder or manufacturer. The justification for this user-centric approach in the Data Act is seen in the fact that both the manufacturer/data holder (through the design of the product/service) and the user (through the use of the product/service) contribute to data generation. As the data is collected by the data holder, who therefore has a stronger starting position, the Data Act strengthens the rights of users. This leads to a more balanced power relationship between the user and the data holder.

The scope of the Data Act includes both personal and non-personal data, with the GDPR taking precedence for personal data. The Data Act covers raw data and pre-processed data, including the associated metadata. However, information that is inferred or derived from the product data (e.g. through sensor fusion) is not covered by the Data Act and therefore does not have to be shared with the user or a third party. In individual cases, however, it can be difficult to draw a clear line between pure data and information derived from it (see also Part III).

PART II: Empirical sector and provider analysis

As a horizontal regulation, the Data Act is generally relevant for all economic sectors according to common classification systems (NACE, WZ 2008). However, the analysis in

this study at shows that 11 sectors in particular stand out in terms of their relevance for the Data Act. Overall, based on the European Data Market Study, it can be assumed that up to 50,000 companies in Germany are affected by the DA.

- IoT penetration is particularly high in the **manufacturing industry**, especially in the areas of **Industrial IoT** and **Automotive IoT.**
- The ICT sector also stands out in terms of its relevance to the Data Act, particularly the area of **Consumer IoT**.
- In the public sector, the **Smart City** area is particularly important. In terms of IoT connections, it has one of the highest forecast growth rates in the period from 2024-28. This makes the smart city sector one of the most important segments in the IoT market and therefore also of particular importance for the Data Act.
- The **healthcare sector** is also highly relevant, as can be seen from the fact that the medical sector generates the highest share of sales in the German robotics market.
- In addition to the sectors mentioned so far, it can be shown that the **transport and storage**, **energy (supply), trade & maintenance and repair of motor vehicles** as well as the **agriculture, forestry and fishing sectors** are also of particular importance with regard to the Data Act. The identified sectors are summarized in the figure below.

Table 1: Sectors particularly affected by the Data Act

Industrial IoT **Automotive IoT** **Other manufacturing industry**	Manufacturing industry
Consumer IoT **Other IoT sector**	Information and communication
Smart City	Public sector
Energy(supply)	
Health and social services	
Transportation and warehousing	
Trade; maintenance and repair of motor vehicles	
Agriculture, forestry and fisheries	

Source: Own presentation.

In addition to the sectors, the provider analysis also examined a sample of 500 companies in these sectors that were considered potentially relevant. This identified relevant companies operating in the 11 sectors identified. Both qualitative and quantitative indicators were used for this purpose.

- The analysis shows that the relevance in the context of the DA of approximately one third of the companies in the sample could already be demonstrated using publicly available information.
- More than half of the companies identified belong to the ICT sector.
- More than a third of the companies are in the manufacturing sector.

The provider analysis thus underpins the particularly prominent role of these two sectors in the relevance of the Data Act. Around 80% of the companies identified are mainly active in the business-to-business (B2B) environment.

PART III: Selected application challenges of the Data Act

The study carried out in-depth analyses of two application challenges. Firstly, the overlap between the areas of application of the Data Act and the GDPR for personal data was analyzed. Secondly, the handling of trade secrets in the Data Act and the resulting tension between granting access to data and maintaining incentives for innovation were examined in more detail.

In view of the overlapping areas of application of the Data Act and GDPR, it is clear that a dilemma situation can arise for data holders in particular. In order to reconcile the conflicting interests of the two legal acts, a legitimation basis is required for the transfer of personal data. If users and data subjects are identical, the request to disclose data can already be regarded as consent within the meaning of Art. 6 GDPR. However, the situation is different if the user and data subject are different. In this constellation, the Data Act and GDPR must be synchronized via justification criteria. In addition to the fulfillment of a "legitimate interest" (Art. 6 (1 lit. f) GDPR), which places high demands on the necessary balancing process, a data contract between the data holder and user can help. It can incorporate and balance the interests of all parties involved (user, data holder, data subject and data recipient) and define the responsibilities for ensuring compliance with data protection requirements

The legislator has attempted to close possible loopholes for data holders to circumvent data sharing by including trade secrets in the data access claims of data recipients. Technical and organizational measures (TOMs), which the data holder can demand from the user to protect the data, are intended to balance the interests of data holders and data recipients in the case of trade secrets. However, the data holder retains discretionary powers with regard to the declaration of trade secrets and the demand for TOMs to protect them. This discretionary leeway arises in particular from the fact that the data holder has an information advantage over the user / data recipients (and the supervisory authority) due to the confidentiality of the trade secrets. These information asymmetries result in a twofold incentive for the data holder to "overclaim": both with regard to the existence of a trade secret itself and, in a further step, with regard to the demand for TOMs.

This overclaiming is contrary to the intention of the Data Act and is associated with a loss of the welfare potential of the Data Act. Legislators should therefore be sensitized to this

overclaiming problem and, if necessary, take appropriate countermeasures. For small and medium-sized enterprises in particular, for example, it could be expedient to support them in the implementation of TOMs in order to reduce the transaction costs of claiming data access rights and make overclaiming less attractive as a strategy for the data holder.

1 Einleitung

Beim vorliegenden Report handelt es sich um die Studie zur Umsetzung des Data Act in Deutschland. Die Studie wurde im Auftrag der Bundesnetzagentur (Vergabenummer: Z25-3-2024-0020) durchgeführt.

Ziel der wissenschaftlichen Studie ist es, Inhalt und Ausgestaltung der Regeln des Data Act in Bezug auf Datenzugang und -bereitstellung sowie Datennutzung und -weitergabe zu erfassen, anschaulich darzustellen und ausgewählte Problemfelder zu analysieren. Gleichzeitig erfolgt eine empirische Bestandsaufnahme der relevanten Akteure in den wichtigsten datengetriebenen Branchen in Deutschland. Der Fokus der Untersuchungen liegt auf den im Data Act enthaltenen Regelungen zum B2B- und B2C-Data Sharing (im Wesentlichen Kapitel II – IV des Data Act).

Der Abschlussbericht lässt sich in 3 Teile untergliedern:

Im Teil I erfolgt zunächst die grundlegende Darstellung, Aufbereitung und Konkretisierung des Data Sharing gemäß Data Act, insbesondere hinsichtlich der neu geschaffenen Regeln für Datenzugang und -bereitstellung sowie Datennutzung und -weitergabe (Kapitel 2 – 5).

Die empirische Sektoruntersuchung und Anbieteranalyse bildet den Teil II des Berichts. In einem ersten Schritt werden dabei die für den Data Act relevantesten Sektoren in Deutschland ermittelt. Anschließend erfolgt die Anbieteranalyse in diesen Sektoren (Kapitel 6 – 8).

In Teil III des Berichts werden zwei ausgewählte Anwendungsherausforderungen des Data Act in Form von Fallstudien eingehend analysiert. Zum einen handelt es sich um den weiten Datenbegriff des Data Acts und die daraus resultierenden Herausforderungen bei Erfüllung von Datenzugangsansprüchen in Ansehung des Datenschutzrechts aus der DSGVO. Zum anderen werden die im Data Act getroffenen Regelungen zum Schutz von Geschäftsgeheimnissen und das daraus resultierende Spannungsfeld zwischen der Gewährung des Datenzugangs und der Aufrechterhaltung von Innovationsanreizen näher untersucht (Kapitel 9 – 10).

Die Studie schließt mit einem Gesamtfazit in Kapitel 11.

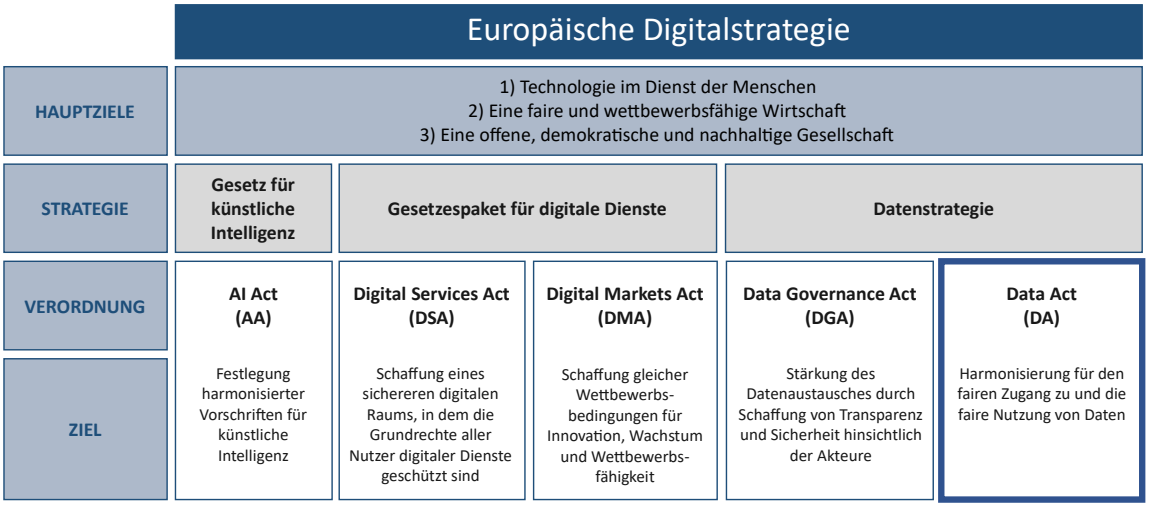
TEIL I: Data Sharing gemäß Data Act: Zielsetzung, Anwendungsbereich & Ablauf

2 Zielsetzung und beabsichtige Wirkungsweise des Data Act für das Data Sharing

Der Rat der Europäischen Union (EU) hat am 27. November 2023 die „**Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung“ (kurz: Data Act (DA))** verabschiedet, die am 11. Januar 2024 in Kraft getreten ist und in seinen wesentlichen Bestandteilen nach einer Übergangsfrist von 20 Monaten ab dem 12. September 2025 direkt anwendbares Recht in der EU werden wird.[1]

Der Data Act reiht sich gemeinsam mit dem AI Act, dem Digital Service Act (DSA), dem Digital Markets Act (DMA) sowie dem Data-Governance Act (DGA) in die **Europäische Digitalstrategie** der Europäischen Kommission ein, die das Ziel verfolgt, einen europäischen Binnenmarkt für Daten zu etablieren, der die globale Wettbewerbsfähigkeit und Datensouveränität Europas sichert. Der DGA und der DA bilden dabei gemeinsam die rechtliche Umsetzung der **europäischen Datenstrategie**.

Abbildung 1: Einordnung des Data Act in die Europäische Digitalstrategie



Quelle: Eigene Darstellung in Anlehnung an Demary (2022).

Erklärtes Ziel des DA ist es, die **Datenökonomie in der EU zu stärken** und das **Entstehen eines wettbewerbsfähigen Datenmarkts** zu fördern.[2]

1 Vgl. BMDV (2023).
2 Siehe EU-Kommission (2024b).

Zentrale Bestandteile des DA sind dabei die Regelungen zum **B2B- sowie B2C-Data Sharing**, welche im Wesentlichen in den Kapiteln II bis IV des DA zu finden sind.[3] Diese bilden den Untersuchungsgegenstand des vorliegenden Projektes.

Im Rahmen des B2B- und B2C-Data Sharings legt der Data Act (DA) Zugangsrechte zu Daten fest, die durch die Nutzung vernetzter Produkte und verbundener Dienste generiert werden. Bisher bzw. vor der Einführung des DA lagen die Verfügungsrechte über solche Nutzungsdaten zwar nicht *de jure*, aber *de facto* meist beim Hersteller des Produkts.[4] Die aktuelle Marktsituation führt dazu, dass Hersteller Daten entweder gar nicht oder nur begrenzt mit den Nutzern und / oder Drittparteien teilen.

Dies hat mehrere Gründe: Unter anderem können sich Hersteller durch den alleinigen Datenzugang Wettbewerbsvorteile verschaffen, indem sie Informationen über das Nutzungsverhalten oder die Funktionalität der Produkte exklusiv zur Optimierung ihrer Angebote verwenden und / oder nachgelagerte Services abschotten können. Außerdem können z. B. rechtliche Unsicherheiten, die starke Fragmentierung in Datensilos sowie fehlende Schnittstellen / Standards dazu beitragen, dass das Teilen der Daten eingeschränkt ist.[5]

Der DA zielt darauf ab, diese exklusive Datenhoheit aufzubrechen und einen fairen Zugang zu Daten zu schaffen, der sowohl den Nutzern als auch Drittparteien eine breitere Verwendung der Daten ermöglicht und so Innovation und Wettbewerb fördert.

Die aus dem eingeschränkten Teilen der Daten resultierende **mangelnde Liquidität des Datenmarkts** ist aus **volkswirtschaftlicher Sicht als ineffizient** zu betrachten. Wesentliches Merkmal von Daten als ökonomisches Gut ist nämlich, dass diese in ihrer Nutzung **non-rival** sind. Die Grenzkosten einer zusätzlichen Nutzung derselben Daten bestehen daher lediglich aus den Transaktionskosten der Bereitstellung der Daten. Anders ausgedrückt bedeutet dies, dass Daten(sätze) mehrfach und gleichzeitig verwendet werden können, ohne dass diese wesentlich an Wert oder Verfügbarkeit verlieren.[6]

Dementsprechend ermöglicht eine **Mehrfachnutzung** von Daten **volkswirtschaftliche Wertschöpfungspotenziale**. Diese zu heben und möglichst umfassend zu realisieren, ist die Intention des DA.

Die **Liquidität** des Datenmarkts soll mit der Einführung von **Zugangsansprüchen** für Nutzer und Drittparteien an den von vernetzten Produkten und / oder verbundenen Diensten generierten Daten erhöht werden, und infolgedessen die **Marktzugangs- und -eintrittshürden** abgebaut werden. Durch die hierdurch beabsichtigte **Öffnung von**

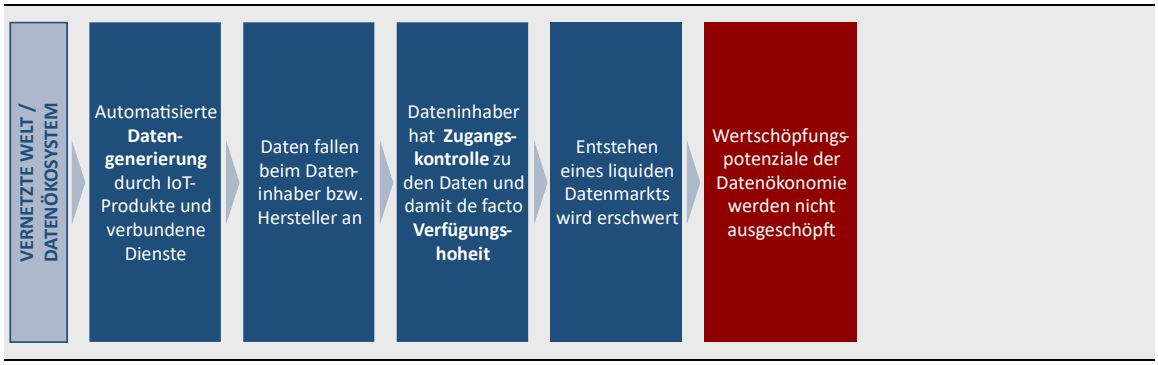
---

3 Weitere wesentliche Regelungsbestandteile des DA sind das B2G-Data Sharing (Kapitel V) sowie die Interoperabilität und Portabilität von Daten zwischen verschiedenen Datenverarbeitungsdiensten („Cloud-Switching"; Kapitel VI – VIII). Diese werden jedoch im vorliegenden Projekt nicht näher betrachtet.
4 Siehe hierzu Eckardt / Kerber (2023).
5 Siehe hierzu auch Erw.-Gr. (2) DA.
6 Vgl. Steffen, et al. (2021).

insbesondere nachgelagerten Märkten soll eine **verstärkte Nutzung** der Daten erzielt werden, wodurch wiederum ein **positiver Wettbewerbseffekt** resultiert. Aus dem intensivierten Wettbewerb ist gemäß marktwirtschaftlicher Wirklogik ein **Innovationsschub** zu erwarten, von dem wiederum **Wachstumseffekte** für die europäische Wirtschaft ausgehen würden. Auf diese Weise sollen die Wertschöpfungspotenziale der (mehrfachen) Datennutzung möglichst weitgehend gehoben und somit die Datenökonomie in der EU gestärkt werden.

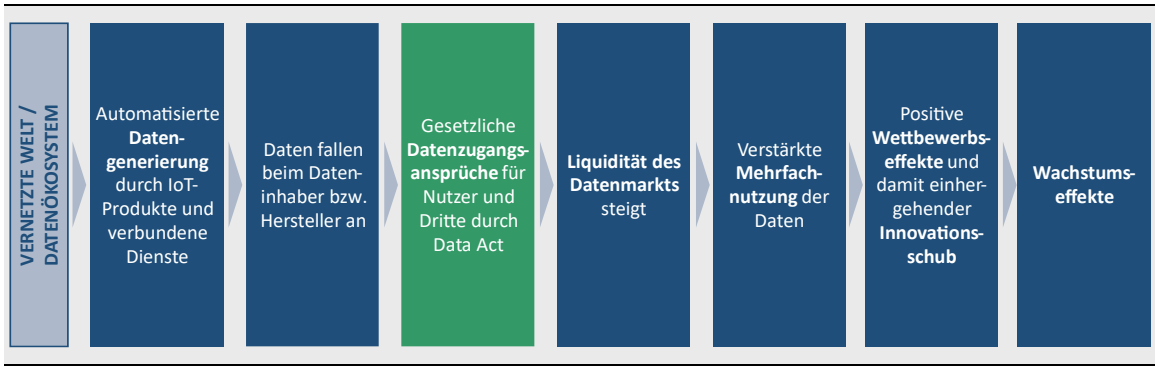
Zusammenfassend sind die vom DA intendierten Effekte des Data Sharing anhand der Gegenüberstellung des Wirkkanals ohne Data Act (Abbildung 2) mit dem beabsichtigten Wirkkanal mit Data Act (Abbildung 3) illustriert.

Abbildung 2: Wirkkanal ohne Data Act



Quelle: Eigene Darstellung.

Abbildung 3: Beabsichtigter Wirkkanal mit Data Act



Quelle: Eigene Darstellung.

3 Anwendungsbereich des Data Act

Den Gegenstand und Anwendungsbereich des Data Act beschreibt Art. 1 DA. Art. 2 DA legt hierfür die wichtigsten Begriffsdefinitionen fest und definiert sie für die Zwecke des DA (vgl. Art. 2 „für die Zwecke“). Sie stehen neben den Begriffsbestimmungen der DSGVO und des DGA, wenngleich die Begriffsbestimmungen z.T. auf diese Rechtsakte verweisen und daher mit ihnen übereinstimmen.

3.1 Sachlicher Anwendungsbereich des Data Act

Der sachliche Anwendungsbereich der im DA geregelten Datenzugangs- und Datenweitergabeansprüche erstreckt sich auf Daten die aus der Nutzung von „vernetzten Produkten“ und mit letzteren „verbundenen Diensten“ generiert werden. Erfasst sind dabei sowohl personenbezogene als auch nicht-personenbezogene Daten. Bezogen auf die personenbezogenen Daten stellt Art. 1 (2) DA klar, dass weiterhin die Vorgaben der DSGVO einzuhalten sind.[7]

3.1.1 Begriff „Daten“

Anknüpfungspunkt für den Anwendungsbereich des Data Act sind Daten. Der Begriff „Daten“ umfasst nach der **Legaldefinition in Art. 2 Nr. 1 DA** „jede digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen auch in Form von Ton-, Bild- oder audiovisuellem Material“. Damit sind zunächst **alle Arten von Daten erfasst**, die von Menschen und / oder Maschinen erzeugt werden können[8] und unabhängig davon, ob sie personenbezogen oder nicht-personenbezogenen sind. Der Begriff „Daten“ ist dabei ganz bewusst weit gefasst, da der Gesetzgeber den Zugang und die Nutzung zu einer Vielzahl von ökonomisch werthaltigen Daten ermöglichen wollte (Erw.-Gr. (3 ff.)).

Der DA knüpft in seinen Vorschriften sodann kontextbezogen an unterschiedliche Datentypen an und definiert diese vorab in den Begriffsbestimmungen (Art. 2 DA). Neben der grundlegenden Unterscheidung zwischen „personenbezogene und nicht-personenbezogene Daten“ in Art. 2 Nr. 3 und Nr. 4 (vgl. dazu 3.1.2) wird weiter zwischen „Metadaten“ in Art. 2 Nr. 2 (vgl. dazu 3.1.3), „Produktdaten“ in Art. 2 Nr. 15 (vgl. dazu 3.1.4), „verbundenen Dienstdaten“ in Art. 2 Nr. 16 (dazu 3.1.5) sowie „ohne weiteres verfügbaren Daten“ in Art. 2 Nr. 17 (vgl. dazu 3.1.6) differenziert, die ihrerseits durch Kategorisierungen wie „exportierbare Daten“ in Art. 2 Nr. 38 (vgl. dazu 3.1.7) eine Ergänzung erfahren.

In den Erwägungsgründen (Erw.-Gr. (15)) werden mit „Rohdaten“ und „aufbereitete Daten“ weitere Datenkategorien benannt und kurz erläutert, die jedoch keine eigene

7 Siehe Staudenmayer NJW 2024, 1377, 1379 sowie Weinhold/Schröder, ZD 2024, 306, 311.
8 Schild, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Data Act, Art. 2 Rn. 6.

Begriffsdefinition in Art. 2 DA erfahren haben. Diese Begriffe werden daher nachfolgend an geeigneter Stelle (dazu 3.1.2, FN 11 und 3.1.3) erläutert.

3.1.2 Personenbezogene und nicht-personenbezogene Daten

Personenbezogene Daten (Art. 2 Nr. 3 DA) sind in Art. 4 (1) DSGVO legal definiert. Dazu gehören alle Informationen, **die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen**. Als identifizierbar wird eine natürliche Person angesehen, sofern sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Der Personenbezug eines Datums ist dabei sehr schnell gegeben. Selbst ein „eigentlich" nicht personenbezogenes Datum (sog. Sachdatum) kann in bestimmten Verwendungszusammenhängen zu einem personenbezogenen werden, sofern eine Verknüpfung zu einem personenbezogenen Datum möglich wird. Dabei ist es nach einem objektiven Verständnis ausreichend, dass eine beliebige Stelle (und nicht nur der Verantwortliche) den Personenbezug herstellen kann.[9]

> Eine Fahrzeugidentifizierungsnummer (FIN) ermöglicht in erster Linie die Identifizierung eines Fahrzeugs und wäre damit ein Sachdatum, welches als solches auch keinen Personenbezug hat. Verfügt eine Stelle allerdings „bei vernünftiger Betrachtung" über Mittel, die es ihr ermöglichen, „Daten, wie die FIN" einer bestimmten Person zuzuordnen, werden diese Daten zu personenbezogenen Daten.[10]

Nicht-personenbezogene Daten sind solche, die **keinen Personenbezug** besitzen (vgl. dazu auch Art. 2 (1) Datenverkehrs-VO). Als Beispiel benennt Erw.-Gr. (9) der Datenverkehrs-VO aggregierte und anonymisierte Datensätze für Big-Data-Analysen sowie Daten die der Überwachung oder Optimierung dienen (z. B. Daten zum Wartungsbedarf von Industriemaschinen). Als nicht-personenbezogen gelten zudem statistische Daten, die auf der Basis einer entsprechenden Datenmenge aggregiert worden sind (z. B. Summen, Mittelwerte, Anzahl und mathematische Kennzahlen), wie auch unstrukturierte Roh-/Quelldaten[11] (z. B. unformatierte, nicht aggregierte

---

9 Schild, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Data Act, Art. 2 Rn. 23.

10 Vgl. hierzu EuGH Urt. v. 9.11.2023 – C-319/22, InTeR 2023 mit Anm. Gesmann-Nuissl; vgl. auch EuGH Urt. v. 19.10.2019 – C-582/14 Rn. 44 ff. „Breyer")

11 Unter **Roh-/Quelldaten** versteht man Daten, die unmittelbar aus den erzeugenden Quellen stammen. Die Daten unterliegen dabei einer vordefinierten Kodierung, die durch das Quellsystem vorgegeben sind. Typischerweise handelt es sich entweder um fortlaufend generierte, einzelne Daten (Datenpunkte), Datenblöcke (etwa von Sensoren) oder um ganze Datensätze mit einer klar vordefinierten Struktur. Vgl. *Sarre/Pruß*, in: Auer-Reinsdorff/Conrad IT- und DatenschutzR-HdB, § 2 Rn. 40. Vgl. auch Erw. G (15) S. 8 DA.

Sensordaten, vgl. Erw.-Gr. (15) S. 8), die als solche keinen Rückschluss auf Personen ermöglichen.

Bei anonymisierten Daten muss deren De-Anonymisierung oder Re-Identifizierbarkeit durch verfügbare Technologien ausgeschlossen sein, weil ansonsten der Personenbezug wieder möglich würde (Erw.-Gr. (9) der Datenverkehrs-VO).

3.1.3 Metadaten

Nach der Legaldefinition des Art. 2 Nr. 2 DA werden **„Metadaten“** als eine „strukturierte Beschreibung der Inhalte oder der Nutzung von Daten bezeichnet, die das Auffinden eben jener Daten bzw. deren Verwendung erleichtert“.

Metadaten sind in der Regel[12] **strukturierte Informationen**, die beschreiben, erklären, lokalisieren oder es einfacher gestalten, wie eine Informationsquelle aufzufinden, abzurufen, zu verwenden oder zu verwalten ist (z. B. Metadaten im Dublin Core Format ermöglichen eine strukturierte Beschreibung von Dokumenten; Geodaten erleichtern das Auffinden von Datenpunkten; Zeitstempel lassen Rückschlüsse auf Abläufe zu; Nutzerdaten lassen sich mittels der Metadaten validieren). Sie können auch „aufbereitet“ sein, um sie nutzbar zu machen, sog. „**aufbereitete Daten**“ (Erw.-Gr. (15) S. 10).

Metadaten bieten mithin Informationen über die Struktur und den Inhalt **anderer** Daten. Sie sind – wie zuvor verdeutlicht – als **Kontextinformationen** für den Nutzer potenziell wertvoll, weil ihm z. B. über die Zeitstempelerfassung die regelmäßige Wartung und Reparatur der betreffenden vernetzten Produkte erleichtert wird (Erw.-Gr. (15)). Ob sie auch erforderlich sind (Art. 4 (1) DA) ist kontextabhängig; der DA gibt hier keine weiteren Hinweise.

Während Metadaten jedenfalls vom DA erfasst sind, werden die aus den Metadaten **abgeleiteten oder gefolgerten Informationen,** die erst das Ergebnis zusätzlicher Investitionen in die Zuweisung von Werten oder Erkenntnissen aus den Daten sind (insbesondere mittels komplexer proprietärer Algorithmen, einschließlich solcher, die Teil proprietärer Software sind), **nicht vom Anwendungsbereich des DA erfasst**. Die Dateninhaber sollen bezüglich derartiger Informationen, die über das reine Metadatum hinausgehen, nicht dazu verpflichtet sein, sie einem Nutzer oder Datenempfänger bereitzustellen, es sei denn, der Nutzer und der Dateninhaber haben ausdrücklich etwas anderes vereinbart (Erw.-Gr. (15)).

---

12 Weitere Anknüpfungen finden sich in der Inspire-RL (RL 2007/2/EG) v. 14.3.2007 (ABl. L 108, 1) zuletzt geändert durch Art 4 VO (EU) 2019/1010 v. 5.6.2019 (ABl. L 170, 115), wonach Metadaten als Informationen gelten, die Geodatensätze und Geodatendienste beschreiben und es ermöglichen, diese zu ermitteln, in Verzeichnisse aufzunehmen und zu nutzen (Art. 3 Nr. 6 Inspire-RL). Ebenso findet sich der Begriff im Erw.-Gr.16 sowie Art. 12 lit. c) DGA, wo als Metadaten benannt werden, z. B. Datum, Uhrzeit und Geolokalisierungsdaten, Dauer der Nutzung oder Verbindungen des Nutzers zu anderen Personen.

Hierzu können nach Erw.-Gr. (15) DA bspw. „Informationen gehören, die durch Sensorfusion gewonnen werden, bei dem Daten von mehreren Sensoren abgeleitet oder gefolgert werden, die in dem vernetzten Produkt unter Verwendung komplexer proprietärer Algorithmen erhoben werden und möglicherweise Rechten des geistigen Eigentums unterliegen."

3.1.4 Vernetzte Produkte und Produktdaten

Der **Begriff der „vernetzten Produkte"** wird in **Art. 2 Nr. 5 DA** legal definiert. Darunter versteht das Gesetz „einen Gegenstand, der Daten über seine Nutzung oder Umgebung erlangt, generiert oder erhebt und der Produktdaten über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang übermitteln kann und dessen Hauptfunktion nicht die Speicherung, Verarbeitung oder Übertragung von Daten im Namen einer anderen Partei – außer dem Nutzer – ist".

Umfasst werden körperliche Gegenstände (i.S. des § 90 BGB), die auch in einem unbeweglichen Gegenstand enthalten sein können (z. B. Smart Home Devices). Gemeinhin gehören dazu insbesondere Produkte, die dem Bereich des „Internet of Things (IoT) zugerechnet werden (mit Ausnahme von Prototypen).

Kennzeichnend ist, dass vernetzte Produkte Daten über ihre Leistung, Nutzung oder Umgebung verarbeiten und diese Produktdaten (Art. 2 Nr. 15 DA; siehe näher unten) nach außen kabelgebunden oder drahtlos übermitteln können (z. B. über einen geräteinternen Zugang oder eine WLAN-Verbindung). Letzteres schließt auch die Übermittlung von Daten außerhalb des Produkts auf „Ad-Hoc-Basis" (z. B. während Wartungsarbeiten) mit ein.[13] Insofern ist die Möglichkeit zur Übermittlung der durch die Geräte generierten Daten nach Außen für die Qualifikation eines „vernetzten Produktes" entscheidend (Erw.-Gr. (15)).

Welche Daten von einem vernetzten Produkt bereitgestellt werden, obliegt der Entscheidung des Entwicklers bzw. Herstellers bei der Konzeption des Produkts, wobei er die gesetzlichen Vorgaben (z. B. aus Harmonisierungsverordnungen und -richtlinien, mandatierten technischen Normen) zu berücksichtigen hat (Erw.-Gr. (14)). Bezüglich der erzeugten und verfügbaren Daten muss jedenfalls gewährleistet sein, dass der Nutzer darauf leicht und sicher zugreifen kann (Erw.-Gr. (20)), um sie unter bestimmten Bedingungen weiterzugeben.

13 Siehe EU-Kommission (2024c): FAQs zum DA, Frage 4.

Beispiele für vernetzten IoT-Produkte i.S. von Art. 2 Nr. 5 DA sind u. a.:[14] Smart Cars (autonome oder teilautomatisierte Fahrzeuge), Wearables (Fitness-Tracker, Smartwatches, intelligente Brillen, VR-Headsets etc.), Smartphones, Tablets Computer, Smart Home Geräte (z. B. smarte Küchen- oder TV-Geräte, intelligente Beleuchtung, intelligente Stromzähler, intelligente Feuermelder, intelligente Türschlösser etc.), Ausrüstungsgegenstände (z. B. intelligente Prothesen, Exoskelette), Lifestyle-Artikel (intelligente Fahrräder), vernetztes medizinisches Gerät, intelligente Sicherheitssysteme, vernetzte landwirtschaftliche oder industrielle Maschinen (z. B. automatisierte Fertigungsstraßen, vernetzte Stickmaschinen, Energieverwaltungssysteme, landwirtschaftliche Robotiksysteme, wie Feldspritzen).

Produktdaten sind nach der **Legaldefinition des Art. 2 Nr. 15 DA** „Daten, die durch die Nutzung eines vernetzten Produkts generiert werden und die der Hersteller so konzipiert hat, dass sie über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang von einem Nutzer, Dateninhaber oder Dritten – ggf. einschließlich des Herstellers – abgerufen werden können“.

Bei den Produktdaten ist also wesentlich, dass sie **durch die Nutzung eines vernetzten Produkts generiert** werden. Dies schließt aktiv erfasste Daten (z. B. durch Sensoren sowie Daten zu Hardwarestatus, Fehlfunktionen oder Störungen) wie auch passiv generierte Daten (z. B. Nutzungsdauer) ein. Entscheidend ist, dass es sich um Daten handelt, die technisch abrufbar aus dem vernetzten / verbundenen Produkt selbst heraus entstehen, wie z. B. Daten zu Verbräuchen oder zu Fehlfunktionen und Störungen. Die Daten müssen nicht notwendigerweise in einem speziell aufbereiteten Format vorliegen: Sowohl **Rohdaten** („Quell- oder Primärdaten, die sich auf Datenpunkte beziehen und ohne jegliche Form der Verarbeitung automatisch generiert werden“; Erw.-Gr. (15, S. 8)) als auch **aufbereitete Daten**, die ihrerseits nur verständlicher und nutzbarer gemacht wurden (Erw.-Gr. (15 S. 9); z. B. durch Umrechnung physikalischer Größen in anschauliche Einheiten), fallen unter diesen Begriff. Ebenso die für den Nutzer **ohne weiteres verfügbaren Daten** (siehe dazu 3.1.6), die technisch direkt dem Produkt entspringen, wie z. B. physikalische Größen eines Produktes, wie Temperatur, Öldruck, Position.

Bei Produktdaten kann es sich um nicht-personenbezogene Daten, also reine Sachdaten handeln, wie auch – wegen eines bestimmten Anwendungsbezuges – um personenbezogene Daten.

14 Vgl. auch Ehlen/Sebulke CR 2024, 84.

Erw.-Gr. (14) nennt als Beispiel für Produktdaten des vernetzten Produktes „Fahrzeug“, die Daten zur Leistung des Fahrzeugs (z. B. PS, Reichweiten), zur Nutzung (z. B. Tageszeiten, Wettereinflüsse auf Nutzung) oder seiner Umgebung (z. B. Orte). Dabei wird deutlich, dass sowohl nicht-personenbezogene (z. B. PS, Reichweite), als auch personenbezogene Daten (z. B. Tageszeiten, Orte) angesprochen sind.

Informationen, **die aus Produktdaten gefolgert oder abgeleitet sind**, fallen dagegen **nicht in den Anwendungsbereich des DA** (Erw.-Gr. (15 S. 11)); sie müssen folglich auch **nicht an die Nutzer herausgegeben** werden. Dabei handelt es sich z. B. um Informationen, die erst bei der Verarbeitung vorgenannter Daten mittels proprietärer Algorithmen und zusätzlicher Investitionen entstehen (z. B. die Interpretation der zuvor genannten Geschwindigkeitsdaten).[15] Diese Begrenzung wird unter anderem damit begründet, dass sie einerseits einen neuen wirtschaftlichen Akt erfordern und zum anderen solche abgeleiteten Informationen oftmals dem Schutz des geistigen Eigentums (z. B. Geschäftsgeheimnisschutz, Urheber- oder Patentrecht) unterliegen können, wie z. B. ein Quellcode einer Software. Allerdings wird es im Einzelfall **schwierig sein, die exakte Grenze zwischen umfassten und nicht (mehr) umfassten Daten zu ziehen**.

Rein beschreibende Daten, die dem vernetzten Produkt nurmehr beiliegen (z. B. in Benutzerhandbüchern oder auf der Verpackung) sind ebenfalls **keine Produktdaten**.[16]

Im Zusammenhang mit den vernetzten Produkten und Produktdaten ist schließlich das Konkurrenzverhältnis zur ePrivacy-RL zu berücksichtigen, die bestimmte Datenkategorien der Privatsphäre unterwirft und von der Kommunikation nach außen ausnimmt. Insofern können solche Daten ebenfalls keine Produktdaten i.S. des DA darstellen.

Bei der Speicherung und Verarbeitung von Daten durch den Nutzer über Smartphones, Computer oder Tablets, sind diese Geräte zwar vernetzte Produkte und generieren z. B. Verbindungsdaten. Letztere würden aber der ePrivacy-RL unterliegen und wären damit keine Produktdaten. Gleiches gilt, wenn Computer oder Tablets im Rahmen eines Kommunikationsdienstes nach der ePrivacy-RL genutzt werden. Bei der selbst veranlassten Speicherung von Daten durch den Nutzer liegen daher keine Produktdaten vor. Bei einer automatisierten Datenabschöpfung über ein Betriebssystem wären jedoch Produktdaten gegeben. Beispiel entnommen aus *Schild*, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK, Datenschutzrecht, DA, Art. 2 Rn. 89b.

15 Vgl. EU-Kommission (2024c), FAQ zum DA, Frage 5.
16 Vgl. EU-Kommission (2024c); FAQs zum DA, Frage 4.

3.1.5 Verbundener Dienst und verbundene Dienstdaten

Der **Begriff des verbundenen Dienstes** wird in **Art. 2 Nr. 6 DA legaldefiniert** als "digitaler Dienst, bei dem es sich nicht um einen elektronischen Kommunikationsdienst handelt, – einschließlich Software –, der zum Zeitpunkt des Kaufs, der Miete oder des Leasing so mit dem Produkt verbunden ist, dass das vernetzte Produkt ohne ihn eine oder mehrere seiner Funktionen nicht ausführen könnte oder der anschließend vom Hersteller oder einem Dritten mit dem Produkt verbunden wird, um die Funktionen des vernetzten Produkts zu ergänzen, zu aktualisieren oder anzupassen."

Verbundene Dienste **ergänzen vernetzte Produkte funktional**. Es handelt sich dabei um digitale Dienste, die eine oder mehrere Funktionen des vernetzten Produkts ermöglichen, indem sie etwa durch Befehle an das vernetzte Produkt auf dessen Aktivität oder dessen Verhalten einwirken (Erw.-Gr. (17)). Verbundene Dienste sind somit solche, die ausdrücklich mit dem Betrieb der Funktionen des vernetzten Produkts verknüpft sind und dieses ggf. auch steuern können (z. B. Analyse- oder Wartungsdienste). Die verbundenen Dienste können daher selbst Daten generieren, die für den Nutzer des vernetzten Produkts von Wert sind. Durch den verbundenen Dienst werden jedenfalls Daten zwischen dem vernetzten Produkt und dem Diensteanbieter ausgetauscht.

Verbundene Dienste müssen nicht vom Hersteller des vernetzten Produkts stammen, sondern sie können als Teil eines Kauf-, Miet- oder Leasingvertrags von Dritten angeboten werden.

> Ein verbundener Dienst kann z. B. eine mobile App sein, die für die umfassende Nutzung eines Wearable (z. B. Fitness-Tracker) benötigt wird. Dabei kann die App vom Hersteller des Fitness-Trackers stammen, aber auch von einem Drittanbieter.[17] Bezogen auf ein Navigationsgerät (als vernetztes Produkt) in einem Kfz kann das z. B. ein Dienst sein, der zur aktuellen Verkehrslage mit einer darauf angepassten Navigation reagiert.

Bei den vernetzten Produkten und verbundenen Diensten werden oftmals auch **virtuelle Assistenten (z. B. Bots)** einbezogen. Diese werden in Art. 2 Nr. 31 DA legaldefiniert als „Software, die Aufträge, Aufgaben oder Fragen verarbeiten kann, auch aufgrund von Eingaben in Ton- und Schriftform, mit Gesten oder Bewegungen, und die auf der Grundlage dieser Aufträge, Aufgaben oder Fragen den Zugang zu anderen Diensten gewährt oder die Funktionen von vernetzten Produkten steuert."

Virtuelle Assistenten können z. B. in einer Smart-Home-Umgebung (vgl. Erw.-Gr. (23)) als Interface dienen oder sie können herkömmliche Touchscreens oder Smartphone-Apps durch humanoide Interfaces, z. B. ein sprach- oder gestengesteuertes Interface, ersetzen und dabei erhebliche Mengen relevanter Daten darüber erfassen, wie der Nutzer mit Produkten interagieren soll.[18] Ein „virtueller Assistent" kann nach Art. 1 (4) DA

17 Siehe Weinhold/Schröder (2024), S. 306, 308.
18 Siehe Weinhold/Schröder (2024), S. 306, 308.

als „verbundener Dienst“ eingestuft werden, sofern er einbezogen ist, d. h. für die Funktion des vernetzten Produkts unerlässlich bzw. in dieses integriert ist.[19]

Hinsichtlich des Einbezugs der von dem virtuellen Dienst vermittelten Daten in den Anwendungsbereich des DA, gilt also Art. 1 (4) DA. Einbezogen sind danach Daten, die durch die Interaktion des Nutzers mit dem vernetzten Produkt – vermittelt durch den virtuellen Assistenten – entstehen (Erw.-Gr. (23 S. 2 und S. 6)). Nicht einbezogen sind hingegen die Daten, die der virtuelle Assistent unabhängig von der Nutzung des vernetzten Produktes oder des verbundenen Dienstes erstellt (Erw.-Gr. (23 S. 7)). Auch wenn dieser Hinweis deutlich zu sein scheint, bleibt die genaue Festlegung, wann ein virtueller Assistent tatsächlich unabhängig vom Produkt oder Dienst „eigene“ Daten erstellt, unklar.[20]

Wird in einer Smart-Home-Umgebung eine sprachgesteuerte Befehlserkennungssoftware implementiert, die zum einen virtueller Assistent ist, aber auch zwingend notwendig, um vernetzte Produkte zu steuern und dessen vollen Funktionsumfang zu ermöglichen, liegt zugleich ein „verbundener Dienst“ vor.[21] Die vom virtuellen Dienst generierten Daten, werden nach Art. 1 (4) DA Gegenstand des Zugangsrechts (Erw.-Gr. (23 S. 4)).

„**Verbundene Dienstdaten**“ sind nach Art. 2 Nr. 16 DA „Daten, die die Digitalisierung von Nutzerhandlungen oder Vorgängen im Zusammenhang mit dem vernetzten Produkt darstellen und vom Nutzer absichtlich aufgezeichnet oder als Nebenprodukt der Handlung des Nutzers während der Bereitstellung eines verbundenen Dienstes durch den Anbieter generiert werden.“ Sie bilden **Nutzerhandlungen oder -vorgänge** im Zusammenhang mit dem vernetzten Produkten ab und werden während der Erbringung eines verbundenen Dienstes durch den Anbieter generiert (Erw.-Gr. (15 S. 4)).

Im Wesentlichen handelt es sich um Daten, die die Interaktion des Nutzers mit dem verbundenen Dienst widerspiegeln. Dies umfasst sowohl bewusst erfasste Daten als auch Daten, die implizit während der Nutzung entstehen. Erw.-Gr. (15) benennt dazu zahlreiche Beispiele: Statusinformationen („genutzt“ / “nicht genutzt“), Modi Wechsel (etwa „Stand-by“ zu „Off“), Aufzeichnungen eingebetteter Anwendungen, Hardware-Status, Funktionsstörungen und Sensordaten. Das können Daten über die Umgebung oder Interaktionen des vernetzten Produkts sein, wie z. B. Daten der Verbindungszeiten zu Internetanschlüssen oder anderen Produkten.[22] Auch aufbereitete Daten sind eingeschlossen, sofern die Aufbereitung lediglich der besseren Verwertbarkeit dient und keinen eigenständigen Mehrwert darstellt (Erw.-Gr. (15 S. 8)).

Während Produktdaten (vgl. 3.1.4.) automatisch bei der Nutzung der vernetzten Produkte entstehen, weil die Produkte von den Entwicklern / Herstellern so konzipiert wurden,

19 Siehe Bomhard (2024),S. 71, 73.
20 Bomhard (2024), S. 71, 73.
21 Siehe Bomhard (2024), S. 71, 73.
22 Vgl. Lommatzsch/Albrecht (2024), S. 302.

werden verbundene Dienstdaten alleine **durch den Nutzer veranlasst**, d. h. sofern sich der Nutzer bewusst dafür entscheidet Daten zu generieren. Dies zum einen durch seine Handlungen bezogen auf das vernetzte Produkt, zum anderen durch den Wunsch des Nutzers diese aufzuzeichnen. Dabei können die Daten auch nur als Nebenprodukt anfallen, wenn sie nur erzeugt werden, um andere Daten zu gewinnen.[23]

> Betreibt der Nutzer z. B. ein Energiemanagementsystem (EMS) werden je nach angeschlossenen Devices die Daten der eingebundenen Systeme (Heizung, Staubsauger, Ladestation etc.) erhoben und fließen als verbundene Dienstdaten in das EMS zurück. Dabei werden ggf. auch Zustandsdaten zu Ladekapazität oder Bereitschaft erfasst, obschon der Nutzer inaktiv ist, die ebenfalls als verbundene Dienstdaten gelten. Bezogen auf das o. g. Beispiel zum Navigationsgerät, wären etwa Daten darüber, wie der Fahrer auf eine Staumeldung reagiert, solche verbundenen Dienstdaten.

3.1.6 Ohne weiteres verfügbare Daten

Der in Art. 4 DA verwendete Begriff der „**ohne Weiteres verfügbare Daten**“ wird in Art. 2 Nr. 17 Data Act definiert als „Produktdaten und verbundene Dienstdaten, die ein Dateninhaber rechtmäßig und ohne unverhältnismäßigem Aufwand aus dem vernetzten Produkt oder der verbundenen Dienstleistung gewinnen kann”.
Bei diesen Daten handelt es sich sowohl um Produktdaten, wie auch um verbundene Dienstdaten. Ihnen ist gemein, dass ein **Dateninhaber sie rechtmäßig von dem vernetzten Produkt oder verbundenen Dienst erhält oder erhalten kann**, etwa aufgrund der Konzeption des vernetzten Produkts oder aufgrund eines Vertrags des Dateninhabers mit dem Nutzer über die Erbringung verbundener Dienste und diese Daten zudem aufgrund der technischen Mittel für den Datenzugang **ohne unverhältnismäßig hohem Aufwand erlangt werden können**, sie also jederzeit oder ohne weiteres verfügbar sind (vgl. Erw.-Gr. (20)). Eine konkrete Grenze, ab wann Daten „ohne unverhältnismäßigen Aufwand verfügbar“ oder als nicht mehr „ohne Weiteres verfügbar“ gelten, nennt der DA hingegen nicht. Die Abgrenzungskriterien, die in Erw.-Gr. (20) benannt sind, bleiben ebenfalls unscharf. Entsprechend der dort benannten Hinweise kann z. B. nicht mehr von leicht verfügbaren Daten ausgegangen werden, wenn das vernetzte Produkt nicht dafür entwickelt wurde, die Daten unmittelbar am Gerät abzurufen (etwa bei Produkten ohne datenfähige Nutzerschnittstelle).[24] Das ist eindeutig. Bei Daten hingegen, die beispielsweise die Kommunikationsfunktionalitäten eines vernetzten Fahrzeugs in gängigen Formaten beschreiben, ist dies nicht mehr eindeutig. So wird man zwar zunächst davon ausgehen dürfen, dass diese ohne unverhältnismäßigen Aufwand zugänglich sind, wobei sich dies dann vollkommen anders darstellen kann, wenn der praktische Zugriff trotz theoretischer Möglichkeit durch Faktoren wie extreme Speicherintensität erschwert wird. Hier helfen die Hinweise in Erw.-Gr. (20) dann

23 Siehe Schild, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK, Datenschutzrecht, DA, Art. 2 Rn. 92).
24 Vgl. Apel/Huber, JUS 2024, 410, 412.

nicht mehr weiter, sondern die Fragen nach dem „unverhältnismäßigen Aufwand“ erfordert eine Einzelfallprüfung, die sowohl technische als auch wirtschaftliche Aspekte berücksichtigen muss.[25]

Als „ohne weiteres verfügbare Daten“ gelten im Allgemeinen: Produktdaten, verbundene Dienstdaten, Rohdaten, aufbereitete Daten, Metadaten und zwar in der Form, wie sie vorliegen. Nicht hingegen: Aufbereitete Informationen, die erst aus diesen Daten gefolgert oder abgeleitet werden, und das Ergebnis zusätzlicher (wesentlicher) Informationen sind, etwa weil sie mit der Hilfe komplexer proprietärer Algorithmen analysiert wurden.

3.1.7 Exportierbare Daten

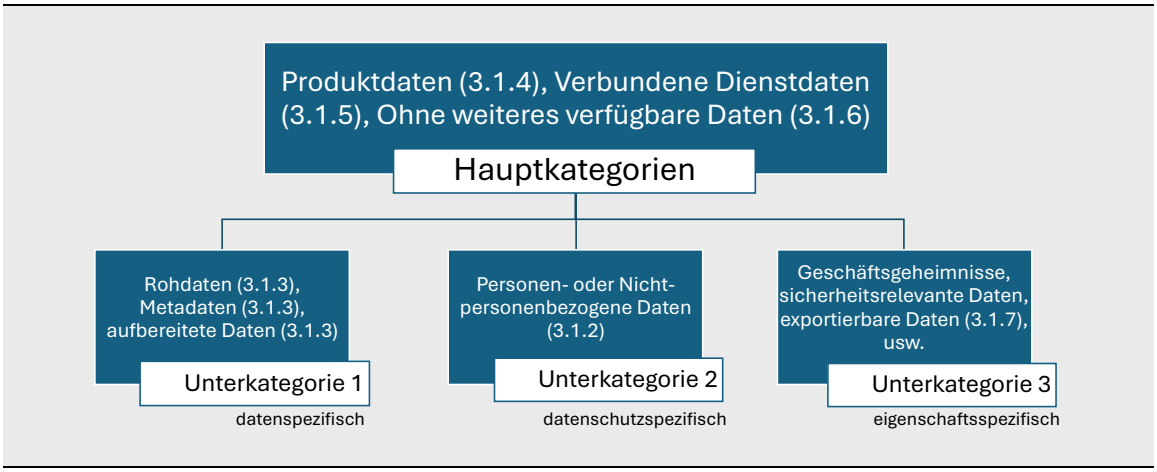
„**Exportierbare Daten“** sind gemäß Art. 2 Nr. 38 DA (i.V.m. Erw.-Gr. (82)) die **Eingabe- und Ausgabedaten** einschließlich **Metadaten** (vgl. dazu oben 3.1.3), die unmittelbar oder mittelbar durch die Nutzung des Datenverarbeitungsdienstes durch den Kunden oder gemeinsam generiert werden, mit Ausnahme der Vermögenswerte oder Daten eines Anbieters von Datenverarbeitungsdiensten oder Dritter, die durch Rechte des geistigen Eigentums geschützt sind oder ein Geschäftsgeheimnis darstellen.

Die exportierbaren Daten erhalten ihre Bedeutung, wenn die Nutzer zu anderen Datenverarbeitungsdiensten wechseln (Art. 23 – 31 und Art. 35 DA).

3.1.8 Zusammenfassung „Daten“ und Beispiele

Die in Art. 2 DA benannten Datentypen lassen sich durchaus in eine qualitative Struktur überführen, siehe nachfolgende Abbildung 4 (die Klammerzusätze beziehen sich auf vorstehende Abschnitte oder Fußnoten):

Abbildung 4: Qualitative Struktur der Datenkategorien des DA



Quelle: Eigene Darstellung.

25 Vgl. Frank / Freifrau von Imhoff (2025)

Dabei kann festgehalten werden, dass ein bestimmtes Datum, sofern es einem der drei genannten Hauptkategorien zugeordnet werden kann, immer eine der daten- oder datenschutzspezifischen Eigenschaften der Unterkategorien 1 und 2 aufweisen wird. Die Eigenschaften aus der Unterkategorie 3 sind hingegen nur gegebenenfalls erfüllt.

Nachfolgend soll noch anhand von zwei Beispielen[26] aufgezeigt werden, wie die diversen Datenkategorien in konkreten Anwendungsszenarien zusammentreffen können.

Beispiel 1: Fahrzeug im Straßenverkehr

Fahrzeuge sind mit Sensoren und Systemen ausgestattet, die Daten sammeln und für verschiedene Funktionen nutzen.

Ein Navigationssystem schlägt auf Basis von GPS-Daten und vergangenen Fahrten eine Route vor und schätzt die Fahrzeit ab, indem auch Echtzeitinformationen über Verkehrslage und Staus berücksichtigt werden.

- Rohdaten bzw. ohne weiteres verfügbare Daten zu Position und Route = Zugangsanspruch.
- Metadaten bezüglich der Zeitstempel der GPS-Daten = Zugangsanspruch.
- Abgeleitete Informationen bezüglich der Abschätzung der Fahrzeit und der Routenoptimierung = kein Zugangsanspruch.

Gleichzeitig sammelt das Fahrzeug Daten über den Zustand wichtiger Komponenten wie Motor, Getriebe und Bremsen. Dabei melden die Sensoren wegen Unterschreitung des Mindestölstandes einen kritischen Zustand und eine Meldung fordert den Fahrer dazu auf, die Werkstatt aufzusuchen.

- Produktdaten bzw. ohne weiteres verfügbare Daten bezüglich der Ölstands-anzeige / -warnung = Zugangsanspruch.
- Abgeleitete Information bezüglich der Aufforderung, eine Werkstatt aufzusuchen = kein Zugangsanspruch.

Beispiel 2: Robotik-System bei einem Automobilhersteller

Im Unternehmen A befindet sich eine Fertigungsstraße mit Robotersystemen des Herstellers A, die durch eine cloudbasierte Software des Herstellers B gesteuert werden. Die Roboter erfassen während des Betriebs genaue Positionsdaten (X-, Y-, Z-Koordinaten, Winkel) in Echtzeit. Der Bediener kann über die Software Bewegungsparameter (Geschwindigkeit, Kraft) einstellen. Das System protokolliert diese Eingaben und die daraus resultierenden Bewegungen. Zusätzlich werden Umgebungsdaten wie Temperatur und Luftfeuchtigkeit mittels Sensoren erfasst, soweit sie für die Funktionalität und Genauigkeit des Systems relevant sind. Der Zustand des Robotersystems (aktiv/inaktiv, Fehlermeldungen) wird ebenfalls aufgezeichnet. Das System analysiert die gesammelten

26 Angelehnt an Frank / Freifrau von Imhoff (2025).

Daten langfristig und erstellt anschließend Berichte über Ausfallwahrscheinlichkeit, Verschleiß und Effizienz.

- Produktdaten und / oder verbundene Dienstdaten bezüglich der Positionsdaten der Roboterarme = Zugangsanspruch.
- Metadaten, bezüglich der genauen Skalierung der Roboterarme (Zoll, Zentimeter) = Zugangsanspruch.
- Verbundene Dienstdaten bezüglich der Bewegungsprotokolle, die aus den Befehlen des Bedieners folgen = Zugangsanspruch.
- Produktdaten bezüglich der Systemzustandsdaten (aktiv / inaktiv, Fehlermeldung) = Zugangsanspruch.
- Produktdaten bzw. ohne weiteres verfügbaren Daten bezüglich der Umgebungsdaten (Temperatur und Luftfeuchtigkeit) = Zugangsanspruch.
- Abgeleitete Informationen bezüglich der Langzeitanalysen und Verschleiß = kein Zugangsanspruch.

3.2 Persönlicher Anwendungsbereich des Data Act („Akteure“)

Der persönliche Anwendungsbereich ergibt sich aus Art. 1 (3) DA, der die wichtigsten Anwender benennt. Das sind der Nutzer eines vernetzen Produkts (vgl. 3.2.1), der Dateninhaber (vgl. 3.2.2) sowie der Datenempfänger (vgl. 3.2.3).

3.2.1 Nutzer

Zentrale Person des DA ist der **Nutzer**. Bei diesem handelt es sich nach Art. 2 Nr. 12 DA um „eine natürliche oder juristische Person, die ein vernetzten Produkt besitzt oder dem vertraglich zeitweilig Rechte für die Nutzung des vernetzten Produktes übertragen wurden und die verbundenen Dienste in Anspruch nimmt“. Erw.-Gr. (18) stellt dabei klar, dass im Einzelfall nicht dauerhaft dieselbe Person Nutzer sein muss (z. B. bei Nutzung eines Car-Sharing-Dienstes). Maßgeblich ist also nicht die sachenrechtliche Stellung als Eigentümer, sondern vielmehr die **tatsächliche (berechtigte) Verwendung des vernetzten Produkts**.[27] Er genießt vor allem die **Vorteile der Nutzung** des vernetzten Produkts; er ist in der Lage aus den von diesem vernetzten Produkt und allen verbundenen Diensten generierten Daten einen Nutzen zu ziehen. Dabei ist es unerheblich, ob die Daten bei der Nutzung absichtlich generiert werden (z. B. Ingangsetzung eines Fahrzeugs) oder indirekt durch das Nutzungsverhalten entstehen (z. B. automatisch von Sensoren generierte Daten oder Daten, die von eingebetteten Anwendungen aufgezeichnet werden); selbst Inaktivität genügt (siehe oben).

27 Vgl. Etzkorn, RDi 2024, 116, 118.

Nutzer können typischerweise z. B. Eigentümer, Miteigentümer und Mieter eines vernetzten Produkts sein. **Keine Nutzer** sollen hingegen Personen sein, die ein vernetztes Produkt nur vorrübergehend und ohne ein „stabiles Recht zur Nutzung“[28] lediglich tatsächlich nutzen (z. B. Familienmitglieder; Nachbarn im Rahmen von Gefälligkeitsverhältnissen).[29] Der Ausschluss von Personen, die ihr Recht zur (Mit-)Nutzung des vernetzen Produkts nicht auf eine Berechtigung (z. B. vertragliche Einräumung; Einrichtung eines eigenen Kundenkonto etc.) stützen können, erscheint auch bei näherer Betrachtung mit Blick auf die Zielrichtung des DA konsequent, da diese Personengruppen von der Nutzung des vernetzten Produkts profitieren würden, jedoch mangels Bindung keine eigenen Verpflichtungen in Bezug auf das Produkt eingehen müssten. Sie wären daher juristisch und wirtschaftlich weitaus weniger Risiken ausgesetzt als vertraglich gebundene Nutzer (vgl. auch Erw.-Gr. (18)). Insofern ist die Differenzierung berechtigt. Allerdings kann auch eine zunächst unberechtigte Person zum Nutzer im Sinne des DA werden, sofern sie sich eine Berechtigung zur Nutzung vom Dateninhaber einräumen lässt, z. B. durch Eröffnung eines eigenen Nutzerkontos beim Dateninhaber. Als Beispiel kann z. B. die Nachbarin gelten, die sich den vernetzen Rasenmäher „ausleiht“ oder Kinder, die innerhalb des gemeinsamen Haushalts, das Fahrzeug der Eltern fahren oder die Ehegatten, die ein betriebliches Wearable; Fahrzeug) nutzen, ohne beim Dateninhaber als Nutzer angemeldet zu sein.

3.2.2 Dateninhaber

Beim **Dateninhaber** handelt es sich nach Art. 2 Nr. 13 DA um „eine natürliche oder juristische Person, die […] berechtigt oder verpflichtet ist, Daten – soweit vertraglich vereinbart, auch Produktdaten oder verbundene Dienstdaten – zu nutzen und bereitzustellen, die sie während der Erbringung eines verbundenen Dienstes abgerufen oder generiert hat“. Die Definition kann nur so verstanden werden, dass der Dateninhaber derjenige ist, der die **tatsächliche Kontrolle über die Daten hat** und in der Lage ist, die Ansprüche nach dem Data Act zu erfüllen. Er ist derjenige, der die während der Erbringungen des Dienstes oder Nutzung des vernetzten Produktes abgerufenen bzw. generierten Daten sammelt.

Auch wenn in den meisten Fallkonstellationen der Hersteller eines vernetzten Produktes oder der Anbieter eines Dienstes Dateninhaber sein wird, ist das nicht zwingend. Der DA erlaubt es einem Unternehmen, die **Rolle des „Dateninhabers“** an ein anderes Unternehmen **auszulagern**, z. B. an Zulieferer oder Unternehmen, die weitere Services zu dem vernetzten Produkt anbieten. Insofern hängt die Festlegung als Dateninhaber

28 Siehe EU-Kommission (2024c); FAQs zum DA, Frage 11:„This implies the user has a stable right on the connected product (e.g. ownership, or a right from a rent or lease contract).“
29 Vgl. Dannhausen/Abel (2024), S. 931, 932.

nicht davon ab, wer die Hard- oder Software hergestellt hat, sondern davon, **wer** den Zugriff auf die **verfügbaren Daten kontrolliert**.[30]

Auftragsdatenverarbeiter i.S.v. § 4 Nr. 8 DSGVO **gelten nicht als Dateninhaber** im Sinne des DA (Erw.-Gr. (22)). Ebenso wenig sind öffentliche Stellen im Allgemeinen von der Begriffsdefinition erfasst, hingegen durchaus öffentliche Unternehmen (Erw.-Gr. (63); z. B. eine ‚kommunale GmbH).

3.2.3 Datenempfänger

Wer nicht selbst Nutzer oder Dateninhaber ist, kommt als **Datenempfänger** in Betracht. In Art. 2 Nr. 16 DA ist dieser als „eine natürliche oder juristische Person, die zu Zwecken innerhalb ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit handelt, ohne Nutzer eines vernetzten Produktes oder verbundenen Dienstes zu sein, und dem vom Dateninhaber Daten bereitgestellt werden, einschließlich eines Dritten, dem der Dateninhaber auf Verlangen des Nutzers […] Daten bereitstellt“ definiert.

Hiernach ist Datenempfänger jede natürliche oder juristische Person, welche von dem Dateninhaber Daten erhält, ohne Nutzer zu sein. Ebenso ein Dritter auf Verlangen des Nutzers (Art. 5 (1) DA). Diese Form der Weitergabe an einen Datenempfänger bedarf jedenfalls einer Rechtsgrundlage, sofern es sich um personenbezogene Daten handelt.

Der Datenempfänger muss jedenfalls in der Union ansässig sein, damit ihm Daten nach dem DA bereitgestellt werden können (vgl. Art. 1 (3 lit.) d DA).[31]

Als Datenempfänger ausgeschlossen sind die sog. Gatekeeper (Art. 5 (3) DA). Dabei handelt es sich um Unternehmen, die bestimmte Schlüsselpositionen in digitalen Märkten kontrollieren und deshalb von der EU-Kommission gem. Art. 3 des Gesetzes über digitale Märkte (Digital Markets Act - DMA) als Gatekeeper eingestuft worden sind (z. B. Online-Vermittlungsdienste wie Amazon, Suchmaschinen wie Google, Onlinedienste wie Meta, Video Sharing Plattformen wie YouTube, Clouddienste wie iCloud, usw.[32] An sie ist die Herausgabe von Daten untersagt.

30 Siehe Frage 18 FAQs der EU-Kommission zum DA.
31 *Schild*, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK, Datenschutzrecht, DA, Art. 2 Rn. 87.
32 Siehe dazu Beckmann/Müller, in: Hoeren/Sieber /Holznagel, HB Multimedia-Recht, 2024, Kartellrecht, DMA Rn. 165.

4 Ablauf des Data Sharing gemäß Data Act

Im folgenden Kapitel wird zunächst der durch den DA definierte Grundmechanismus des Data Sharing anhand des Beziehungsgeflechts der wichtigsten Akteure für Data Sharing illustriert. Anschließend wird in Kapitel 4.2 in detaillierter Form anhand der Datenwertschöpfungskette Schritt für Schritt der Ablauf des Data Sharing beschrieben, unter Berücksichtigung etwaiger Regelungen, die den Grundmechanismus ergänzen.

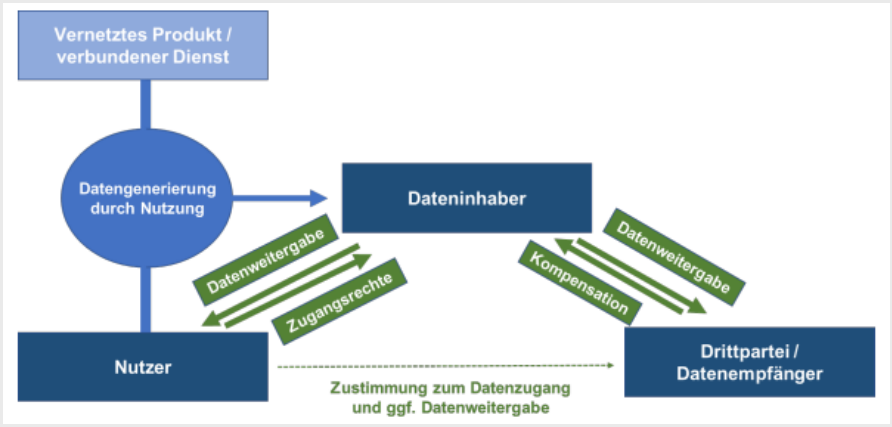
4.1 Grundmechanismus des Data Sharing gemäß Data Act

Der Grundmechanismus ergibt sich aus den jeweiligen zentralen Rechten und Pflichten der fokalen Akteure des Data Sharing und des daraus resultierenden Beziehungsgeflechts der Akteure untereinander.

Wie in Abbildung 5 illustriert, bilden Daten, die durch die Nutzung vernetzter Produkte oder verbundener Dienste generiert wurden, stets den Ausgangspunkt des im DA definierten Data Sharing. Diese Daten fallen beim Dateninhaber an (in der Regel handelt es sich hierbei um den Hersteller). Der DA definiert nun ein Zugangsrecht des Nutzers des vernetzten Produkts bzw. des verbundenen Dienstes zu denjenigen Daten, die durch seine Nutzung des Produkts generiert wurden. Folge dieses Zugangsrechts ist es, dass der Dateninhaber zur kostenfreien Weitergabe an den Nutzer verpflichtet ist.[33] Dem Nutzer wiederum steht es frei, Nutzungsvereinbarungen mit Drittparteien über eben jene Daten zu schließen. Liegt eine solche Datennutzungsvereinbarung zwischen Nutzer und Drittpartei vor, ist der Dateninhaber verpflichtet, mit der Drittpartei einen Vertrag zur Datenweitergabe abzuschließen.[34] Der Dateninhaber kann hierfür eine angemessene Vergütung durch die Drittpartei verlangen.[35] Alternativ kann die Datenweitergabe an die Drittpartei auch durch den Nutzer selbst erfolgen.

33 Siehe Art. 3 DA.
34 Siehe Art. 5 sowie Art. 8 (1) DA.
35 Siehe Art. 9 DA.

Abbildung 5: Zentrales Beziehungsgeflecht des Data Sharing gemäß DA



Quelle: Eigene Darstellung.

Anwendungsorientiertes Beispiel zur Illustration des Grundmechanismus des Data Sharing gemäß DA

Ein Medizintechnikbetrieb (Unternehmen A) setzt in seiner Produktionsstraße Anlagen eines Maschinenbauunternehmens ein (Unternehmen B). Diese Elemente sind mit Sensoren ausgestattet und erfassen bspw. den Durchsatz, die Auslastung, die Materialabnutzung etc. Es handelt sich folglich um vernetzte Produkte. Der Medizintechnikbetrieb als Nutzer der Anlagen bzw. der vernetzten Produkte bekommt durch den DA nun einen Anspruch auf den kostenfreien Zugang zu diesen Daten, die beim Maschinenbauunternehmen (in diesem Fall der Dateninhaber) anfallen. Darüber hinaus kann der Medizintechnikbetrieb die Daten mit Drittparteien teilen. Beispielsweise kann der Betrieb im Falle eines Defekts einer Anlage bzw. vernetzten Produkts des Maschinenbauunternehmens eine Drittpartei mit der Reparatur beauftragen und dieser dazu die beim Maschinenbauunternehmen (= Dateninhaber) angefallen Daten zu Verfügung stellen. Der DA sorgt also in diesem Fall durch die definierten Datenzugangsrechte u. a. dafür, dass die Markteintrittsbarrieren auf nachgelagerten Märkten sinken, da der Hersteller (in diesem Fall das Maschinenbauunternehmen) den After-Sales-Bereich schlechter abschotten kann.[36]

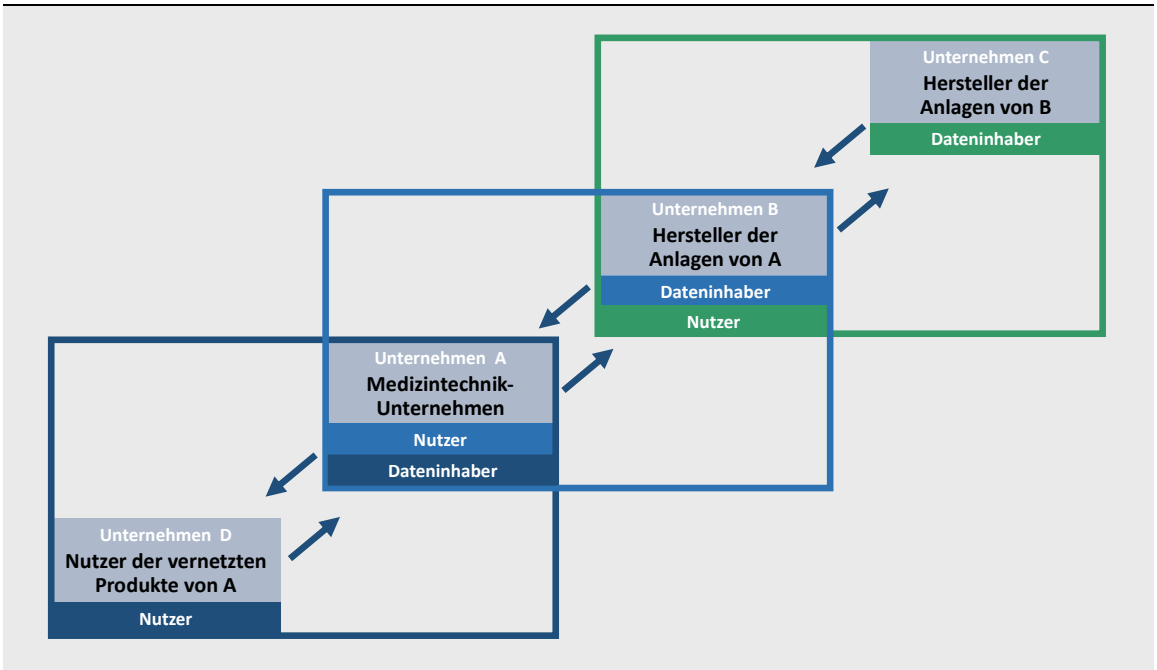
Zu beachten ist bei der Wirkungsweise des DA an dieser Stelle zudem, dass dieser keineswegs zu einer einseitigen Besserstellung des Medizintechnikbetriebs bzw. einer einseitigen Schlechterstellung des Maschinenbauunternehmens führt. Da die Akteure am Markt in vielfältigen wirtschaftlichen Beziehungen stehen, finden sich diese in der Regel sowohl in der Rolle des Dateninhabers als auch des Nutzers und ggf. der Drittpartei wieder – jeweils in Bezug auf andere Daten und deren Entstehungsweise.[37] *Handelt es*

36 In diesem Fallbeispiel werden Datenschutzaspekte nicht berücksichtigt. Handelt es sich bei den Daten um personenbezogene Daten, kann die Datenweitergabe aufgrund der Bestimmungen der DSGVO untersagt sein.

37 Wichtig ist jedoch zu beachten, dass in Bezug auf ***dieselben*** Daten immer **nur eine Rolle** eingenommen werden kann, also Nutzer, Dateninhaber oder Drittpartei.

sich bspw. bei den Präzisionsteilen für die Medizintechnik um vernetzte Produkte, findet sich der Medizintechnikbetrieb beim Verkauf seiner Produkte in der Rolle des Dateninhabers wieder und muss dementsprechend die Datenzugangsansprüche der Nutzer seiner Produkte erfüllen. Gleichzeitig findet sich das Maschinenbauunternehmen B für die diejenigen vernetzten Anlagen, die das Unternehmen für die Herstellung der Anlagen für den Medizinbetrieb einsetzt (sofern er diese nicht selbst herstellt) als Nutzer wieder und erhält somit Zugangsrechte für die im Zuge dessen generierten Daten. Die Parallelität von verschiedenen Rollen für die einzelnen Akteure wird zusammenfassend in Abbildung 6 verdeutlicht. Pauschale Aussagen über die Profiteure des DA sind daher nur schwer zu treffen.

Abbildung 6: Illustration des Praxisbeispiels zur Verdeutlichung der Parallelität der Rollen im Data Act



Quelle: Eigene Darstellung.

Mit Blick auf den Grundmechanismus des Data Sharing lässt sich somit eine prinzipielle Nutzerzentrierung feststellen. Die Verfügungsrechte des Nutzers über die durch ihn generierten Daten werden gegenüber dem Dateninhaber gestärkt. Wie in Kapitel 2 anhand der ökonomischen Wirkkette illustriert, soll auf diese Weise die Nutzung der Daten erleichtert und incentiviert werden, um so die von den Daten ausgehenden Wertschöpfungspotenziale besser ausnutzen zu können.

Im anschließenden Kapitel 4.2 wird anhand der Datenwertschöpfungskette Schritt für Schritt von der Datengenerierung bis zur Datennutzung aufgezeigt, welche Auswirkungen der Data Act auf die jeweiligen Stufen der Datenwertschöpfungskette hat, welche den Grundmechanismus ergänzenden oder teilweise korrigierenden Regelungen und Sonderfälle es auf den einzelnen Stufen gibt und welche Wirkungen wiederum von diesen Regelungen bzw. Sonderfällen zu erwarten sind.

4.2 Ablauf des Data Sharing entlang der Datenwertschöpfungskette

Ausgehend von der Markteinführung eines vernetzten Produkts bzw. eines verbundenen Dienstes sollen im Folgenden die Auswirkungen des Data Sharing Schritt für Schritt entlang der Datenwertschöpfungskette erläutert werden. Für die Datenwertschöpfungskette lassen sich aus dem DA die folgenden Stufen ableiten:

(1) Datengenerierung & Datenerfassung,

(2) Datenzugang,

(3) Datenbereitstellung bzw. Datenweitergabe, sowie die

(4) Datenauswertung bzw. Datennutzung.

Abbildung 7: Wertschöpfungskette des Data Sharing

Quelle: Eigene Darstellung.

4.2.1 Datengenerierung & Datenerfassung

Die Datengenerierung und die Datenerfassung stellen den Nukleus jedes datenbasierten Wirtschaftens und damit auch für das Data Sharing dar.

Datengenerierung durch Zusammenspiel von Hersteller und Nutzer

In den Erwägungsgründen das DA wird die Datengenerierung als das Ergebnis von mindestens zwei Akteuren beschrieben: Dem Hersteller als Konstrukteur des vernetzten Produkts sowie dem Nutzer des Produkts. Hieraus wird geschlussfolgert, dass es die Fairness in der digitalen Wirtschaft gebiete, nicht einem einzelnen Akteur die ausschließlichen Zugangs- und Nutzungsrechte zuzuordnen sondern einen allgemeinen Ansatz bei der Zuweisung von Rechten für den Datenzugang und -nutzung zu verfolgen, der es ermöglicht, dass verschiedene Akteure vom Mehrwert der Daten profitieren können.[38]

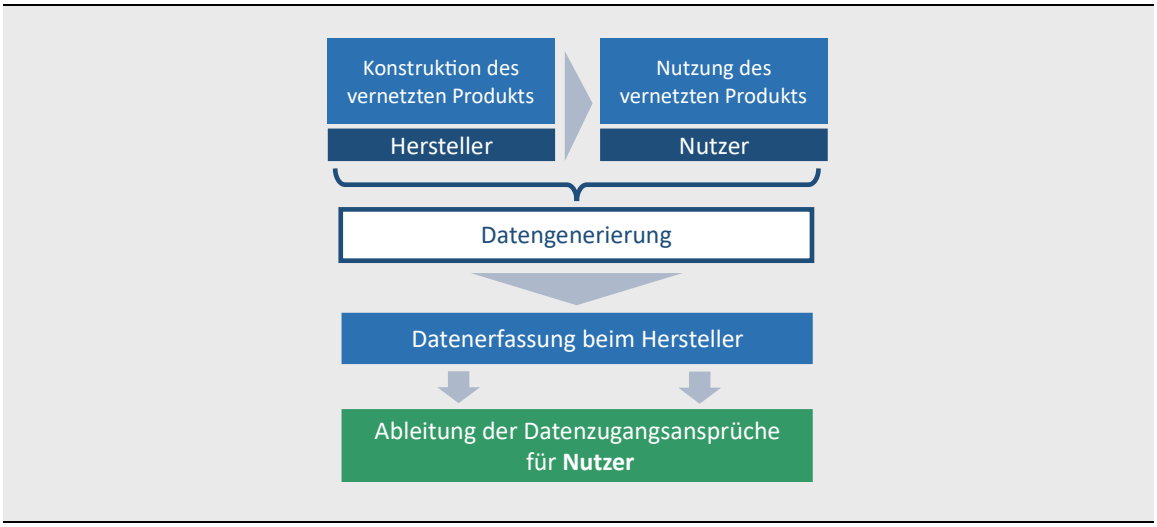
Es wird folglich aus dem Akt der Datengenerierung, welcher auf einem Zusammenspiel von Nutzer und Hersteller basiert, ein direkter Rechtfertigungsgrund für das Data Sharing gemäß DA abgeleitet.

38 Siehe Erw.-Gr. (6) DA.

Erfassung der generierten Daten beim Hersteller

Dass der Data Act bei der Zuordnung der Rechte eine Nutzerzentrierung einnimmt, liegt an der Datenerfassung, die sehr eng mit der Datengenerierung verbunden ist:[39] Soll von der Datengenerierung ein ökonomischer Mehrwert ausgehen, dann müssen die generierten Daten zwangsläufig auch erfasst werden. Bei vernetzten Produkten bzw. verbundenen Diensten fallen die generierten Daten in der Regel beim Hersteller bzw. Anbieter an. Da der Hersteller dementsprechend bereits by design Zugang zu den Daten hat, definiert der DA Zugangsrechte für Nutzer, um auch diesen den Zugriff auf die Daten zu ermöglichen.[40] Dieser Zusammenhang wird in Abbildung 8 prozessual und illustrierend dargestellt.

Abbildung 8: Einordnung der Datenerfassung im Sinne des Data Act



Quelle: Eigene Darstellung.

Informationspflichten der Hersteller für die Nutzer zur Transparenzerhöhung

Für die Ermöglichung der selbstbestimmten Wahrnehmung der Nutzerrechte hat der Gesetzgeber daher vorvertragliche Informationspflichten für die Hersteller bzw. Anbieter erlassen. Gemäß dieser Pflichten muss der Hersteller bzw. Anbieter eines vernetzten Produktes bzw. verbundenen Dienstes noch *vor* Vertragsschluss einem potenziellen Nutzer Auskunft über die Art, das Format sowie den Umfang der Daten geben, die dieses Produkt bzw. Dienst durch die Nutzung generiert. Mit diesem Transparenzgewinn bzgl. der generierten Daten soll die Ausübung der Nutzerrechte (im Sinne der Zugangsansprüche) erleichtert werden. Diesen vorvertraglichen Informationspflichten kann bspw. durch das Aufsetzen einer einfachen Website des Anbieters bzw. Herstellers, auf der die einschlägigen Informationen zu finden sind, nachgekommen werden.[41]

---

39 Zur Nutzerzentrierung siehe z. B. Arioli (2024).

40 Zu betonen ist, dass an dieser Stelle die Datenerfassung bzw. der Datenzugang diskutiert werden. Dies inkludiert nicht automatisch die Datennutzung. So ist bspw. gemäß DA für die Datennutzung durch den Dateninhaber eine Nutzungsvereinbarung mit dem Nutzer erforderlich. Siehe hierzu Kapitel 3.2.4.

41 Siehe Art. 3 DA in Verbindung mit Erw.-Gr. (24) des DA.

Zusammenfassend stellt die Datengenerierung und -erfassung den Ausgangspunkt der Wertschöpfung durch Daten dar. Aus der Tatsache, dass der Nutzer durch seine Nutzung des vernetzten Produkts die Daten generiert, leitet der DA für den Nutzer Zugangsansprüche und Verfügungsrechte an den Daten ab. Vorvertragliche Informationspflichten des Dateninhabers über die durch die Produkte und Dienste generierten und erfassten Daten sollen die Transparenz für die Nutzer erhöhen und dadurch die Wahrnehmung der Rechte der Nutzer an den Daten erleichtern.

4.2.2 Datenzugang

Der Datenzugang stellt den für den DA zentralen Schritt in der Datenwertschöpfungskette dar. Nicht ohne Grund kommt der Begriff „Datenzugang“ auch im Titel des DA vor. Der Datenzugang wird als der entscheidende Bottleneck auf dem Weg zur mehrfachen Nutzung der Daten gesehen. Dementsprechend werden im DA Datenzugangsansprüche definiert, um auf diese Weise Datenmärkte zu öffnen und zu entwickeln.[42] Die Zugangsansprüche richten sich stets gegen den Dateninhaber, bei dem es sich häufig um den Hersteller bzw. Anbieter eines vernetzten Produkts bzw. verbundenen Dienstes handelt.

Zugangsanspruch auf Rohdaten und vorverarbeitete Daten beschränkt

Der nach DA definierte Zugangsanspruch gilt stets nur für Rohdaten und vorverarbeitete Daten *(„pre-processed data*“), nicht aber für aus den Daten gefolgerte oder abgeleitete Informationen *(„inferred or derived data“)*. Das bedeutet, dass sich der Zugangsanspruch auf Daten inkl. der einschlägigen Metadaten einschließlich ihres grundlegenden Kontexts und Zeitstempels erstreckt, nicht aber auf Daten, die das Ergebnis einer Datenauswertung (bspw. mittels proprietärer Algorithmen bzw. Software sind).[43] Die Beschränkung des Zugangsanspruch auf Rohdaten und vorverarbeitete Daten soll bewirken, dass die Wertschöpfung der Dateninhaber nicht zu stark abgeschöpft wird und die Investitionsanreize der Dateninhaber erhalten bleiben.

Mittelbare und unmittelbare Zugangsansprüche

Je nach Akteur lassen sich unmittelbare und mittelbare Datenzugangsansprüche unterscheiden: Ein unmittelbarer Zugangsanspruch besteht für die Nutzer an den Daten, die sie durch ihre Nutzung eines vernetzten Produkts oder verbundenen Dienstes generiert haben. Ein mittelbarer Zugangsanspruch besteht für Drittparteien. Diese haben einen Anspruch auf den Zugang zu den vom Nutzer generierten Daten, wenn eine Datennutzungsvereinbarung zwischen Nutzer und der entsprechenden Drittpartei vorliegt. Davon ausgenommen sind allerdings Gatekeeper im Sinne des Digital Markets Act (EU-Verordnung 2022/1925). Diesen wird gemäß Artikel 5 (3) des DA der Datenzugangsanspruch als Drittpartei entzogen.[44] Hierdurch soll erreicht werden, dass

42 Siehe zur beabsichtigten Wirkkette sowie der Intention des DA auch Kapitel 2.
43 Vgl. hierzu Erw.-Gr. (36) DA.
44 Siehe Art. 5 (3) DA.

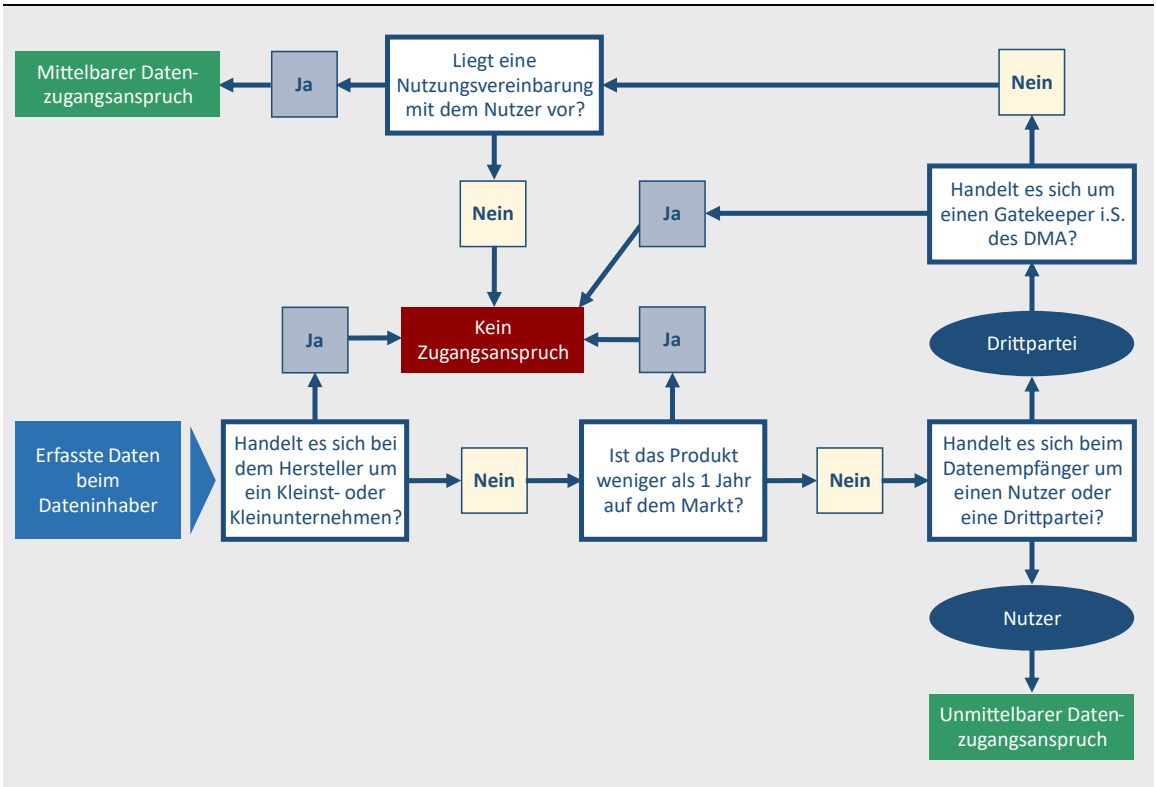
die Unternehmen in Gatekeeper-Positionen durch den DA nicht noch weiter gestärkt werden. Aus dem gleichen Grund ist es daher Drittparteien, die die Daten über den mittelbaren Datenzugangsanspruch des DA erhalten haben, auch untersagt, diese Daten dann wiederum mit einem Gatekeeper zu teilen.[45]

Mittelstandsspezifische Besonderheiten des Zugangsanspruchs

Im DA wird beim Datenzugang zudem eine Schutzklausel für Kleinst- und Kleinunternehmen implementiert. Unternehmen in der Rolle als Dateninhaber mit weniger als 50 Mitarbeitern sowie eines Jahresumsatzes von weniger als 10 Millionen Euro sind von Datenzugangsansprüchen gegen sie ausgenommen. Das bedeutet, dass diese Unternehmen, die durch die Nutzung von vernetzten Produkten und verbundenen Diensten generierte Daten nicht mit Nutzern oder Drittparteien teilen müssen. Gleiches gilt für mittlere Unternehmen (50-249 Mitarbeiter und Jahresumsatz zwischen 10 und 50 Mio. Euro.), wenn diese seit weniger als einem Jahr in diese Größenklasse aufgestiegen sind oder wenn das von ihnen vertriebene vernetzte Produkt bzw. verbundener Dienst weniger als ein Jahr auf dem Markt ist.[46] Ziel dieser Regelung ist es, dass insbes. die Position von Kleinst- und Kleinunternehmen nicht durch etwaige Datenzugangsansprüche gegen sie geschwächt werden soll. Kritisiert wird allerdings, dass die Grenzen für die Schutzklausel im DA sehr eng gefasst sind, so dass nur für einen gewissen Teil des Mittelstands die Schutzklausel greift.[47] Insbesondere der industrielle Mittelstand, in dem mittlere Unternehmen (50 – 249 Mitarbeiter) stark vertreten sind, fällt somit häufig nicht unter die allgemeine Schutzklausel für KMU und muss spätestens nach einem Jahr den Datenzugangsansprüchen nachkommen.

45 Siehe Erw.-Gr. (40) DA.
46 Siehe für die mittelstandsspezifischen Ausnahmen beim Datenzugang Art. 7 DA.
47 Vgl. Krämer (2023), S. 57.

Abbildung 9: Prüfschema für den Datenzugangsanspruch



Quelle: Eigene Darstellung.

4.2.3 Datenbereitstellung bzw. Datenweitergabe

Nimmt der Nutzer bzw. die Drittpartei ihr Datenzugangsrecht in Anspruch, besteht der nächste Schritt in der Datenbereitstellung durch den Dateninhaber. Dem *Datenzugangsrecht* des Nutzers bzw. Dritten steht folglich spiegelbildlich die *Datenbereitstellungspflicht* des Dateninhabers entgegen.

Direkte und indirekte Datenbereitstellung an den Nutzer

Es lassen sich dabei die direkte und die indirekte Datenbereitstellung unterscheiden. Bei der direkten Bereitstellung ist das vernetzte Produkt so konzipiert, dass der Nutzer „by design“ auf die Daten zugreifen kann.[48] Der Nutzer muss folglich bei der direkten Bereitstellung seine Inanspruchnahme des Datenzugangsrecht beim Dateninhaber nicht anzeigen, sondern kann direkt auf die Daten über eine geeignete Schnittstelle zugreifen. Da die direkte Bereitstellung der Daten bei der Konzeption von Produkten mitgedacht werden muss, sieht der DA hier längere Übergangsfristen vor: Die Pflicht zur direkten Bereitstellung besteht für vernetzte Produkte, die ab dem 12. September 2026 auf den Markt gebracht werden.[49]

48 Siehe hierzu Art. 3 (1) DA.
49 Siehe Art. 50 DA.

Für Produkte, die vor dem Stichtag zur direkten Bereitstellung auf den Markt gebracht wurden oder für die eine direkte Bereitstellung nicht relevant oder aus technischen Gründen zu nicht vertretbarem Aufwand möglich ist, greift die indirekte Bereitstellung der Daten. Auf einfaches Ersuchen des Nutzers hat der Dateninhaber diesem die Daten unverzüglich zukommen zu lassen. Die Daten sollen dabei die gleiche Qualität wie für den Dateninhaber aufweisen und sollen dem Nutzer, soweit technisch möglich, kontinuierlich und in Echtzeit zugehen.[50]

Unabhängig davon, ob die Bereitstellung direkt oder indirekt erfolgt, muss diese für den Nutzer unentgeltlich, einfach und sicher sein. Gleichzeitig muss die Bereitstellung umfassend erfolgen und in einem gängigen und maschinenlesbaren Format für den Nutzer auslesbar sein.[51]

Datenbereitstellung an Drittparteien: Indirekte Bereitstellung gegen Vergütung

Besteht ein mittelbarer Datenzugangsanspruch für eine Drittpartei, d. h. liegt eine Nutzungsvereinbarung für diese Daten zwischen dem Nutzer und einer Drittpartei vor, gelten für die Datenbereitstellung an die Drittpartei durch den Dateninhaber dieselben Anforderungen wie im Fall der indirekten Bereitstellung an den Nutzer. Die Daten müssen demnach unverzüglich und in gleicher Qualität der Drittpartei zur Verfügung gestellt werden.[52]

Ein wesentlicher Unterschied der Datenbereitstellung durch den Dateninhaber an eine Drittpartei im Vergleich zum Nutzer besteht in der Vergütung: Während die Bereitstellung durch den Dateninhaber an den Nutzer unentgeltlich erfolgen muss, kann der Dateninhaber bei einer Bereitstellung an eine Drittpartei eine angemessene Gegenleistung verlangen. Gemäß Art. 9 des DA können bei der Höhe der Gegenleistung sowohl die Kosten für die Bereitstellung der Daten als auch die Kosten für Investitionen in die Erhebung der Daten berücksichtigt werden. Die Gegenleistung hat sich somit an den Kosten und nicht an dem Wert der Daten, die übermittelt werden, zu orientieren. Handelt es sich bei der Drittpartei um ein kleines oder mittleres Unternehmen (KMU) oder gemeinnützige Forschungseinrichtung, greift eine Ausnahmeregelung: Hier dürfen bei der Höhe der Gegenleistung vom Dateninhaber nur die Kosten der Bereitstellung, nicht aber die Kosten der Investition in die Generierung der Daten berücksichtigt werden.[53]

Alternativ kann die Bereitstellung der Daten an die Drittpartei auch über den Nutzer erfolgen. Hat dieser die Daten vom Dateninhaber über die direkte oder indirekte Bereitstellung erhalten, kann er die Daten an die Drittpartei weitergeben . Zu den Konditionen der Datenweitergabe an eine Drittpartei durch den Nutzer macht der DA keine Vorgaben. Diese sind somit zwischen Nutzer und Drittpartei frei auszuhandeln.

50 Siehe hierzu Art. 4 (1) DA.
51 Siehe Art. 3 (1) sowie Art. 4 (1) DA.
52 Siehe Art. 5 DA.
53 Siehe Art. 9 (4) DA.

Bereitstellung von als Geschäftsgeheimnis klassifizierten Daten

Mit Blick auf die Wahrung von Geschäftsgeheimnissen muss der DA einen Trade-Off lösen: Für das Funktionieren der marktwirtschaftlichen Mechanismen ist es einerseits wichtig, dass wesentliche Geschäftsgeheimnisse der Dateninhaber gewahrt bleiben. Würde man allerdings pauschal alle vom Dateninhaber als Geschäftsgeheimnis klassifizierten Daten von der Bereitstellung für Nutzer und Dritte ausnehmen, würde man ein Schlupfloch für das Umgehen des DA schaffen, welches die Wirksamkeit des DA untergraben würde.

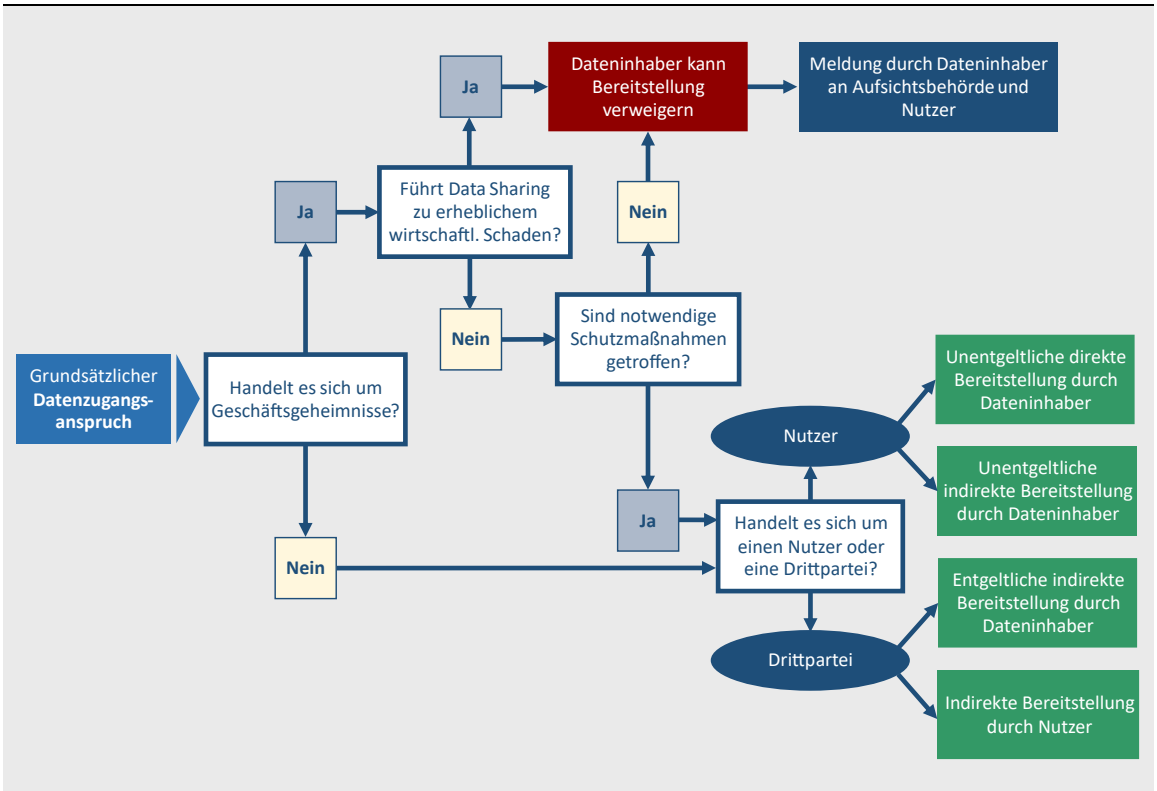
Der Gesetzgeber hat daher versucht, im DA ein zweistufiges Vorgehen im Hinblick auf den Umgang mit Geschäftsgeheimnissen zu etablieren, welches den Trade-Off austarieren soll. Grundsätzlich sind Geschäftsgeheimnisse zunächst nicht von den Datenzugangsansprüchen der Nutzer und Drittparteien ausgenommen. Werden Daten vom Dateninhaber als Geschäftsgeheimnis eingestuft, müssen die Datenempfänger und Nutzer allerdings vor der Datenbereitstellung nachweisen, dass sie hinreichende organisatorische und technische Schutzmechanismen zur Wahrung der Geschäftsgeheimnisse implementiert haben. Welche Schutzmaßnahmen als notwendig erachtet werden, sind dabei zwischen Dateninhaber und Nutzer bzw. Dritten auszuhandeln. Darüber hinaus muss der Dateninhaber bereits vorvertraglich auf die Geschäftsgeheimnisse hinweisen.[54]

Bei Daten, deren Teilen nach Einschätzung des Dateninhabers für diesen zu einem erheblichen wirtschaftlichen Schaden führen würde, kann der Dateninhaber im Einzelfall die Bereitstellung der Daten verweigern. Die Verweigerung der Datenbereitstellung ist dem Nutzer und zusätzlich der zuständigen Aufsichtsbehörde dabei unverzüglich unter der Darlegung objektiver Gründe schriftlich mitzuteilen. Dem Nutzer bzw. der Drittpartei steht es offen, hiergegen Beschwerde einzulegen. Die Hürden für die Inanspruchnahme dieser Ausnahmeregelung durch den Dateninhaber sind allerdings hoch gesetzt. Diese ist gemäß Gesetzestext nur unter „außergewöhnlichen Umständen“ möglich.[55]

Zusammenfassend ist die Datenbereitbestellung gemäß DA in Form eines Prüfschemas in Abbildung 10 dargestellt.

54 Vgl. Art. 3 (3) DA.
55 Siehe Art. 4 (8) DA.

Abbildung 10: Prüfschema der Datenbereitstellung gemäß Data Act



Quelle: Eigene Darstellung.

4.2.4 Datenauswertung & Datennutzung

Der Phase der Datenbereitstellung schließt sich die Phase der Datennutzung an. Da sich der Zugangsanspruch des DA auf Rohdaten bzw. vorverarbeitete Daten beschränkt, dürfte in vielen Fällen des Data Sharing auf der Basis des DA noch eine weitergehende Datenauswertung der eigentlichen Datennutzung, aus der schließlich die Mehrwerte resultieren, vorgeschaltet sein. Die Form und Intention der Nutzung der bereitgestellten Daten durch den Nutzer des vernetzten Produkts ist stark abhängig von der jeweiligen Situation und den Ressourcen des Nutzers. Es lassen sich dabei insbesondere die Nutzung der Daten für unternehmensinterne Zwecke von der Nutzung für rein monetäre Zwecke unterscheiden.

Nutzung der Daten für unternehmensinterne Zwecke

Erwartet der Nutzer einen Mehrwert aus den Daten für sein eigenes Unternehmen, hängt die Form der Nutzung stark von den Ressourcen und Kapazitäten im Unternehmen ab. Hat der Nutzer bspw. entsprechendes Data Science-Know-how im Unternehmen, kann dieser die bereitgestellten (Roh-)Daten selbst auswerten und zur Optimierung seiner Prozesse einsetzen. Ist der Nutzer bspw. ein produzierendes Unternehmen und nutzt vernetzte Maschinenbauteile eines anderen Herstellers, kann der Nutzer die vom

Hersteller bereitgestellten Maschinendaten selbst auswerten und daraus idealerweise Optimierungen seiner Produktionsabläufe ableiten.

Hat der Nutzer keine entsprechenden Ressourcen, kann er alternativ die Daten an eine Drittpartei weitergeben und diese damit beauftragen, die Daten auszuwerten und geeignete Maßnahmen daraus abzuleiten. Je nach Kapazität und Ressourcen des Nutzers kann diese oder eine weitere Drittpartei vom Nutzer auch direkt damit beauftragt werden, die Maßnahmen umzusetzen. Hat der Nutzer das notwendige Know-how für das Umsetzen der Maßnahmen inhouse vorhanden, kann er diese auch selbst durchführen.

Anwendungsorientiertes Beispiel: Bei dem produzierenden Unternehmen A (Nutzer) tritt ein Defekt in seiner Produktionsstraße auf. In der Produktionsstraße kommen vernetzte Maschinen des Herstellers B (Dateninhaber) zum Einsatz. Das Unternehmen A hat selbst nicht das entsprechende Know-how den Defekt unternehmensintern hinreichend zu analysieren. Es beauftragt daher Dienstleistungsunternehmen C als Drittpartei zunächst mit der Analyse des Defekts. Dazu schließen A und C eine Nutzungsvereinbarung bzgl. der Daten der von B hergestellten Maschinen. B muss C daher die Daten gegen eine angemessene Vergütung unverzüglich und in vollem Ausmaß bereitstellen. Dazu ist eine vertragliche Vereinbarung zwischen B und C zu treffen, die die Vorgaben der Kapitel 3 und 4 DA berücksichtigt. C analysiert auf Basis der Daten den Defekt und präsentiert das Ergebnis gegen Vergütung dem Unternehmen A. A kommt auf Basis des Ergebnisses zum Schluss, dass der Defekt nicht selbst behoben werden kann. Nach einer Sondierung der Preise am Markt für die notwendige Reparatur beauftragt A schließlich C mit der Reparatur.

Das gerade angeführte Beispiel verdeutlicht, wie der DA insbesondere im After-Sales-Bereich das Potenzial hat, die Märkte zu öffnen und in Folge der erhöhten Datenverfügbarkeit und -nutzung effizienter zu machen. In der Situation ohne DA und damit ohne gesetzlichen Datenzugangsanspruch für Nutzer und Drittpartien hat der Maschinenhersteller de facto die Kontrolle über die Daten, die durch die Nutzung der von ihm hergestellten Maschinen generiert wurden. Um den After-Sales-Markt vor Wettbewerben abzuschotten, hat er dementsprechend keinen Anreiz, seine Daten mit dem Nutzer oder mit Drittparteien zu teilen. Durch die Aufrechterhaltung der Informationsasymmetrien zwischen ihm und dem Nutzer bzw. der Drittpartei werden Markteintrittshürden in den After-Sales-Bereich, also nachgelagerten Märkten, zementiert. Durch den vom DA nun geschaffenen Datenzugangsanspruch werden eben jene Zugangshürden im After-Sales-Bereich eingerissen und es wird der Wettbewerb intensiviert, was zu volkswirtschaftlichen Wohlfahrtsgewinnen führt.

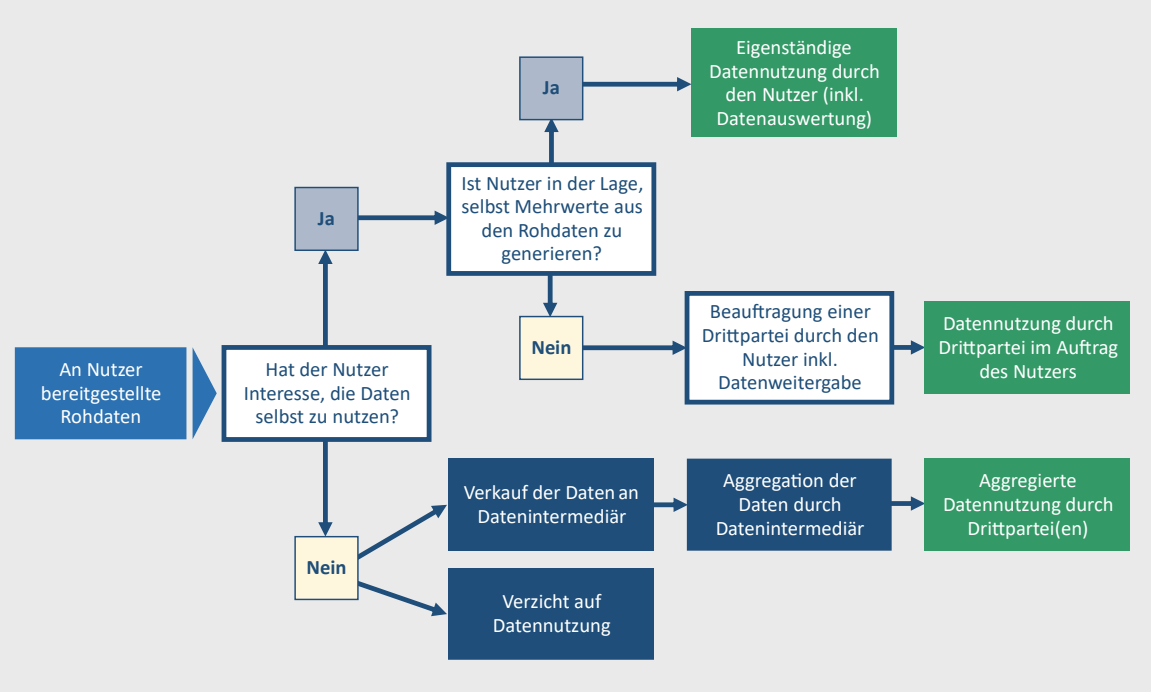
Verkauf der Daten an Datenintermediäre

Zusätzlich zur Verwertung der bereitgestellten Daten für das eigene Unternehmen hat der Nutzer die Option, die Daten an interessierte Drittparteien zu verkaufen. In der Regel dürfte es sich dabei um Datenintermediäre handeln. Diese kaufen die Daten vieler Nutzer

auf, poolen sie und verkaufen sie schließlich in aggregierter Form weiter an Interessenten. Bei den Interessenten kann es sich beispielsweise um Servicedienstleister handeln, die auf der Basis der aggregierten Daten ihre Services verbessern wollen. Auf diese Weise kann der DA zur Erhöhung der Datenliquidität beitragen, selbst wenn der Nutzer in den Daten kein Optimierungspotenzial für sein eigenes Unternehmen sieht.

Zusammenfassend sind die Varianten der Datennutzung aus der Sicht des Nutzers in Abbildung 11 dargestellt.

Abbildung 11: Varianten der Datennutzung gemäß Data Act aus der Sicht eines Nutzers



Quelle: Eigene Darstellung.

Einschränkung der Freiheit der Datennutzung durch Non-Wettbewerbsklausel

Eine Einschränkung erhält die Freiheit der Nutzung der bereitgestellten Daten für Nutzer und Drittparteien durch eine Non-Wettbewerbsklausel im Data Act. Diese besagt, dass Nutzer und Dritte die bereitgestellten Daten nicht dafür nutzen dürfen, konkurrierende Produkte auf den Markt zu bringen.[56]

Der DA fokussiert sich folglich darauf, auf nachgelagerten Märkten den Wettbewerb zu verstärken, nicht aber auf der Produktebene Die Intention dieser Klausel besteht darin, die unternehmerischen Anreize des Herstellers zu wahren. Offen bleibt, wie streng die Klausel ausgelegt werden wird, d. h. was als konkurrierendes Produkt eingestuft wird und mit welchem zeitlichen Horizont agiert wird (heißt: Wie lange muss die letzte Bereitstellung von entsprechenden Daten her sein, damit man auf dem Markt als Wettbewerber

56 Siehe Art. 4 (10) DA für Nutzer sowie Art. 6 (2) (3) für Dritte. Für verbundene Dienste gilt die Non-Wettbewerbsklausel nicht.

auftreten kann?). In Erw.-Gr. (32) heißt es hierzu lediglich, dass die Entscheidung auf Basis bewährter Grundsätze des Wettbewerbsrechts erfolgen soll.

Datennutzung durch den Dateninhaber

Während sich die bisherigen Ausführungen auf die Datennutzung durch den Nutzer bezogen haben, trifft der DA daneben auch Regelungen bzw. Einschränkungen für die Datennutzung durch den Dateninhaber. Dieser darf gemäß DA die Daten nur nutzen, wenn ein Datennutzungsvertrag zwischen ihm und dem Nutzer vorliegt.[57] Für den Datennutzungsvertrag beabsichtigt die EU-Kommission, Mustervertragsklauseln bereitzustellen, die eine faire Datennutzung ermöglichen.[58] Auf diese Weise soll gewährleistet werden, dass missbräuchlichen Vertragsklauseln, insbes. durch den Dateninhaber vorgebeugt wird. Schutz vor missbräuchlichen Vertragsklauseln gewährt für den B2B-Bereich zudem Art. 13 des DA. Dieser definiert zum einen, was als missbräuchlich im Sinne des DA zu verstehen ist und erklärt missbräuchliche Vertragsklauseln für unwirksam. Art. 13 stellt somit eine Schutzklausel für die faire Verteilung der Datennutzung dar. Ähnliches gilt für Art. 7 (2) DA, welcher sowohl für den B2B als auch B2C-Bereich Vertragsklauseln, welche die im DA für das Data Sharing definierten Nutzerrechte untergraben, für nicht bindend erklärt.

57 Siehe Art. 4 (13) DA.
58 Siehe Erw.-Gr. (111) DA.

5 Zwischenfazit zum Teil I

Durch die Darstellung der im DA definierten Regelungen für das Data Sharing entlang der Datenwertschöpfungskette wurde deutlich, dass die Intention des DA darin besteht, die Mehrfachnutzung der Daten, die im Bereich der vernetzten Produkte und verbundenen Dienste anfallen, zu ermöglichen. Auf diese Weise sollen volkswirtschaftliche Wertschöpfungspotenziale realisieren werden.

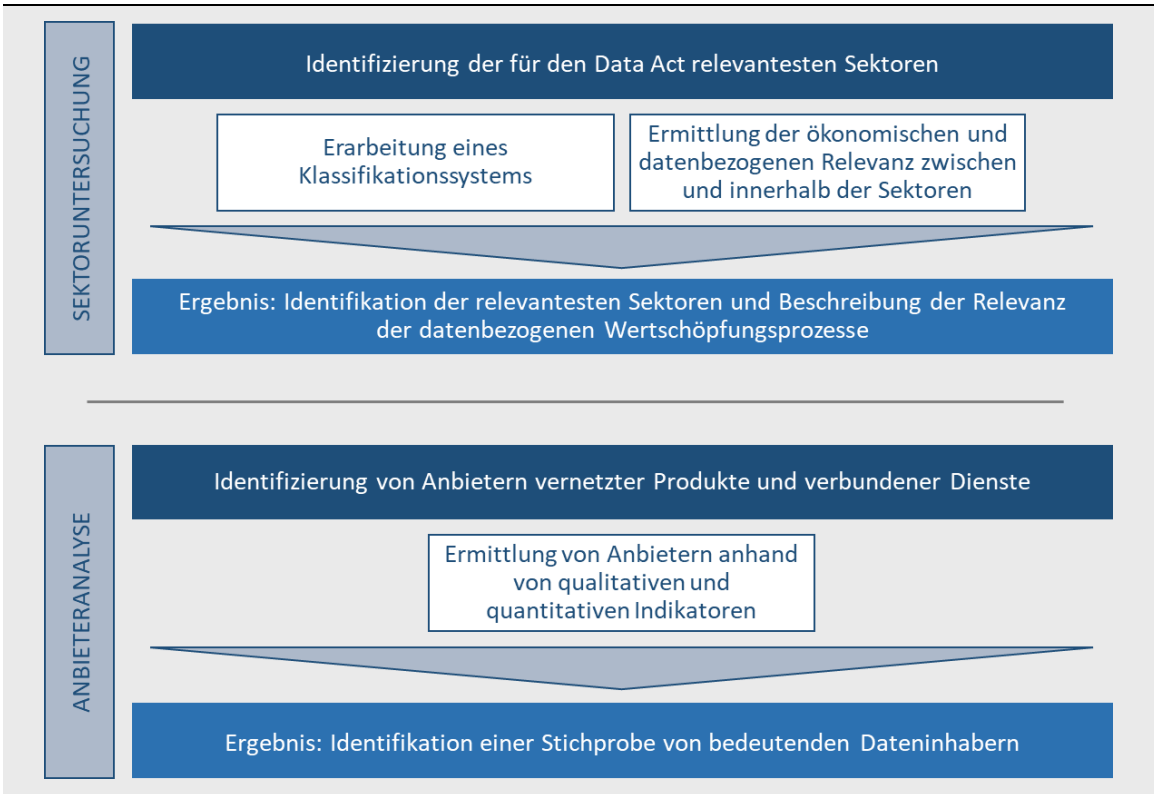
Das Ziel soll durch eine Stärkung der Position des Nutzers erreicht werden. Für ihn sollen Datenzugangsrechte geschaffen und die Verfügungsrechte für die Nutzung der Daten bei ihm konzentriert werden. Damit soll die gegenwärtige de facto-Kontrolle über die von vernetzten Produkten und verbundenen Diensten generierten Daten durch den Dateninhaber bzw. Hersteller aufgebrochen werden.

Die Rechtfertigung für die Zugangsrechte für Datennutzer wird darin gesehen, dass zur Datengenerierung sowohl der Hersteller / Dateninhaber (durch die Konzeption des Produkts / Dienstes) als auch der Nutzer (durch die Nutzung des Produkts / Dienstes) beitragen. Da die Daten durch den Dateninhaber erfasst werden, ist dieser in der besseren Ausgangsposition. Aus diesem Grund wird der Nutzer durch den DA auf den Stufen des Datenzugangs und der Datennutzung in seinen Rechten gestärkt, um so zu ausgeglicheneren Machtverhältnissen zwischen Nutzer und Dateninhaber zu gelangen.

TEIL II: Empirische Sektoruntersuchung und Anbieteranalyse

Im Fokus von Teil II steht die Identifikation der vom DA besonders betroffenen Sektoren und Anbieter. Hierzu wurde eine systematische Analyse vorgenommen, wobei zunächst mit der Sektoruntersuchung begonnen wurde und darauf aufbauend die Anbieteranalyse erfolgte (vgl. Abbildung 12).

Abbildung 12: Vorgehensweise zur Sektoruntersuchung und Anbieteranalyse



Quelle: Eigene Darstellung.

Als horizontale Regulierung ist der DA für alle Wirtschaftsbereiche gleichermaßen einschlägig. Das Ziel der Sektoruntersuchung ist es, diejenigen Sektoren zu identifizieren, die aufgrund ihrer allgemeinwirtschaftlichen sowie datenökonomischen Relevanz besonders von der Verordnung betroffen sind.

Die Auswahl der Sektoren basierte auf qualitativen und quantitativen ökonomischen Indikatoren sowie Indikatoren, die Aussagen über die Relevanz von Daten innerhalb eines Sektors ermöglichen. Im Rahmen der angewandten Identifikationsstrategie von Indikatoren ließen sich nicht für sämtliche Sektoren belastbare Daten ermitteln. Daher bedeutet der Ausschluss einzelner Sektoren nicht notwendigerweise, dass diese irrelevant sind. Vielmehr lagen keine belastbaren Daten vor, um die Relevanz zu belegen. Das Ergebnis ist die Identifikation von elf Sektoren, deren Relevanz sich im Kontext des DA belegen ließ.

Eine ähnliche Situation zeigt sich im Kontext der Anbieteranalyse. Die Auswahl der Unternehmen erfolgte einem iterativen Auswahlmechanismus, bei dem durch die Anwendung zunehmend spezifischer Kriterien eine sukzessive Fokussierung auf Dateninhaber (Anbieter) erfolgte. Die Grundlage für diesen Prozess bildete eine initiale Stichprobe von 500 Unternehmen, die über zugängliche Rankings, Studien und Datenbanken erfasst wurde. Unternehmen, die im Rahmen der angewandten initialen Identifizierungsstrategie nicht erfasst wurden, wurden nicht weiter im Auswahlprozess berücksichtigt. Dies impliziert nicht, dass nicht berücksichtigte Unternehmen grundsätzlich irrelevant sind. Im Ergebnis konnten aus der initialen Stichprobe 166 bedeutende Unternehmen (Dateninhaber) in den Sektoren identifiziert werden, die zuvor in der Sektoruntersuchung ermittelt wurden.

6 Die Sektoruntersuchung

Nachfolgend werden die Arbeitsschritte und die Ergebnisse der Sektoruntersuchung dargestellt.

6.1 Vorgehensweise zur Identifikation relevanter Sektoren

Um die relevanten Sektoren zu identifizieren, wurde in einem ersten Schritt ein geeignetes Klassifikationssystem festgelegt. Die Klassifikation nach Wirtschaftszweigen (WZ 2008) in Deutschland bzw. nach der statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) bietet eine dedizierte Klassifikation wirtschaftlicher Aktivitäten. Aufgrund ihrer weiten Verbreitung und Anwendung in amtlichen Statistiken, gewährleistet sie die höchste Vergleichbarkeit der Sektoren. Des Weiteren erlaubt sie eine möglichst konsistente Analyse auf einer einheitlichen methodischen Grundlage. Aus diesen Gründen wurden **die Wirtschaftszweige bzw. die NACE als Grundlage für die Sektoruntersuchung** herangezogen.[59]

Dabei lag der Fokus auf der Gliederungsebene der Abschnitte. Die Abgrenzung der Sektoren nach NACE erfolgt anhand wirtschaftlicher Tätigkeiten: Der primäre Sektor (Abschnitt A) umfasst Landwirtschaft, Forstwirtschaft und Fischerei. Der sekundäre Sektor (Abschnitte B – F) beinhaltet Industrie und Bauwesen, einschließlich der Herstellung landwirtschaftlicher Maschinen. Der tertiäre Sektor (Abschnitte G – U) umfasst Dienstleistungen, während der quartäre Sektor wissensintensive Tätigkeiten wie Forschung und IT abdeckt.

Mit der Wahl des Klassifikationssystems erfolgte dann die Ermittlung der Indikatoren, die die Einschätzungen zur Relevanz der einzelnen Sektoren für den Data Act ermöglichen. Hierzu waren zwei Sets an Indikatoren bedeutend:

(i) Ökonomische Indikatoren und

(ii) Indikatoren für die Relevanz von datenbezogenen Wertschöpfungsprozessen bzw. Daten im Allgemeinen.

Die Evaluierung der allgemeinen ökonomisch Indikatoren diente dazu, die gesamtwirtschaftliche Bedeutung der Sektoren zu erfassen. Anhaltspunkte für die klassischen wirtschaftlichen Indikatoren lieferten die Datenbanken staatlicher Ämter wie Eurostat oder die Datenbank des deutschen Statistischen Bundesamtes. In diesen Datenbanken werden ökonomische Indikatoren weitestgehend für alle Wirtschaftszweige nach NACE einheitlich erfasst. Als Indikatoren für die allgemeine wirtschaftliche Relevanz wurden die Bruttowertschöpfung, der Nettoumsatz, Forschungs- und Entwicklungsausgaben sowie

59 Folgende Klassifikationssysteme wurden ebenfalls auf ihre Eignung und Kontext untersucht: Global Industry Classification Sector von MSCI, sektorale Gliederung im Rahmen des Common European Data Space, European Monitor of Industrial Ecosystems & European Data Market Study 2024-2026. Diese wurden nicht für die Untersuchung verwendet, da sie keine zum NACE bzw. WZ breit anerkannte Klassifikationsstruktur bieten. Daten werden vermindert nach diesen Klassifikationssystemen erhoben. Dies schränkt die Vergleichbarkeit der Daten ein.

die Anzahl der Erwerbstätigen und Anzahl der Unternehmen herangezogen. Die Anzahl der Unternehmen und der Nettoumsatz geben Aufschluss über die Größe des Sektors und die Marktdynamik. Die Bruttowertschöpfung ist relevant, um den gesamtwirtschaftlichen Stellenwert eines Sektors zu erfassen. Die Anzahl der Erwerbstätigen geben Aufschluss über die sozioökonomische Bedeutung des Sektors. Die Forschungs- und Entwicklungsausgaben dienen als Indikator für die Innovationskraft eines Sektors.

Für die Indikatoren, die die Relevanz von datenbezogenen Wertschöpfungsprozessen innerhalb der Sektoren verdeutlichen, existiert ein Defizit an spezifischen, differenzierten und einheitlich erfassten Daten in amtlichen Statistiken. Daher wurden weitere Quellen wie z. B. die Statista und die Dealroom-Datenbank in die Analyse einbezogen, die Angaben über die datenökonomische Relevanz der Sektoren enthalten. Diese Indikatoren weisen jedoch signifikante Unterschiede in ihrer Erhebungsmethodik, Definition und Granularität auf und sind daher nicht direkt miteinander vergleichbar, geben aber einen umfassenden Überblick über die Relevanz des entsprechenden Sektors im Rahmen des DA.

Für die Bewertung der Relevanz der Sektoren im Hinblick auf datenbezogene Wertschöpfungsprozesse wurden sowohl die Nutzer- als auch Anbieterseite näher betrachtet. Somit wurde in einem ersten Schnitt erfasst, wie intensive vernetzte Produkte und verbundene Dienste in den verschiedenen Sektoren verwendet werden. Die Anwendung von IOT-Geräten und -Diensten innerhalb von Unternehmen und die Anzahl von IOT-Verbindungen innerhalb von Branchensegmenten wurden als Näherungswert hinzugezogen. Diese Daten stammen von Eurostat bzw. Statista.

Im zweiten Schritt wurden die Struktur der Anbieter von vernetzten Geräten und verbundenen Diensten nachvollzogen. Hierzu wurde primär die Dealroom-Datenbank[60] herangezogen. Die Plattform erfasst vor allem Start-ups, Scale-ups und führende Technologieunternehmen, die im Bereich der Datentechnologien tätig sind. Mitte Mai umfasste die Dealroom-Datenbank etwa 3,3 Millionen Unternehmen aus folgenden Märkten: Health, Home living, Hosting, Robotics, Fintech, Wellness Beauty, Travel, Telecom, Food, Real Estate, Semiconductors, Dating, Media, Education, Music, Engineering and Manufacturing Equipment, Marketing, Energy, Event Tech, Space, Fashion, Kids, Jobs Recruitment, Consumer Electronics, Enterprise Software, Sports, Security, Chemicals, Transportation, Gaming, Legal. Die Gesamtheit aller DA-relevanten Unternehmen wird durch diese Datenbank zwar nicht repräsentativ abgebildet, aber aufgrund des Fokus auf innovative (Start-ups und Scale-ups) und führende Technologieunternehmen, kann sie Hinweis darauf geben, in welchen Industrien relevante Unternehmen operieren. Der EU Data Landscape Report 2024[61] nutzte ebenfalls die

60 Die Datenbank „Dealroom.co“ wird von der gleichnamigen Firma Dealroom.co B.V. betrieben – einem privat geführten Unternehmen mit Sitz in Amsterdam, Niederlande. Die Datenbank umfassende Daten zu Start-ups, Scale-ups und führende Technologieunternehmen weltweit. Die Daten werden aus einer Kombination an öffentlich zugänglichen Quellen, maschinelles Lernen, direkten Partnerschaften mit Unternehmen, Investoren und Regierungen erfasst. (vgl. https://dealroom.co/).

61 EU-Kommission (2024e). The European Data Market Study 2024-2026 – EU Data Landscape report. Studie erstellt durch IDC, CARSA, The Lisbon Council. https://digital-strategy.ec.europa.eu/en/library/european-data-market-study-2024-2026.

Dealroom-Datenbank, um festzustellen, in welchen Branchen die wichtigsten Datenunternehmen in Europa tätig sind. Im Rahmen dieser Studie wurde der Fokus insbesondere auf operative Unternehmen gelegt, die Dealroom im Zusammenhang mit „IoT“ und „Connected Devices“ aufführt (Filter: „Technologies“). Zudem wurde nach Unternehmen mit Sitz in Deutschland oder Europa gefiltert. Da die Datenbank eine von den NACE-Codes abweichende Gliederung von Märkten vornimmt, wurden diese nachtäglich und wenn möglich in die gewählte Klassifikation überführt.

Eine zweite Quelle für die Herleitung der Anbieterstruktur war die WIK-Datenbank zum Mittelstand in Deutschland. Die Datenbank umfasst eine Sammlung von insgesamt 266 Digitalprojekten von kleinen und mittleren Unternehmen in Deutschland. Für die Aufnahme in die Datenbank mussten die Projekte mehrere Kriterien erfüllen. (1) KMU ist als Anwender involviert / die Anwendung ist auf KMU ausgerichtet; (2) die Anwendung ist marktreif; (3) die Anwendung enthält digitale Lösungen und/oder digitale Technologien; und (4) es liegen gut nachvollziehbarer Informationen für die Anwendung vor. Für diese Studie wurde die Verteilung von Projekten nach NACE Sektoren betrachtet, die in Verbindung mit folgenden Schlagwörtern in der Datenbank in erfasst wurden: vernetzte Geräte, vernetzte Maschinen, vernetzte Produktion, IoT, LoRaWAN, Sensoren und intelligente Sensorik. Das Ergebnis sind 124 Projekte.

In den nachfolgenden Ausführungen werden die Ergebnisse des soeben skizzierten Vorgehens dargestellt, anhand dessen die besonders relevanten Sektoren für den DA identifiziert wurden. Die Auswahl der Sektoren basierte auf der kombinierten Betrachtung der verschiedenen Datenquellen. Damit ein Sektor als relevant für den DA eingestuft werden konnte, mussten sowohl ausreichend belastbare wirtschaftliche als auch datenbezogene Indikatoren vorliegen.

6.2 Ergebnisse der Sektoruntersuchung

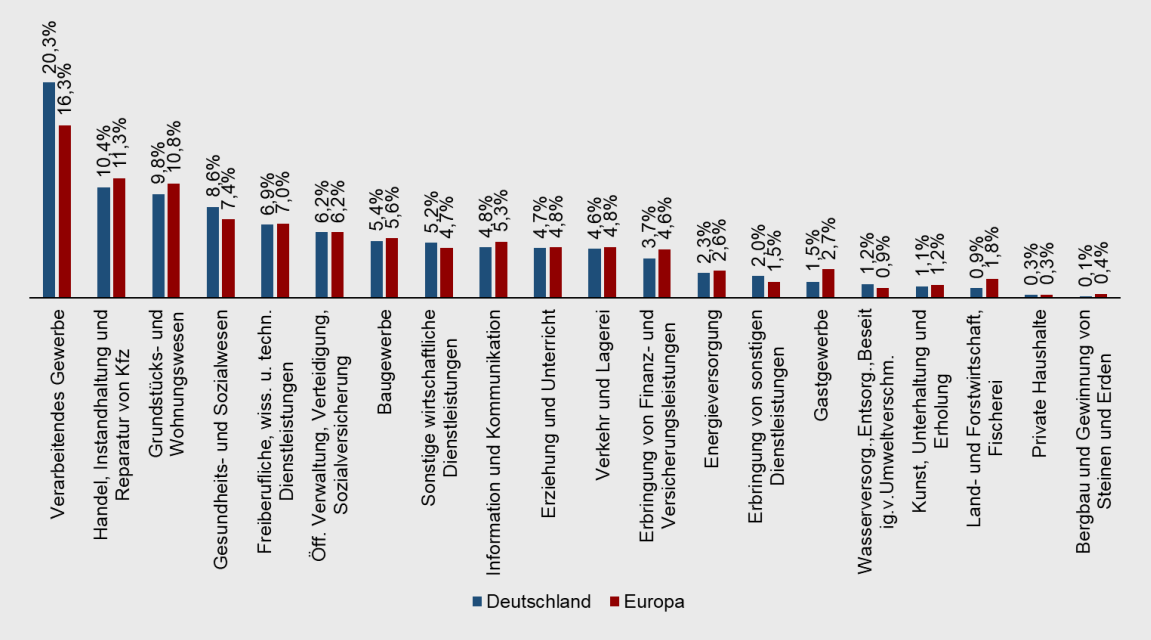
In diesem Kapitel werden die Ergebnisse der Sektoruntersuchung zusammengefasst. Wie im vorherigen Kapitel beschrieben, wird zunächst die Relevanz der Sektoren basierend auf ökonomischen Indikatoren bewertet. Im Anschluss wird der Fokus auf die datenbezogenen Wertschöpfungsprozesse gelegt. Abschließend werden die Ergebnisse zusammengefasst und die relevanten Sektoren abgeleitet.

6.2.1 Die ökonomische Relevanz von Sektoren

Die Ableitung ökonomisch relevanter Sektoren erfolgt anhand einer Auswahl von fünf Indikatoren. In Deutschland sowie im europäischen Kontext tragen die Sektoren „verarbeitendes Gewerbe“, „Handel; Instandhaltung, Reparatur von Kfz“, „Grundstücks- und Wohnungsbauwesen“ sowie „Gesundheits- und Sozialwesen“ die größten Beiträge zur Bruttowertschöpfung bei (vgl. Abbildung 13:). Die Sektoren „freiberufliche, wissenschaftliche und technische Dienstleistungen“, „öffentliche Verwaltung, Verteidigung, Sozialversicherung“, „Baugewerbe“, „sonstige wirtschaftliche Dienstleistungen“, sowie

„Information und Kommunikation“ tragen jeweils mindestens noch ca. 5 % zur Bruttowertschöpfung bei.

Abbildung 13: Bruttowertschöpfung Verteilung in Deutschland & Europa, 2023



Quelle: Eigene Darstellung basierend auf Daten des Statistisches Bundesamt (Destatis) „VGR des Bundes – Bruttowertschöpfung (nominal/ preisbereinigt): Deutschland, Jahre, Wirtschaftsbereiche“, Code: 81000-0102 (https://www-genesis.destatis.de/datenbank/online/statistic/81000/table/81000-0102/) & Daten von Eurostat „Bruttowertschöpfung und Einkommen nach detaillierten Wirtschaftsbereichen (NACE Rev. 2)“, Code: nama_10_a64 (https://ec.europa.eu/eurostat/databrowser/view/nama_10_a64__custom_14919422/default/table). Anmerkung: Keine Eintragung für den Sektor „exterritoriale Organisationen und Körperschaften“.

Diese insgesamt neun Sektoren erreichen in der Regel auch bei den anderen Indikatoren hohe Ränge. In Deutschland sind z. B. viele **Arbeitnehmer bzw. Erwerbstätige** im „verarbeitenden Gewerbe“ (17 % bzw. 16 %), „Gesundheits- und Sozialwesen“ (14 %) sowie „Handel; Instandhaltung und Reparatur von Kfz“ (13 %) beschäftigt.[62] Diese Sektoren bilden damit die wichtigsten Beschäftigungsbereiche.[63]

Neben diesen drei Sektoren spielen auch das „Baugewerbe“ (11 %) und „freiberufliche, wissenschaftliche und technische Dienstleistungen“ (14 %) hinsichtlich der absoluten **Anzahl an Unternehmen** in Deutschland eine besondere Rolle. Der Sektor „Handel;

62 Vgl. Statistisches Bundesamt (Destatis) „VGR des Bundes - Erwerbstätige: Deutschland, Jahre, Wirtschaftsbereiche“, Code: 81000-0123 (https://www-genesis.destatis.de/datenbank/online/statistic/81000/table/81000-0123); Statistisches Bundesamt (Destatis) „VGR des Bundes - Arbeitnehmer: Deutschland, Jahre, Wirtschaftsbereiche“, Code: 81000-0124. (https://www-genesis.destatis.de/datenbank/online/statistic/81000/table/81000-0124).

63 Vgl. Statistisches Bundesamt (Destatis) „Sozialversicherungspflichtig Beschäftigte am Arbeitsort: Deutschland, Stichtag, Geschlecht, Wirtschaftsabschnitte“, Code: 13111-0003 (https://www-genesis.destatis.de/datenbank/online/table/13111-0003/search/s/MTMxMTEtMDAwMw==).

Instandhaltung und Reparatur von Kfz“ nimmt mit einem Anteil von ca. 17 % dabei einen Spitzenwert ein.[64]

Einen hohen **Nettoumsatz** verzeichnen in Deutschland insbesondere das „verarbeitende Gewerbe“ (2,92 Mio. Euro), „Handel; Instandhaltung und Reparatur von Kfz“ (2,62 Mio. Euro) sowie die „Energieversorgung“ (1,24 Mio. Euro).[65] Im verarbeitenden Gewerbe tragen insbesondere die Herstellung von Kraftwagen und Kraftwagenteilen sowie der Maschinenbau zum Umsatz bei.[66] Der Sektor „Verkehr und Lagerei“ bildet dabei eine wichtige Inputgröße für die inländische Produktion und Importe im Sektor „Handel; Instandhaltung und Reparatur von Kfz“.[67]

Insbesondere investieren Unternehmen des verarbeitenden Gewerbes (83 %) aus dem Sektor „freiberufliche, wissenschaftliche und technische Dienstleistungen“ (8 %) sowie des Informations- und Kommunikationssektor (7 %) in **Forschung und Entwicklung**.[68] Die Werte beziehen sich auf den Anteil der Ausgaben für Forschung und Entwicklung im Unternehmenssektor an den gesamten F&E-Ausgaben über alle Wirtschaftssektoren. Laut Rammer et al. (2024) investieren besonders viele Unternehmen aus der Chemie- und Pharmaindustrie (57 %), Elektroindustrie (48 %), Maschinenbau (42 %), dem Fahrzeugbau (37 %) sowie dem Informations- und Kommunikationssektor (35 %) kontinuierlich in Forschung und Entwicklung. Diese Branchen haben zudem besonders hohe Innovationsausgaben. Auch in Bezug auf die Innovationsintensität nehmen der Fahrzeugbau und die Elektroindustrie Spitzenwerte ein.[69]

Die Übersicht in Abbildung 14 ergibt sich durch die Bildung einer Rangfolge der einzelnen Sektoren für die jeweiligen Indikatoren. Die Farbgebung des markierten Feldes spiegelt die Hierarchie der Sektoren für den jeweiligen Indikator wider. Eine höhere Einordnung des Sektors geht mit einer dunkleren Markierung des Feldes einher. Es lässt sich feststellen, dass dadurch insbesondere die Sektoren „verarbeitendes Gewerbe“ und „Handel; Instandhaltung und Reparatur von KfZ“ in führenden Positionen verortet werden können.

---

64 Vgl. Statistisches Bundesamt (Destatis) „Unternehmen (EU) (Unternehmensregister-System): Deutschland, Jahre, Wirtschaftszweige (Abschnitte), Beschäftigtengrößenklassen", Code: 52111-0001(https://www-genesis.destatis.de/datenbank/online/table/52111-0001/search/s/NTIxMTEtMDAwMQ==).

65 Vgl. Eurostat „Unternehmensstatistiken nach Größenklassen und Wirtschaftszweigen der NACE Rev. 2 (ab 2021)“, Code: sbs_sc_ovw (https://ec.europa.eu/eurostat/databrowser/view/sbs_sc_ovw__custom_16349184/default/table?lang=en&page=time:2023).

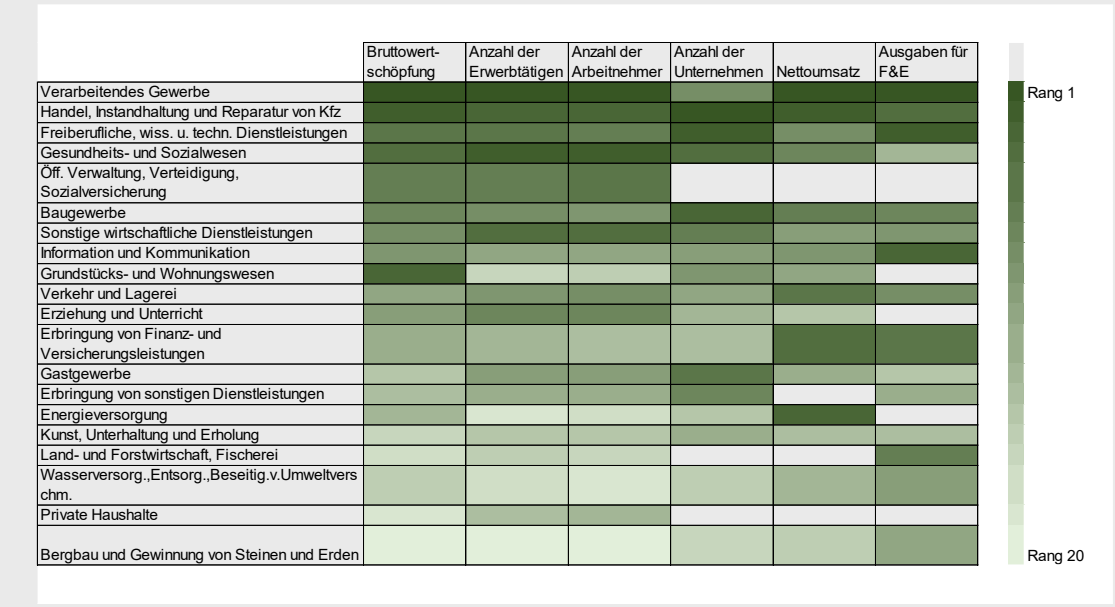
66 Vgl. Statista (2025a).

67 Vgl. Statistisches Bundesamt (Destatis) (2025).

68 Vgl. Eurostat „Bruttoausgaben für FuE im Unternehmenssektor nach NACE Rev. 2 Tätigkeit“, Code: rd_e_berdindr2 (https://ec.europa.eu/eurostat/databrowser/view/rd_e_berdindr2/default/table?lang=de).

69 Vgl. Rammer et al. (2024).

Abbildung 14: Rangordnung der Sektoren in Bezug auf die jeweiligen Indikatoren



Quelle: Eigene Darstellung basierend auf den Daten des Statistisches Bundesamt (Destatis) und Eurostat, siehe Quellen in Abbildung 13 sowie Fußnoten 62, 64, 65, 68. Anmerkung: Keine Eintragungen für den Sektor „exterritoriale Organisationen und Körperschaften“. Für die freistehenden Felder waren keine Daten vorhanden.

Gemäß dem durchschnittlichen Rang für die jeweils verfügbaren Indikatoren, ergeben sich folgende 10 Sektoren, die sich in besonderer Weise für ökonomische Relevanz auszeichnen:

- Verarbeitendes Gewerbe
- Handel, Instandhaltung und Reparatur von Kfz
- Grundstücks- und Wohnungswesen
- Gesundheits- und Sozialwesen
- Freiberufliche, wiss. u. techn. Dienstleistungen
- Öff. Verwaltung, Verteidigung, Sozialversicherung
- Baugewerbe
- Sonstige wirtschaftliche Dienstleistungen
- Information und Kommunikation
- Verkehr und Lagerei

Der Rang der Bruttowertschöpfung als zentraler Indikator für den ökonomischen Erfolg eines Sektors und seiner Akteure fließt stärker gewichtet in die Bewertung ein.

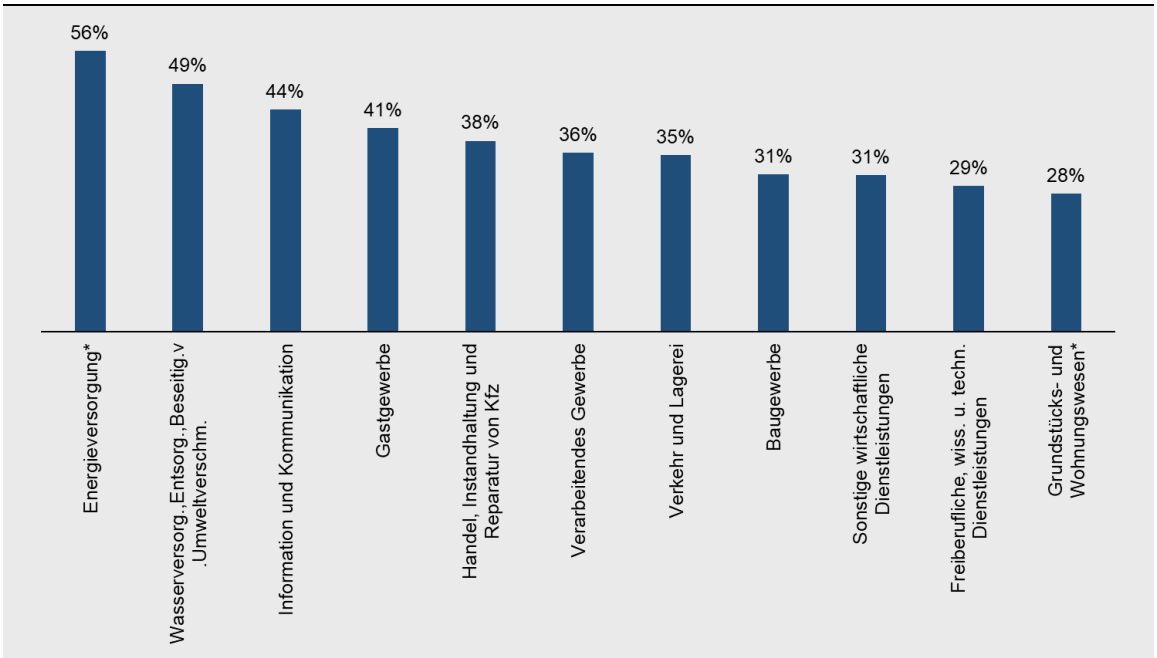
6.2.2 Die Relevanz von datenbezogenen Wertschöpfungsprozessen in den Sektoren

Die Bedeutung datenbezogener Wertschöpfungsprozesse in den Sektoren wird, wie in Kapitel 6.1 beschrieben, im Wesentlichen aus vier Datenquellen hergeleitet. Um ein umfassendes Bild der datenbezogenen Wertschöpfungsprozesse zu erhalten, werden sowohl die Nutzer- als auch die Anbieterseite betrachtet.

Nutzung von vernetzten Produkten und verbundenen Diensten

Um einen Überblick über die Nutzung von vernetzten Produkten und verbundenen Diensten innerhalb der EU zu erhalten, ist die von Eurostat bereitgestellte Statistik zum Anteil der Unternehmen, die IoT nutzen, einschlägig.[70] An diesen Daten wird deutlich, das insbesondere Unternehmen der Sektoren „Energieversorgung", „Wasserversorgung, Entsorgung, Beseitigung von Umweltverschmutzung" und „Information und Kommunikation" zu einem hohen Anteil IoT nutzen – definiert als vernetzte Geräte oder Systeme, die über das Internet überwacht oder gesteuert werden können. Etwa durchschnittlich viele Unternehmen, die IoT nutzen, finden sich zudem in den Sektoren „Gastgewerbe" und „Handel, Instandhaltung und Reparatur von Kfz".

Abbildung 15: Anteil der Unternehmen in Deutschland, die IoT nutzen, 2021

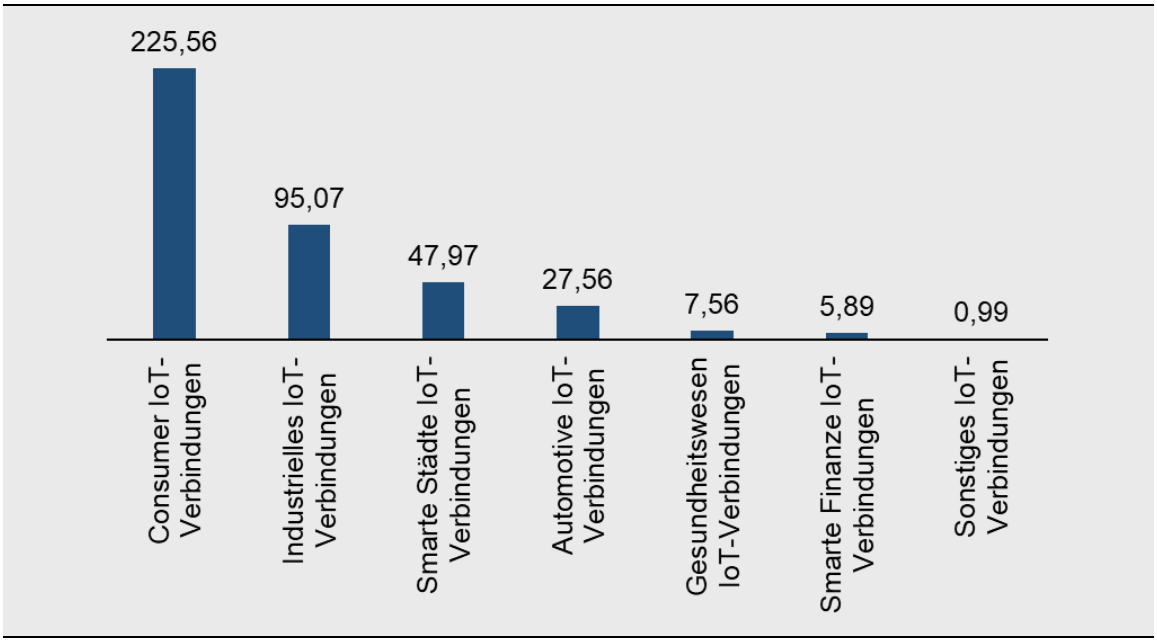


Quelle: Eigene Darstellung basierend auf Daten von Eurostat „Internet of Things by NACE Rev.2 activity", Code: isoc_eb_iotn2 (https://ec.europa.eu/eurostat/databrowser/view/isoc_eb_iotn2__custom_14755252/default/table?lang=en). Vermerk: Für die Sektoren, die nicht aufgelistet sind, sind keine Daten vorhanden. *Schätzungen basiert auf eigenen Berechnungen.

70 Eurostat „Internet of Things by NACE Rev.2 activity", Code: isoc_eb_iotn2 (https://ec.europa.eu/eurostat/databrowser/view/isoc_eb_iotn2__custom_14755252/default/table?lang=en).

Des Weiteren weist Statista auch eine Statistik zur Anzahl der IoT-Verbindungen in ausgewählten Segmenten aus. Diese wird als die Gesamtzahl der Geräte, die mit den IoT-Technologien (sowohl Wide-Area als auch Short-Range IoT) definiert. Diese gibt Hinweise auf die Nutzung von IoT in verschiedenen Bereichen. Nach dieser Statistik heben sich insbesondere die Segmente Consumer IoT (d. h., IoT, die vom Endverbraucher verwendet werden)[71], Industrial IoT (d. h., IoT, die zur Steuerung und Optimierung der Maschinenumgebung in Fabriken, Lagern, Transportsystemen etc. genutzt werden)[72] sowie IoT im Bereich Smarte Städte (d. h., IoT, mit denen die Lebensqualität der Bürger verbessert und städtische Dienstleitungen optimiert werden)[73] hervor.

Abbildung 16: Anzahl der IoT-Verbindungen in Deutschland, 2024



Quelle: Eigene Darstellung basierend auf Daten von Statista (2024c). Vermerk: Die Anzahl der IoT-Verbindungen gibt die Gesamtzahl der Geräte, die mit den IoT-Technologien (sowohl Wide-Area als auch Short-Range IoT) in Deutschland im Jahr 2024 verbunden waren, wieder.

Gemäß den von Statista veröffentlichten Daten wird der höchste Umsatz im Jahr 2024 in Deutschland mit 7,6 Milliarden Euro jedoch im Bereich Automotive IoT erzielt. Es folgt der Bereich Industrial IoT mit einem geschätzten Umsatz von 7,09 Milliarden Euro, gefolgt von Consumer IoT mit 6,27 Milliarden Euro, Smart Cities mit 3,33 Milliarden Euro, IoT im Gesundheitswesen mit 2,59 Milliarden Euro, Smart Finance mit 2,5 Milliarden Euro und schließlich Sonstiges IoT mit 0,33 Milliarden Euro.[74]

71 Vgl. Statista (2024e).
72 Vgl. Statista (2024n).
73 Statista (2024o).
74 Statista (2024b).

Anbieter von vernetzten Produkten und verbundenen Diensten

Wie in Kapitel 6.1 beschrieben, werden die Anbieterstrukturen in den Sektoren insbesondere aus der Datenanalyse der Dealroom-Datenbank und der WIK-Datenbank zum Mittelstand in Deutschland hergeleitet. Die folgende zwei Tabellen zeigen die Anzahl der in der Dealroom-Datenbank identifizierten Unternehmen, untergliedert nach Märkten. Betrachtet werden ausschließlich operative Unternehmen mit Sitz in Deutschland oder Europa, die Dealroom im Zusammenhang mit den Technologien „IoT“ und „Connected Devices“ aufführt.

Tabelle 2: Dealroom-Datenbank – Top 15 Branchen/Märkte in der EU, 2024

Branche	Anzahl der in der Datenbank identifizierten Unternehmen	Prozent der in der Datenbank identifizierten Unternehmen
Softwareunternehmen	1057	17,6%
Gesundheit	667	11,1%
Energie	650	10,8%
Transport	566	9,4%
Robotik	517	8,6%
Sicherheit	401	6,7%
Halbleiter	358	6,0%
Telekommunikation	345	5,8%
Home living	308	5,1%
Lebensmittel	286	4,8%
Fintech	259	4,3%
Immobilien	248	4,1%
Marketing	213	3,6%
Medien	172	2,9%
Sport	168	2,8%

Quelle: Dealroom-Database (https://dealroom.co/). Anmerkung: Doppelzählungen möglich.

Tabelle 3: Dealroom-Datenbank –Top 15 Branchen/Märkte in Deutschland, 2024

Branche	Anzahl der in der Datenbank identifizierten Unternehmen	Prozent der in der Datenbank identifizierten Unternehmen
Unternehmenssoftware	175	21,1%
Transport	97	11,7%
Gesundheit	80	9,7%
Energie	80	9,7%
Robotik	75	9,0%
Sicherheit	52	6,3%
Halbleiter	49	5,9%
Fintech	48	5,8%
Home living	47	5,7%
Telekommunikation	46	5,5%

Branche	Anzahl der in der Datenbank identifizierten Unternehmen	Prozent der in der Datenbank identifizierten Unternehmen
Immobilien	26	3,1%
Medien	25	3,0%
Lebensmittel	23	2,8%
Marketing	19	2,3%
Sport	16	1,9%

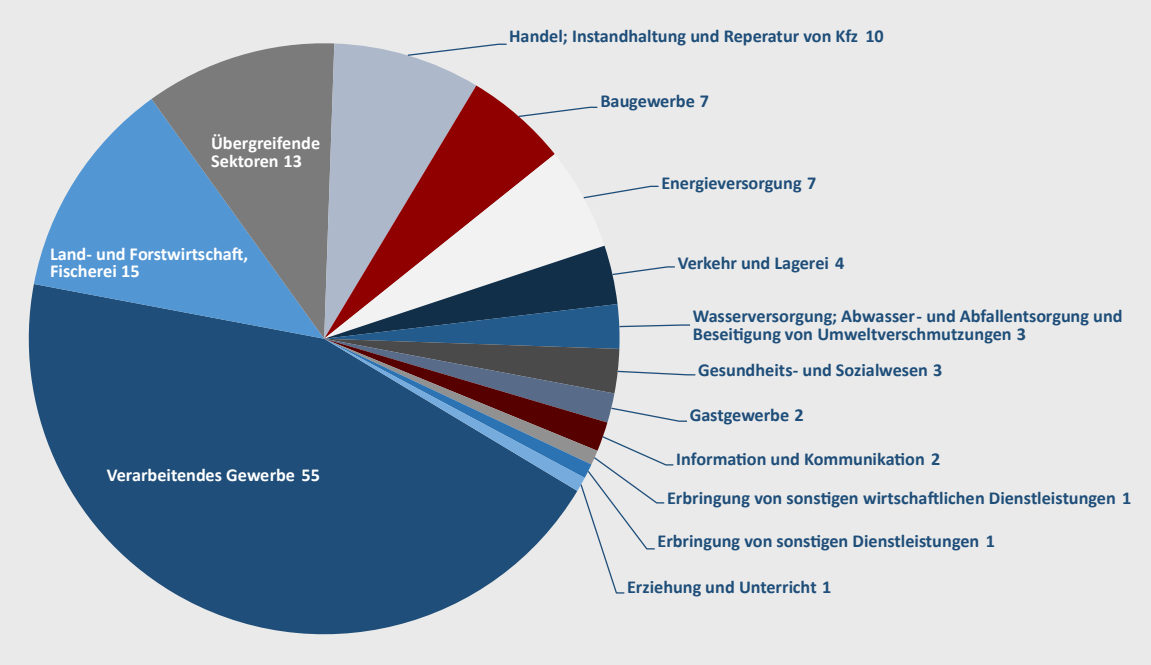
Quelle: Dealroom-Database (https://dealroom.co/). Anmerkung: Doppelzählungen möglich.

Das Ergebnis deutet darauf hin, dass hinsichtlich der Anzahl an Unternehmen, die im Bezug zu IoT und vernetzten Geräten stehen, insbesondere die Software- sowie Gesundheit-, Energie- und Transport-Branche zu den wichtigsten in der EU gehören. In der äquivalenten Darstellung für Deutschland wird ebenfalls deutlich, dass die Unternehmenssoftware-, Transport-, Gesundheits- und Energiebranche zu den wichtigsten Bereichen gehören, wobei allerdings zum Teil die Reihenfolge der Branchen von der auf EU-Ebene abweicht.

Der zweite Indikator „Anzahl von Anwendungen nach Sektoren“ stammt aus der WIK-Datenbank zum Mittelstand in Deutschland. Die Datenbank enthält insgesamt 266 Digitalprojekten, inklusive 124 IoT-Projekte, von kleinen und mittleren Unternehmen in Deutschland.[75] Die folgende Abbildung zeigt die sektorale Verteilung der IoT-Anwendungsbeispiele. Hierbei tritt das verarbeitende Gewerbe als dominierender Sektor klar hervor, gefolgt von der Land- und Forstwirtschaft sowie Fischerei.

75 Die Auswahl der IoT-Projekte erfolgte auf Grundlage einschlägiger Schlagwörter wie „vernetzte Geräte“, „vernetzte Maschinen“, „vernetzte Produktion“, „IoT“, „LoRaWAN“, „Sensoren“ und „intelligente Sensorik“.

Abbildung 17: Datenbank Praxisbeispiele@Mittelstand – Verteilung der IoT-Projekte nach Sektoren



Quelle: WIK Recherche im Rahmen der Datenbank Praxisbeispiele@Mittelstand.

Im Gegensatz zu den Daten zu den ökonomischen Indikatoren bedienen sich die Datenquellen bei der Betrachtung der Sektoren bzw. Märkten gänzlich unterschiedlicher Klassifikationen. Die angewandte Systematik zur Ermittlung der ökonomischen Relevanz erweist sich in diesem Fall als nicht anwendbar. Indikatoren zu datenökonomischen Relevanz, die nicht nach NACE vorliegen, wurden daher zunächst in diese Klassifikation überführt. In der Folge wurde insbesondere die kumulierte Anzahl der Nennungen in den drei bzw. fünf führenden Positionen je Indikator als Indiz für die Relevanzfeststellung herangezogen. Somit ergibt sich die in der folgende Tabelle dargestellten Auswahl der Sektoren.

Tabelle 4: Auswahl der DA-relevanten Sektoren

Ökonomische Indikatoren	Indikatoren bezüglich der datenbezogenen Wertschöpfungsprozesse				Finale Auswahl der relevanten Sektoren
	Anbieterseitige Indikatoren aus folgenden Quellen:		Nutzerseitige Indikatoren aus folgenden Quellen:		
	Dealroom[1]	Datenbank Praxisbeispiele@ Mittelstand[2]	Eurostat[3]	Statista[4]	
Verarbeitendes Gewerbe	Verarbeitendes Gewerbe (Robotik)	Verarbeitendes Gewerbe	Verarbeitendes Gewerbe	Verarbeitendes Gewerbe (Industrielles IoT)	✓
Handel, Instandhaltung und Reparatur von Kfz		Handel, Instandhaltung und Reparatur von Kfz	Handel, Instandhaltung und Reparatur von Kfz		✓
Freiberufliche, wiss. u. techn. Dienstleistungen					✗
Gesundheits- und Sozialwesen	Gesundheits- und Sozialwesen (Gesundheit)				✓
Öff. Verwaltung, Verteidigung, Sozialversicherung				Öff. Verwaltung, Verteidigung, Sozialversiche-rung (Smart City)	✓
Baugewerbe					✗
Sonstige wirtschaftliche Dienstleistungen					✗
Information und Kommunikation	Information und Kommunikation (Softwareunterneh men)		Information und Kommunikation	Information und Kommunikation (Consumer IoT)	✓
Grundstücks- und Wohnungswesen					✗
Verkehr und Lagerei	Verkehr und Lagerei (Transport)				✓
	Energieversorgung (Energie)		Energieversorgung		✓
		Land- und Forstwirtschaft, Fischerei			✓
			Wasserversorg., Entsorg.,Beseitig.v .Umweltverschm.		✗
			Gastgewerbe		✗

Quelle: Eigene Darstellung. [1]Die gelisteten Sektoren umfassen diejenigen Top-Branchen, in denen die Unternehmen mindestens ca. 60 % aller identifizierten Unternehmen repräsentieren. [2]Die gelisteten Sektoren sind diejenigen, auf die mindestens ca. 60 % der identifizierten IoT-Projekte entfallen.[3]Die gelisteten Sektoren sind diejenigen, in denen mindestens 36 % der Unternehmen IoT nutzen. Dies ist der geschätzte deutschlandweite Durchschnitt laut dem Statistischen Bundesamt (2022).[4]Die gelisteten Sektoren umfassen diejenigen Top-Segmente, auf die etwa 90 % aller von Statista ausgewiesenen IoT-Verbindungen entfallen.

Bei der Auswahlentscheidung und damit der Gesamtbewertung der Wichtigkeit eines Sektors für den DA war der Beleg der ökonomisch Relevanz alleine nicht ausreichend. Es musste zudem die datenökonomische Relevanz belegt werden können. So reichte es bei Sektoren, bei denen die ökonomische Relevanz belegt wurde, wenn lediglich eine der anderen Quellen die datenökonomische Bedeutung des Sektors belegte. Fehlte die

deutliche ökonomische Bedeutung, musste die datenökonomische Relevanz durch mindestens zwei weitere Quellen belegt sein. Dabei wurden anbieterseitige Indikatoren aufgrund der Ausrichtung der Studie doppelt gewertet. Sofern die datenökonomische Relevanz eines Sektors nachgewiesen werden konnte, war das Vorhandensein einer allgemeinen wirtschaftlichen Relevanz nicht mehr zwingend erforderlich, sie, stärkte jedoch die Auswahlentscheidung. So wurde darauf abgezielt, die Exklusion von Sektoren, die volkswirtschaftlich als weniger relevant einzustufen sind, für die Daten jedoch essenziell in der Wortschöpfung sind, zu vermeiden.

Zusammenfassend bedeutet dies, Sektoren wurden nur dann als relevant eingestuft, wenn sowohl ausreichend belastbare ökonomische und/oder datenbezogene Wertschöpfungsinformationen vorlagen. Das bedeutet aber nicht, dass die anderen Sektoren per se nicht relevant sind. So lag z. B. für die Sektoren „Wasserversorgung, Entsorgung, Beseitigung von Umweltverschmutzung“ und „Gastgewerbe“ gemessen an dem definierten Bewertungsschema nicht genügend Evidenz vor. Ähnlich verzeichnet der Smart-Finance-Sektor zwar eine steigende Anzahl an IoT-Verbindungen und erzielte rund 2,5 Mrd. Euro im Jahr 2024, seine durchschnittliche jährliche Wachstumsrate ist aber seit 2019 stark fallend.[76] Auch hinsichtlich der Verteilung der Bruttowertschöpfung in Deutschland nach Sektoren rangiert der Finanzsektor nur im unteren Mittelfeld, sodass dieser Sektor hier nicht als einer der relevantesten Sektoren eingestuft wurde. Mehrere Studien betonen zudem die Bedeutung von IoT im Bausektor bzw. dessen Potenzial, allerdings sind belastbare quantitative Kennzahlen, die eine Einschätzung der sektoralen Relevanz für Deutschland ermöglichen, bislang nicht verfügbar.[77]

Dadurch ergibt sich die erste Ableitung folgender relevanter Sektoren:

- Verarbeitendes Gewerbe
- Information und Kommunikation
- Handel, Instandhaltung und Reparatur von Kfz
- Gesundheits- und Sozialwesen
- Öffentlicher Sektor (Smart City)
- Verkehr und Lagerei
- Energie(-versorgung)
- Land- und Forstwirtschaft, Fischerei

Im Rahmen der Sektoruntersuchung stechen die beiden Sektoren „Verarbeitendes Gewerbe“ und „Informationen und Kommunikation“ besonders heraus. Während das verarbeitende Gewerbe ökonomisch besonders wichtig ist, befinden sich nach den betrachteten Dealroom-Daten die meisten Anbieter im Informations- und Kommunikationssektor. Um der speziellen Bedeutung dieser beiden Sektoren gerecht zu

76 Vgl. Statista (2024).
77 Vgl. DIGI (2024).sowie Mittelstand-Digital Zentrum Bau (2021) und Human, S. (2019).

werden, werden diese weiter untergliedert. Dabei orientiert sich die Untergliederung an der von Statista vorgenommenen Abgrenzung von Automotive-, Industrial- und Consumer-IoT. Das Ergebnis ist damit 11 (Unter-)Sektoren.

Tabelle 5: Vom Data Act besonders stark betroffene Branchen

Industrielles IoT **Automotive IoT** **Sonstiges verarbeitende Gewerbe**	Verarbeitendes Gewerbe
Consumer IoT **Sonstiger IKT-Sektor**	Information und Kommunikation
Smart City	Öffentlicher Sektor
Energie(-versorgung)	
Gesundheits- und Sozialwesen	
Verkehr und Lagerei	
Handel; Instandhaltung und Reparatur von Kfz	
Landwirtschaft, Forstwirtschaft und Fischerei	

Quelle: Eigene Darstellung.

In dem nächsten Schritt werden diese Sektoren einer weiteren detaillierten Betrachtung unterzogen.

6.2.3 Detaillierter Einblick in die ausgewählten Sektoren

Für die ausgewählten Sektoren wurde eine techno-ökonomische tiefere Untersuchung vorgenommen. Die Ergebnisse zeigen Branchen, die anhand ihre Nutzung von IoT und anderen für den DA relevanten Anwendungen besonders relevant sind.

Studien bestätigen die herausragende Bedeutung von IoT-Technologie in der Produktion bzw. im **verarbeitenden Gewerbe**.[78]

- 35,7 % der Unternehmen im verarbeitenden Gewerbe in Deutschland nutzen IoT, also vernetzte Geräte oder Systeme, die über das Internet überwacht oder gesteuert werden können.[79]
- Im verarbeitenden Gewerbe nehmen insbesondere das Automotive IoT und das Industrielle IoT eine herausragende Rolle ein und es wird erwartet, dass ihr Umsatzwachstum auch in absehbarer Zukunft anhalten wird.[80] Im Jahr 2024 erzielte das Automotive IoT in Deutschland einen Umsatz von 7,6 Mrd. Euro (Platz 1 im Bereich des Internets der Dinge), gefolgt vom Industriellen IoT mit 7,09 Mrd. Euro (Platz 2 im Bereich des Internets der Dinge). Zusammen machen

78 Vgl. Gries/Tenbrock (2023).
79 Vgl. Eurostat „Internet der Dinge, nach Aktivitäten der NACE Rev.2“, Code: isoc_eb_iotn2 (https://ec.europa.eu/eurostat/databrowser/view/isoc_eb_iotn2__custom_14755252/default/table?lang=en).
80 Vgl. Caburn Telecom (2024).

diese beiden Sektoren rund die Hälfte des gesamten Umsatzes im IoT-Markt aus.[81]

- In Bezug auf die absolute Anzahl an IoT-Verbindungen[82] belegt das industrielle IoT mit 95,07 Mio. Verbindungen im Jahr 2024 den zweiten Platz. Im Vergleich dazu ist die Anzahl der Automotive-IoT-Verbindungen mit 27,56 Mio. deutlich niedriger.[83]

Auch der Bereich **Information und Kommunikation (IKT)** ist durch IoT-Anwendungen geprägt:

- Dieses Segment weist einen Spitzenwert auf: 44,3 % der Unternehmen nutzen hier IoT.[84]
- Der Umsatz im **Consumer-IoT-Markt**[85] lag 2024 bei 6,27 Mio. Euro und soll bis 2029 auf 9,58 Mio. Euro steigen, was einem jährlichen Wachstum von durchschnittlich 8,85 % entspricht.
    - Die Anzahl der IoT-Verbindungen wird von 2024 bis 2028 von 225,56 Mio. auf voraussichtlich 438,73 Mio. anwachsen, mit einer durchschnittlichen jährlichen Steigerung von 18,10 %.[86]
    - Als Teilbereich des Consumer-IoT-Marktes ist der Smart-Home-Markt stark vertreten. Laut Statista wird der Umsatz im deutschen Smart-Home-Markt im Jahr 2025 8,8 Mrd. Euro umfassen.[87]
    - Innerhalb dieses Marktes machen smarte Haushaltsgeräte mit einem Umsatz von 3,0 Mrd. Euro den größten Anteil aus. Insbesondere die intelligente Vernetzung und Steuerung von Smart-Home-Produkten verzeichnet einen wachsenden Trend. Laut Prognosen wird der Marktwert bis 2029 weiter auf 12,0 Mrd. Euro steigen und damit ein erwartetes durchschnittliches jährliches Umsatzwachstum von 8,06 % erzielen.[88]
    - Prognosen hinsichtlich der Anzahl der Smart-Home-Haushalte in Deutschland zeigen einen kontinuierlichen Anstieg. Es wird erwartet, dass

---

81 Vgl. Statista (2024b). Die Definition von IoT von Statista umfasst keine Smartphones, Laptops, Tablets, PCs und sonstige Geräte, die ausschließlich für den Internetzugang bestimmt sind.
82 Die Anzahl an IoT-Verbindung ist definiert als die Gesamtzahl der Geräte, die in einem bestimmten Jahr über IoT-Technologien (sowohl Wide-Area IoT als auch Short-Range IoT) mit einem Netzwerk verbunden sind.
83 Vgl. Statista (2024c).
84 Vgl. Eurostat „Internet der Dinge, nach Aktivitäten der NACE Rev.2“, Code: isoc_eb_iotn2 (https://ec.europa.eu/eurostat/databrowser/view/isoc_eb_iotn2__custom_14755252/default/table?lang=en).
85 Consumer IoT ist aufgrund seiner Dominanz von digitalen Diensten primär der Branche Information und Kommunikation zugeordnet. Das verarbeitende Gewerbe spielt eine unterstützende Rolle durch die Bereitstellung von Hardware, ist jedoch nicht der Haupttreiber der Wertschöpfung in diesem Sektor. Vgl. eco – Verband der Internetwirtschaft e. V./Arthur D. Little GmbH (2020).
86 Vgl. Statista (2024a); Statista (2024b).
87 Der Consumer-IoT-Markt umfasst den Smart-Home-Markt. Während sich der Umsatz des Consumer IoT aus dem Verkauf von IoT-Komponenten ergibt, basiert der Umsatz im Smart-Home-Markt auf den verkauften Endprodukten.
88 Vgl. Statista (2024d).

die deutschen Smart-Home-Haushalte zwischen 2024 und 2028 stetig um insgesamt 20,2 Mio. Nutzende (+104,12 %) zunehmen, sodass 2028 ein Höchstwert von 39,61 Mio. Smart-Home-Haushalten erreicht wird.[89]

Der Digitalisierungsindex des Bundesministerium für Wirtschaft und Klimaschutz (BMWK) (2023) unterstreicht, dass der IKT-Sektor sowie das sonstige verarbeitende Gewerbe besonders digital vernetzt sind. Von den Unternehmen im IKT-Sektor haben 30 % ihre Unternehmensprozesse mit externen Unternehmenspartnern oder im Marktumfeld digital vernetzt oder nehmen in einem digitalen Netzwerk eine koordinierende Funktion ein. Im sonstigem verarbeitenden Gewerbe sind es fast so viele mit 21,5 % der Unternehmen.[90] Auch hinsichtlich der Innovationslandschaft, IT-Qualifizierung und Forschungs- und Innovationsaktivitäten nehmen der IKT-Sektor und die Elektrotechnik, Maschinen- und Fahrzeugbau als Teil des verarbeitenden Gewerbes laut BMWK die höchsten Ränge ein.[91]

Im **öffentlichen Sektor bzw. in der öffentlichen Verwaltung**, insbesondere bei der Entwicklung smarter Städte und Regionen, gewinnen IoT-Lösungen zunehmend an Bedeutung.[92]

- Im Jahr 2024 wurde im deutschen ***Smart-City-Markt*** ein Umsatz von 3,33 Mrd. Euro erzielt.[93] Prognosen zufolge wird der Umsatz von IoT-Anwendungen im Bereich Smart Cities im Zeitraum von 2024 bis 2029 voraussichtlich mit einer durchschnittlichen jährlichen Wachstumsrate von 10,3 % weiter ansteigen.[94]
- Laut Statista wird die Anzahl der IoT-Verbindungen in smarten Städten zwischen 2024 und 2028 von 47,97 Mio. auf 114,23 Mio. steigen, was einem durchschnittlichen jährlichen Wachstum von etwa 24,2 % entspricht. Gemessen an der absoluten Anzahl der IoT-Verbindungen zählt der Smart-City-Sektor zum drittgrößten IoT-Bereich.[95]
- Zwar haben intelligente Städte viele verschiedene Infrastrukturebenen, IoT-Geräte sind aber zunehmend das zentrale System, auf das zurückgegriffen wird.[96] Von der intelligenten Umweltüberwachung bis hin zur smarten Bewässerung von kommunalen Grünflächen unterstützen IoT-Geräte deutsche Städte, Gemeinden und Landkreise dabei, kommunalen Herausforderungen zu begegnen und den Bürgerinnen und Bürgern durch digitale Vernetzung besser und effizienter zu helfen.[97]

---

89 Vgl. Statista (2025b)
90 Vgl. BMWK (2023).
91 Ebd.
92 Vgl. Fraunhofer-Institut für Offene Kommunikationssysteme Fokus (o.J.) sowie Caburn Telecom (2024).
93 Vgl. Statista (2024b).
94 Ebd.
95 Vgl. Statista (2024c).
96 Vgl. Expert Market Research (2024).
97 Vgl. BMWK (2025).

- Eine explorative Befragung der TU München unter deutschen Städten ergab, dass etwa die Hälfte LPWAN (Low Power Wide Area Network)-Technologien nutzt, wobei die Verwendung von LoRaWAN (Long Range Wide Area Network) deutlich dominierte.[98] LoRaWAN-Netzwerke nutzen Kommunen jeder Größenklasse, wobei die Lösungen von der Kommune selbst, den kommunalen Unternehmen (insbesondere Stadtwerke) und spezialisierten IT-Dienstleistern ausgebaut werden.[99] Seit 2021 häufen sich die Meldungen zum Ausbau von LoRaWAN-Netzwerken in Stadtverwaltungen und Stadtwerken.[100]

Im **Energiesektor** spielt IoT ebenfalls eine zentrale Rolle bei der digitalen Transformation, wobei sich in Deutschland intelligente Stromnetze (Smart Grids) immer stärker durchsetzen.[101]

- Der Einsatz von Smart Grids ermöglicht in Deutschland jährliche Kosteneinsparungen in Höhe von 9,03 Mrd. Euro sowie zusätzliche wirtschaftliche Wachstumsbeiträge von geschätzten 1,7 Mrd. Euro pro Jahr.[102]
- Studien zeigen, dass die LoRaWAN-Technologie und Smart Meter[103] vermehrt in der deutschen Energiewirtschaft eingesetzt werden.[104] Darüber hinaus findet auch der Einsatz sogenannter intelligenten Straßenbeleuchtung zunehmend Anwendung.[105] Die Stadtwerke übernehmen häufig eine entscheidende Rolle bei der Umsetzung des LoRaWAN-Netzes.[106] Insbesondere vor dem Hintergrund der Dezentralisierung der Energieproduktion ist IoT besonders relevant, denn es ermöglicht, das dezentrale System mithilfe von Echtzeitüberwachung und -steuerung kontinuierlich zu koordinieren. Das novellierte Messstellengesetz (MsbG) sieht vor, dass Smart Meter bis spätestens 2032 flächendeckend die herkömmlichen Stromzähler in Haushalten und Unternehmen ersetzen. Ab 2025 sind Smart Meter für Verbraucher mit einem Jahresstromverbrauch ab 6.000 Kilowattstunden verpflichtend, während Großverbraucher ab 100.000 Kilowattstunden bis spätestens 2028 entsprechende Systeme installieren müssen. Die Einführung intelligenter Stromzähler (Smart Meter) und IoT-Lösungen ermöglicht Netzbetreibern eine nahezu in Echtzeit erfolgende Überwachung und Steuerung smarter Stromnetze (Smart Grids). Dabei übertragen Stromerzeuger, von Privathaushalten bis hin zu Energiedienstleistern, ihre Daten über IoT-Geräte. Neben der Optimierung der Netze eröffnen die generierten Daten innovative Geschäftsmodelle wie den Weiterverkauf überschüssigen Stroms an E-Autofahrer.[107] In Deutschland ist die Industrie (verarbeitende Gewerbe und

98 Vgl. TU München (2022).
99 Vgl. WIK (2023).
100 Vgl. Ravin (2021).
101 Vgl. Caburn Telecom (2024).
102 Bitkom / Fraunhofer-Institut für System- und Innovationsforschung ISI (2012).
103 Smart Meter wird dem Energiesektor zugewiesen, da es hauptsächlich für die Optimierung und Steuerung von Energieflüssen eingesetzt wird.
104 Vgl. WIK (2023). sowie Sylla/Wendlinger (2023).
105 Vgl. eco / Arthur D. Little GmbH (2020).
106 Vgl. WIK (2023).
107 Vgl. Statista (2024f); Wörrle (2024).

Bergbau) neben privaten Haushalten und dem Verkehr einer der bedeutendsten Energieverbraucher.[108]

Neben den smarten Städten, die 2024 einen Umsatz von 3,33 Mrd. Euro durch IoT-Anwendungen verzeichneten, spielt auch das **Gesundheitswesen** mit 2,59 Mrd. Euro Umsatz eine bedeutende Rolle.[109]

- Laut Statista ist Deutschland führend im Einsatz von IoT im Gesundheitswesen und treibt gezielt Innovationen in diesem Markt voran.[110]
- Es wird erwartet, dass der Umsatz von 2025 bis 2029 eine durchschnittliche jährliche Wachstumsrate von ca. 6,9 % aufweisen wird. Das prognostizierte Marktvolumen im Jahr 2029 beliefe sich damit auf 3,64 Mrd. Euro.[111]
- Eine Studie des Fraunhofer-Instituts für System- und Innovationsforschung (ISI) kommt zu dem Ergebnis, dass jährliche Impulse für das Wirtschaftswachstum in Höhe von 2,6 Mrd. Euro sowie Effizienzsteigerungen im Gesundheitssystem von etwa 9,6 Mrd. Euro durch die intelligente Vernetzung möglich sind.[112]
- Die Medizinbranche setzt IoT in vielerlei Bereichen ein – von medizinischen Wearables über die Patientenüberwachung bis hin zur Kontrolle der Temperatur pharmazeutischer Produkte. Ziel ist es, die Präzision zu optimieren, die Effizienz zu erhöhen, die Kosten zu reduzieren, gesetzliche Vorgaben einzuhalten sowie Gesundheit und Sicherheit zu fördern.[113]
- Laut Studien werden IoT-Technologien eine zunehmend wichtige Rolle im Gesundheitswesen spielen.[114]
- Die zunehmende Nachfrage nach intelligenten medizinischen Geräten und automatisierten Lösungen für die Fernüberwachung von Patienten wird voraussichtlich das Wachstum des Marktes weiter fördern.[115]
- Der Robotik-Markt, der in den vergangenen Jahren ein starkes Wachstum verzeichnete und laut Prognosen auch künftig weiter wachsen wird, erzielte im Jahr 2024 seinen höchsten Umsatzanteil mit 44,93 % im Medizinsektor.[116]

---

108 Vgl. Statistisches Bundesamt (Destatis) (2025). Bedeutung der energieintensiven Industriezweige in Deutschland. https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Industrie-Verarbeitendes-Gewerbe/produktionsindex-energieintensive-branchen.html; Fraunhofer-Institut für Produktionsanlagen und Konstruktionstechnik (n.d.).
109 Vgl. Statista (2024b).
110 Vgl. Statista (2024g).
111 Vgl. Statista (2024h).
112 Vgl. Bitkom / Fraunhofer-Instituts für System- und Innovationsforschung ISI (2012).
113 Vgl. Locke (2021).
114 Vgl. Fortune Business Insights (2024).
115 Vgl. Fortune Business Insights (2024).
116 Vgl. Statista (2024i).

Rund 21,7 % der Unternehmen im Sektor **Verkehr und Lagerei** nutzten im Jahr 2021 IoT-Anwendungen für die Verwaltung von Produktionsprozessen und Logistik. Damit nimmt dieser Sektor eine führende Position in diesem Bereich ein.[117]

- Die intelligente Vernetzung im Verkehrsbereich kann bei der prädiktiven Wartung, dem intelligenten Verkehrs- und Parkraummanagement, der Logistik sowie bei der Verkehrsüberwachung unterstützen.[118]
- Informations- und Kommunikationssysteme in Fahrzeugen sowie die Vernetzung der Verkehrsträger, der Fahrzeuge untereinander und der umgebenden Infrastruktur sorgen dafür, dass der Verkehr auf Straßen und Schienen effizienter, sicherer und ressourcenschonender abläuft.[119]
- Im Jahr 2024 umfasste der Smart-Mobility-Markt ein Umsatzvolumen von 60,6 Mrd. Euro. Shared Mobility machte dabei einen Umsatz von 9,5 Mrd. Euro aus. Es wird erwartet, dass der Smart-Mobility-Markt bis 2026 auf 89,9 Mrd. Euro ansteigen wird.[120]
- Die Anzahl der Carsharing-Fahrzeuge ist dabei über die letzten Jahre kontinuierlich gestiegen. Im Jahr 2024 gab es in Deutschland 43.110 Carsharing-Fahrzeuge.[121] Der Umsatz betrug dabei im Jahr 2024 ca. 0,8 Mrd. Euro. Es wird erwartet, dass der Umsatz bis 2029 auf rund 0,9 Mrd. Euro ansteigen wird.[122]
- Datenräume und Datenplattformen fördern die Vernetzung im Bereich der Mobilität. Projekte wie der Mobility Data Space oder moveID als Teil von Gaia-X-Ökosystem gewinnen zunehmend an Bedeutung im Kontext der vernetzten Mobilität.[123]
- Insgesamt zählt die Datenwirtschaft im Transport- und Mobilitätssektor zu den fünf am schnellsten wachsenden Sektoren in Europa.[124]
- Der Logistik-Servicerobotik-Markt verzeichnete im Jahr 2024 einen Umsatz von 177,0 Mio. Euro. Es wird erwartet, dass dieser Umsatz bis 2029 auf 201,3 Mio. Euro ansteigen wird (durchschnittliche jährliche Wachstumsrate: 2,61 %).[125]
- In Deutschland steigt zudem die Nachfrage nach automatisierten Lagerlösungen in der Logistikdienstleistungsrobotik des Servicerobotikmarktes deutlich. Haupttreiber dieses Trends sind die wachsenden Anforderungen an Effizienz und Kostensenkung in der Logistik sowie der Arbeitskräftemangel in der Branche. Dadurch verzeichnet der Markt für autonome mobile Roboter und automatisierte Lager- und Abrufsysteme ein dynamisches Wachstum. Dieser Entwicklung wird

117 Vgl. Eurostat „Internet der Dinge, nach Aktivitäten der NACE Rev.2“, Code: isoc_eb_iotn2 (https://ec.europa.eu/eurostat/databrowser/view/isoc_eb_iotn2__custom_14755252/default/table?lang=en).
118 Statista (2022).
119 Vgl. acatech (2019).
120 Vgl. Statista (2021).
121 Vgl. Statista (2025c).
122 Vgl. Statista (2025d).
123 Vgl. eco (2023).
124 Vgl. EU-Kommission (2023).
125 Vgl. Statista (2024j).

auch in Zukunft eine hohe Bedeutung zugeschrieben, mit weitreichenden Konsequenzen für Logistikunternehmen und ihre Kunden. Gleichzeitig fördert sie die Weiterentwicklung innovativer Technologien wie künstliche Intelligenz und maschinelles Lernen, die die Leistungsfähigkeit von Servicerobotern weiter steigern.[126]

Auch der Sektor **Handel; Instandhaltung und Reparatur von Kfz** ist vor dem Hintergrund des DA von zentraler Bedeutung.

- Im Jahr 2022 beliefen sich die Risikokapitalinvestitionen in KI-Start-ups in Deutschland im Sektor Groß- und Einzelhandel sowie Logistik auf etwa 238,1 Mio. Euro, während datengetriebene Start-ups im selben Sektor Investitionen von rund 167,6 Mio. Euro verzeichneten. Diese vergleichsweise hohen Investitionsvolumina in Groß- und Einzelhandel sowie Logistik verdeutlichen die Bedeutung und Innovationskraft dieses Sektors.[127]
- Der deutsche Markt für vorausschauende Wartung erwirtschaftete im Jahr 2023 einen Umsatz von ca. 455,7 Mio. Euro und wird bis 2030 voraussichtlich 2.637,9 Mio. Euro erreichen. Hier wird von 2023 bis 2030 eine durchschnittliche jährliche Wachstumsrate von 28,5 % erwartet.[128] Insbesondere die Nachfrage nach Wartung von Produktionsanlagen, einschließlich Maschinen, Aufzügen, Industrierobotern und Pumpen (Fertigungssektor) zur Reduzierung von Kosten und Gesamtausfallzeiten wird voraussichtlich den Markt weiter anführen.[129] Aber auch im Bereich der Kfz-Instandhaltung werden beispielsweise Fahrzeugdaten, die durch Sensoren in den Fahrzeugen erfasst werden, kontinuierlich überwacht, um den Zustand von Motor, Bremsen oder Reifen zu analysieren und Wartungsbedarf frühzeitig zu erkennen.

IoT spielt eine entscheidende Rolle in der **Landwirtschaft, Forstwirtschaft und Fischerei**, da es eine Vielzahl von Zielsetzungen unterstützt, wie etwa die Reduzierung von Abfällen, die Minimierung des manuellen Arbeitsaufwands, die Gewährleistung einer besseren Übersicht für Landwirte sowie die Förderung eines höheren Ertrags und einer verbesserten Pflanzengesundheit.

- Der Marktwert des industriellen Internet of Things (IoT) in der Landwirtschaft in Europa wird im Jahr 2025 voraussichtlich rund 2 Mrd. Euro erreichen, was im Vergleich zum Jahr 2020 einer durchschnittlichen jährlichen Wachstumsrate von etwa 14,39 % entspricht.[130]
- Das Wachstum wird dabei insbesondere durch den verstärkten Einsatz von IoT-Technologien in den Bereichen wie der Überwachung von Nutztieren, der Analyse

126 Ebd.
127 Vgl. OECD.AI (2025). Live data. https://oecd.ai/en/data?selectedArea=investments-in-ai-and-data&selectedVisualization=total-vc-investments-in-data-start-ups-by-country-and-industry%20Accessed%20on%2008%2F01%2F2025.
128 Vgl. Grand View Research (2025).
129 Vgl. Fortune Business Insights (2025).
130 Vgl. Statista (2024k).

von Bodenverhältnissen und dem Management von Ernteprozessen vorangetrieben.[131] Im Jahr 2022 war IoT die wichtigste technologische Neuerung in der Agrartechnikbranche.[132]

- Laut Allied Market Research war das Segment der Präzisionslandwirtschaft im Jahr 2021 der dominierende Bereich innerhalb des IoT-Marktes für die Landwirtschaft und wird voraussichtlich auch bis 2031 führend bleiben. Intelligente Gewächshäuser und Fischzuchtüberwachung hatten zwar einen geringeren Marktanteil, zeigen jedoch bis 2031 ein erhebliches Wachstumspotenzial. Im Jahr 2021 spielte insbesondere das Softwaresegment eine bedeutende Rolle auf dem weltweiten IoT-Markt für die Landwirtschaft. Es stellt eine Vielzahl von Hardware-Steuerungslösungen zur Verfügung, wie zum Beispiel Ertragsmonitoren, Bodensensoren, Wassersensoren und Klimasensoren. Diese Technologien kommen in Bereichen wie der Präzisionslandwirtschaft, in intelligenten Gewächshäusern und in der Aquakultur zum Einsatz.[133]
- Laut einer Studie des Bitkom sind digitale Technologien wie Hightech-Landmaschinen, Agrar-Apps, Robotik und Drohnen mittlerweile ein wesentlicher Bestandteil der Landwirtschaft.[134]
    - In Deutschland nutzen mehr als 82 % der landwirtschaftlichen Betriebe digitale Technologien oder Anwendungen. Besonders finden GPS-gesteuerte Landmaschinen weit verbreitet Anwendung, wobei 45 % der Landwirte diese Technologie nutzen.
    - In 46 % der Betriebe, die Nutztiere halten, kommen intelligente Fütterungssysteme zum Einsatz.
    - Eine präzise Anwendung von Pflanzenschutz- und Düngemitteln wird bereits in jedem dritten Betrieb (32 %) eingesetzt, wodurch sowohl Ressourcen effizient genutzt werden als auch die Umwelt geschont wird.[135]
- Laut einer Studie von PwC weist der Reifegrad im Bereich Smart Farming in Deutschland allerdings erhebliche Unterschiede auf: Während 36 % der Akteure digitale Technologien primär zur Informationsgewinnung nutzen („Einsteiger“), verfügen 24 % („Experten“) über erste Erfahrungen mit fortgeschrittenen Technologien wie Sensorik, Robotik oder Luftüberwachung.[136] Im Gegensatz dazu haben 20 % („Leader“) sowie 17 % („Profis“) Smart Farming als integralen Bestandteil ihrer Prozesse und IT-Infrastruktur etabliert und nutzen Echtzeitinformationen zur flexiblen Prozessanpassung.[137]

131 Vgl. Report Prime (2025).
132 Vgl. Statista (2024l).
133 Vgl. Allied Market Research (2023).
134 Vgl. Bitkom (2020).
135 Ebd.
136 Vgl. PWC (2016).
137 Ebd.

6.2.4 Zusammenfassung der Ergebnisse der Sektoranalyse

Nach unserer Analyse sind vor dem Hintergrund des DA folgende 11 Sektoren für Deutschland besonders relevant:

Tabelle 6: Vom Data Act besonders stark betroffene Branchen

Industrielles IoT **Automotive IoT** **Sonstiges verarbeitende Gewerbe**	Verarbeitendes Gewerbe
Consumer IoT **Sonstiger IKT-Sektor**	Information und Kommunikation
Smart City	Öffentlicher Sektor
Energie(-versorgung)	
Gesundheits- und Sozialwesen	
Verkehr und Lagerei	
Handel; Instandhaltung und Reparatur von Kfz	
Landwirtschaft, Forstwirtschaft und Fischerei	

Quelle: Eigene Darstellung.

Die Sektoren wurden, wie in Kapitel 6.2.2 verdeutlicht, dann als besonders relevant eingestuft, wenn sowohl ausreichend belastbare ökonomische und/oder datenbezogene Wertschöpfungsinformationen vorlagen.

Abschließend zur Sektoruntersuchung werden in Tabelle 7 mögliche Data Sharing-Konstellationen in den 11 identifizierten Branchen illustriert. Dazu wird aufgezeigt, welche Akteure in den jeweiligen Branchen mögliche Dateninhaber, Datennutzer und Datenempfänger bzw. Drittparteien darstellen können.[138] Dies verdeutlicht anschaulich und praxisnah die Relevanz des DA in den jeweiligen Branchen.

138 Zu den einzelnen Rollen, siehe auch Kap. 3.3.

Tabelle 7: Denkbare Rollenkonstellationen in den jeweiligen Sektoren

	Mgl. Dateninhaber	Mgl. Nutzer	Mgl. Datenempfänger
Industrielles IoT	Hersteller vernetzter Maschinen und Anlagen, Robotikunternehmen;	Vor allem Industrieunternehmen	Wartungsdienstleister, Systemintegratoren, Datenintermediäre, etc.
Automotive IoT	Fahrzeughersteller, Infotainment-Diensteanbieter, etc.	Fahrzeughalter, Flottenbetreiber, etc.	Werkstätten, Mobilitätsdienste, Versicherungsunternehmen, Datenintermediäre, etc.
Sonstiges verarbeitendes Gewerbe	Sonstige Hersteller vernetzter Maschinen, Anlagen und Geräte.	(Produktions-)Unternehmen, Endverbraucher	z. B. Service- und Reparaturbetriebe, Systemintegratoren, Datenintermediäre
Consumer IoT	Hersteller von vernetzten Produkten wie bspw. Smart-Home Produkte (z. B. Fernseher, Spielekonsolen, Kühlschrank, etc.)	Privathaushalte, Unternehmen	Reparatur- und Wartungsdienste, Datenintermediäre, etc.
Sonstiger IKT-Sektor	Diensteanbieter (proprietär) , Hersteller von sonstigen vernetzten IKT-Produkten	Unternehmen, Privathaushalte, öffentliche Institutionen	IT-Dienstleister, Systemintegratoren, Datenintermediäre, etc.
Smart City	Anbieter von vernetzten Smart-City-Lösungen (Produkte und zugehörige Dienste),	Städte und Kommunen, Kommunale Unternehmen	IT-Dienstleister, Reparatur- und Wartungsdienstleister, Datenintermediäre
Energie(-versorgung)	Smart Meter- und Smart Grid-Hersteller, Netzbetreiber	Privathaushalte, Unternehmen, Stadtwerke	Energieberater, Energieversorger, Datenintermediäre
Gesundheits- und Sozialwesen	Hersteller vernetzter medizinischer Geräte (z. B. Diagnostikgeräte) und damit verbundener Dienste	Krankenhäuser, Arztpraxen, Pflegeeinrichtungen, Patienten	Telemedizinanbieter, Gesundheitsforschungsinstitutionen, Versicherungen, Datenintermediäre
Verkehr und Lagerei	Hersteller / Anbieter IoT-basierter Logistiklösungen	Spediteure, Transportunternehmen	Kunden der Logistikunternehmen, Servicedienstleister, Datenintermediäre
Handel; Instandhaltung und Reparatur von Kfz	Fahrzeughersteller; Hersteller von smarten Checkout-Systemen	Fahrzeughalter, Flottenbetreiber; Handelsunternehmen	Unabhängige Werkstätten, Versicherungen, Datenintermediäre
Landwirtschaft, Forstwirtschaft und Fischerei	Hersteller vernetzter Landmaschinen, Hersteller von Booten	Landwirte, Fischereibetriebe	Reparatur- und Wartungsdienstleister, Datenintermediäre

7 Anbieteranalyse

Im Bericht zur Folgenabschätzung des DA der Europäischen Kommission wird auf 300.000 private Unternehmen in der EU verwiesen, deren Produkte Daten genieren.[139] Der Bericht verweist hier auf die European Data Market Study aus dem Jahr 2020. Das Datum bezieht sich auf die dort geschätzte Anzahl der „Data Supplier".[140] Der aktuelle Wert, der für Deutschland in der gleichnamigen Folgestudie geschätzt wird, liegt bei rund **50.000 Unternehmen**.[141] Obwohl die Definition der „Data Supplier" in dieser Studie nicht deckungsgleich mit der Definition eines „Data Holders" im Kontext des DA ist, kann dieser Wert als Näherung für die Anzahl potenzieller Dateninhaber in Deutschland interpretiert werden.

Wie einleitend zu diesem Forschungsteil beschrieben, ist es das Ziel der folgenden Anbieteranalyse relevante Anbieter von vernetzten Produkten und verbundenen Diensten zu verifizieren. Dabei erfolgte keine Vollerhebung, sondern eine Analyse einer Stichprobe von 500 potentiell relevanten Anbietern anhand eines strukturierten Prozesses. Im Folgenden werden die Vorgehensweise und die Ergebnisse der Anbieteranalyse beschrieben.

7.1 Vorgehensweise zur Identifikation einer Stichprobe von relevanten Anbietern

Die Anbieteranalyse basierte auf den Ergebnissen der Sektoruntersuchung und konzentrierte sich dabei ausschließlich auf Anbieter, die in den als relevant definierten Sektoren operieren. Die Auswahl der Anbieter folgte einem iterativen Auswahlprozess bestehend aus drei Schritten.

Im ersten Schritt stand die Identifikation einer Stichprobe von potenziell relevanten Unternehmen im Vordergrund. Diese wurden anhand von vier Quellen ermittelt:

- Statista – Ranking von Key Stakeholdern in den Märkten Automotive IoT, Smart Home & Consumer IoT, Smart City, IoT, Robotik und digital Health/Smarte Gesundheit.
- Studien wie Fortune Business Insights / IoT Analytics etc., in denen weltweite relevante Unternehmen aufgelistet werden – insbesondere hinsichtlich relevanter

139 EU-Kommission (2022). Impact Assessment Report – Accompanying the document: Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). Commission Staff Working Document. SWD(2022) 34 final.

140 EU-Kommission (2020). The European Data Market Study 2017-2020. Studie erstellt durch IDC, The Lisbon Council. https://digital-strategy.ec.europa.eu/en/library/results-2017-2020-european-data-market-study

141 EU-Kommission (2024d). The European Data Market Study 2024-2026. Studie erstellt durch IDC, CARSA, The Lisbon Council. https://digital-strategy.ec.europa.eu/en/library/european-data-market-study-2024-2026. Der Wert für 2024 liegt bei 48.326 Unternehmen. Die Schätzung für 2025 liegt bei 50.495 Unternehmen.

Unternehmen im Gesundheitsbereich, relevanter Unternehmen von vernetzten Fahrzeugen, führender IoT-Unternehmen und führender IoT-Software.

- Desk Research über Dealroom und Crunchbase[142] sowie gängige Suchmaschinen – insbesondere für die Sektoren „Energie(versorgung)“, „Verkehr und Lagerei“, Handel, Instandhaltung und Reparatur von Kfz“ und „Landwirtschaft, Forstwirtschaft und Fischerei“

- Smart City Navigator des BMWK

Die initiale Stichprobe von 500 potenziell relevanten Unternehmen bzw. Anbietern von vernetzten Produkten und verbundenen Diensten wurde somit auf Basis von Unternehmensrankings, Datenbanken und anderen Marktanalysen ausgewählt. Diese setzen einen unterschiedlichen Fokus auf verschiedene Unternehmensgrößen und -typen (KMU, Start-ups & Scale-ups, Großunternehmen) und trugen damit dazu bei, ein differenziertes Bild der potentiell relevanten Unternehmen im Kontext des DA zu erhalten. Das Ergebnis aus diesem Schritt war die Ableitung einer Stichprobe von 500 Unternehmen, die potenziell als Dateninhaber gelten können.

Im zweiten Schritt erfolgte eine Sichtung der initialen Stichprobe von 500 Unternehmen (potenzielle Dateninhaber). Im Rahmen dieser Evaluation wurden Unternehmen von der weiteren Betrachtung ausgeschlossen, für die nicht verifiziert werden konnte, dass sie in Deutschland tätig sind. Dies bedeutet, dass ein Ausschluss erfolgte, wenn keine deutschsprachige Webpräsenz vorhanden war oder keine Hinweise darauf vorlag, dass das Unternehmen eine Tätigkeit in Deutschland ausübt. Darüber hinaus wurden Unternehmen ausgeschlossen, auf deren Webseiten keine Anhaltspunkte zu ihrer potenziellen Rolle als Dateninhaber gefunden werden konnten. Die initiale Stichprobe (n=500) reduzierte sich damit auf 235 Unternehmen (potenzielle Dateninhaber).

Im dritten Schritt wurden für die 235 verbleibenden Unternehmen in der Stichprobe ein umfassendes Desk Research ausgeführt und ein Merkmalkatalog ausgefüllt. Die **quantitativen Merkmale** umfassen die Mitarbeiterzahl, den Umsatz, den Unternehmenswert bzw. die Marktkapitalisierung, die Investitionsausgaben für Forschung und Entwicklung, den Marktanteil und die Anzahl an verkauften vernetzten Produkte oder verbundenen Diensten. Die **qualitativen Merkmale** umfassen den Unternehmensnamen, die Rechtsform, eine Kurzbeschreibung, den Sektor, die Webseite, den Standort bzw. Hauptsitz, die Geschäftsbeziehungen, die Art der vertriebenen vernetzten Produkte und verbundenen Dienste und eine Relevanzbewertung als Ordinalskala (sektorübergreifend und im jeweiligen Sektor). Bei der Wahl der Merkmale wurde allgemein der Fokus auf die Datenverfügbarkeit und Relevanz aus Sicht des DA gelegt. Informationen zu den Merkmalen wurden für die 235 Unternehmen systematisch recherchiert. Jedoch waren Informationen zu den quantitativen Merkmalen nicht immer für alle Unternehmen verfügbar.

142 Crunchbase ist eine Plattform, die umfassende Informationen über Unternehmen, wie deren Finanzierungsrunden sowie Investoren bereitstellt (vgl. https://www.crunchbase.com/home).

Bei der Einordnung in die Sektoren wurden zusätzlich spezifische Tätigkeitsbereiche der Unternehmen einbezogen. Ein Unternehmen, das Smart Meter herstellt, wäre beispielsweise formal dem verarbeitenden Gewerbe zuzuordnen, aber da die Anwendung dieser Geräte auf den Energiesektor ausgerichtet ist wäre eine Zuordnung zum Sektor Energieversorgung sinnvoll. Demnach bestand die Möglichkeit, dass ein Unternehmen mehreren Sektoren zugeordnet wurde.

Zur Bewertung der Relevanz der Unternehmen sowohl innerhalb als auch zwischen den definierten Sektoren wurde primär die Umsatzspannen herangezogen. Für die sektorübergreifende Einordnung wurden die Unternehmen nach ihrer Umsätzen sortiert. Anschließend wurden sie in Abhängigkeit ihrer Umsätzen in Gruppen sortiert:

- Gruppe 1/ Rang 1: Umsatz über 9,5 Milliarden Euro
- Gruppe 2/ Rang 2: Umsatz zwischen 950 Millionen und 9,5 Milliarden Euro
- Gruppe 3/ Rang 3: Umsatz zwischen 470 und 950 Millionen Euro
- Gruppe 4/ Rang 4: Umsatz zwischen 95 und 470 Millionen Euro
- Gruppe 5/ Rang 5: Umsatz zwischen 47 und 95 Millionen Euro
- Gruppe 6/ Rang 6: Umsatz zwischen 9,5 und 47 Millionen Euro
- Gruppe 7/ Rang 7: Umsatz zwischen 0,95 und 9,5 Millionen Euro
- Gruppe 8/ Rang 8: Umsatz unter 0,95 Millionen Euro

In Fällen, in denen diese Werte nicht verfügbar sind, wurde die Mitarbeiterzahl als alternative Bezugsgröße herangezogen. Zur sektorspezifischen Einordnung wurde die Kategorisierung an die jeweiligen Umsatz- und Mitarbeiterstrukturen angepasst.

Im Zuge der Recherche wurde zudem näher betrachtet, ob die Unternehmen als Dateninhaber agieren. Allerdings sind Informationen zur Datennutzung und -kontrolle oft nicht öffentlich verfügbar oder nur indirekt erschließbar. Der Einsatz vernetzter Produkte und / oder verbundener Dienste wird zum Teil nicht explizit ausgewiesen. In vielen Fällen musste daher auf Annahmen zurückgegriffen werden, etwa auf Basis des Geschäftsmodells, des Branchenkontexts oder typischer Anwendungsfälle. Des Weitern wurde darauf geachtet, ob die Unternehmen mehr als zehn Mitarbeiter beschäftigen, die Unternehmen tatsächlich in die zuvor ausgewählten Sektoren fallen und ob die Art der angebotenen Produkte und Dienstleistungen unter den Data Act fällt. Wenn diese Kriterien nicht zutreffen wurden die Unternehmen von der weiteren Betrachtung ausgeschlossen.

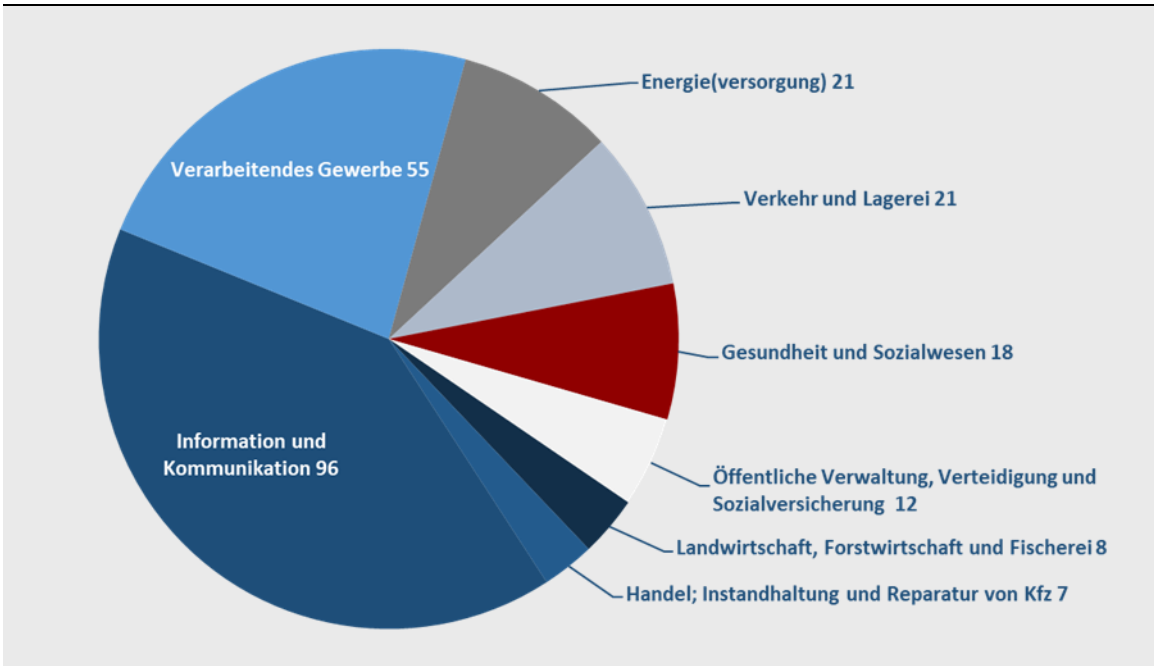
Das Ergebnis dieser Anbieteranalyse sind 166 verifiziert relevante Unternehmen ausgehend von einer Stichprobe von 500 als potentiell relevant eingestuften Unternehmen. Dies bedeutet, dass etwa ein Drittel der initialen Stichprobe basierend auf der verwendeten Methode als relevant im Kontext des DA identifiziert werden konnte. Das Fehlen von öffentlichen Informationen zum Nachweis einer Relevanz impliziert allerdings nicht, dass alle Unternehmen der initialen Stichprobe die nicht weiter betrachtet werden

konnten notwendigerweise als irrelevant im Kontext des DA einzustufen sind. Im Hinblick auf Unternehmen die z.B. ein datengetriebenes Geschäftsmodell verfolgen kann der Anteil der identifizierten DA relevanten Unternehmen in der Stichprobe daher als konservativer unterer Grenzwert interpretiert werden.

7.2 Ergebnisse der Anbieteranalyse

Im Folgenden geben wir einen detaillierten Einblick in die deskriptive Statistik der identifizierten Unternehmen. Abbildung 18 zeigt die Verteilung der Unternehmen nach den acht Hauptsektoren.

Abbildung 18: Verteilung nach Hauptsektoren (absolute Anzahl)



Quelle: Eigene Darstellung. Mehrfachnennung möglich.

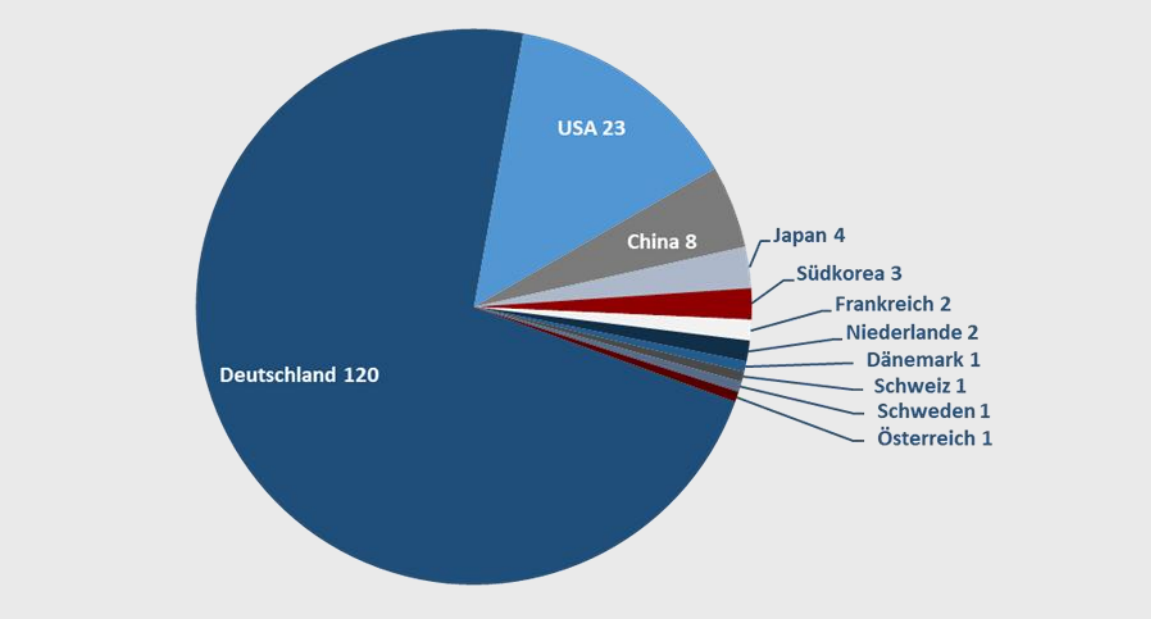
Über die Hälfte der identifizierten Unternehmen stammen aus den Sektor Information und Kommunikation sowie dem verarbeitenden Gewerbe. Die beiden Hauptsektoren gliedern sich in weitere Untersektoren. Von den insgesamt 96 Unternehmen im Bereich IKT sind 23 Unternehmen dem Bereich Consumer IoT zuzuordnen. Im verarbeitenden Gewerbe sind 55 Unternehmen tätig, wobei 11 Unternehmen im Bereich Automotive IoT und 14 Unternehmen im Bereich Industrial IoT tätig sind. Der Hauptsektor Öffentliche Verwaltung, Verteidigung und Sozialversicherung untergliedert sich in den Bereich Smart City, dem 12 Unternehmen zugeordnet sind.

Da die Mehrheit der betrachteten Unternehmen IoT-Produkte wie Maschinen oder Software entwickeln, die den Kategorien verarbeitendes Gewerbe oder Information und Kommunikation zuzuordnen sind, haben wir bei der Sektorzuordnung auch spezifische Tätigkeitsbereiche bzw. die Zielgruppe der Unternehmen berücksichtigt. Dies führt dazu,

dass Unternehmen, die gemäß der klassischen Wirtschaftszweigdefinition beispielsweise dem verarbeitenden Gewerbe zugeordnet sind, aufgrund ihrer Zielgruppe – etwa Landwirte – dem Sektor Landwirtschaft zugeordnet wurden.

Die Mehrheit der identifizierten Unternehmen haben einen Hauptsitz bzw. Standort in Deutschland, gefolgt von Unternehmen mit Sitz in den USA und China (vgl. Abbildung 19).

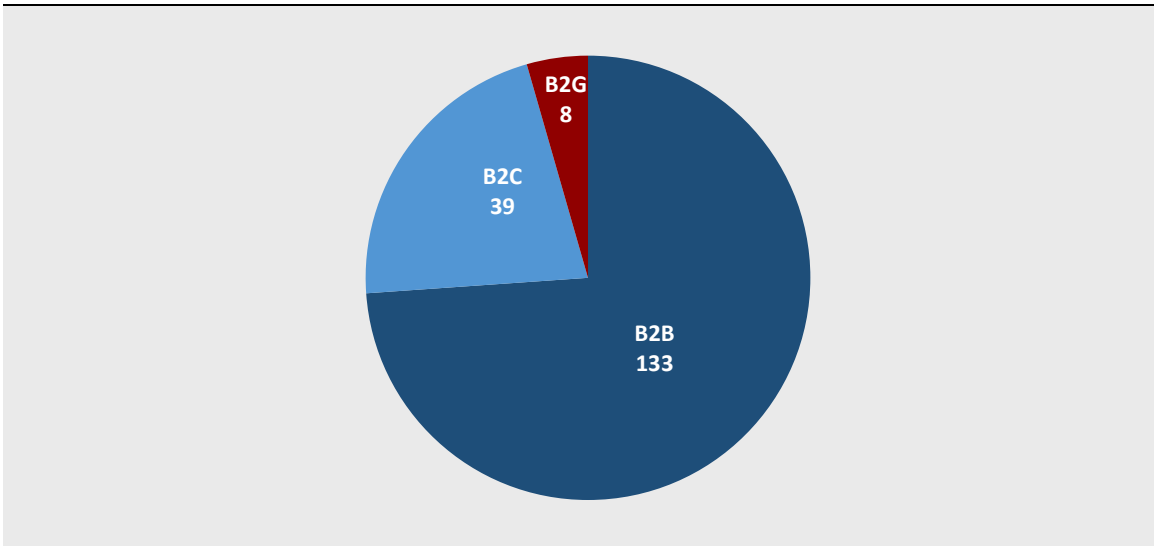
Abbildung 19: Unternehmen nach Hauptsitz (absolute Anzahl)



Quelle: Eigene Darstellung.

Abbildung 20 zeigt, dass die Mehrheit der Unternehmen hauptsächlich im B2B-Bereich operiert, gefolgt von B2C- und B2G-Geschäftsbeziehungen. Die Zuordnung der Geschäftsmodelle, erfolgt auf Grundlage der überwiegenden Geschäftstätigkeit, die den primären Umsatzanteil ausmacht, als auch unter Berücksichtigung der Hauptzielgruppen.

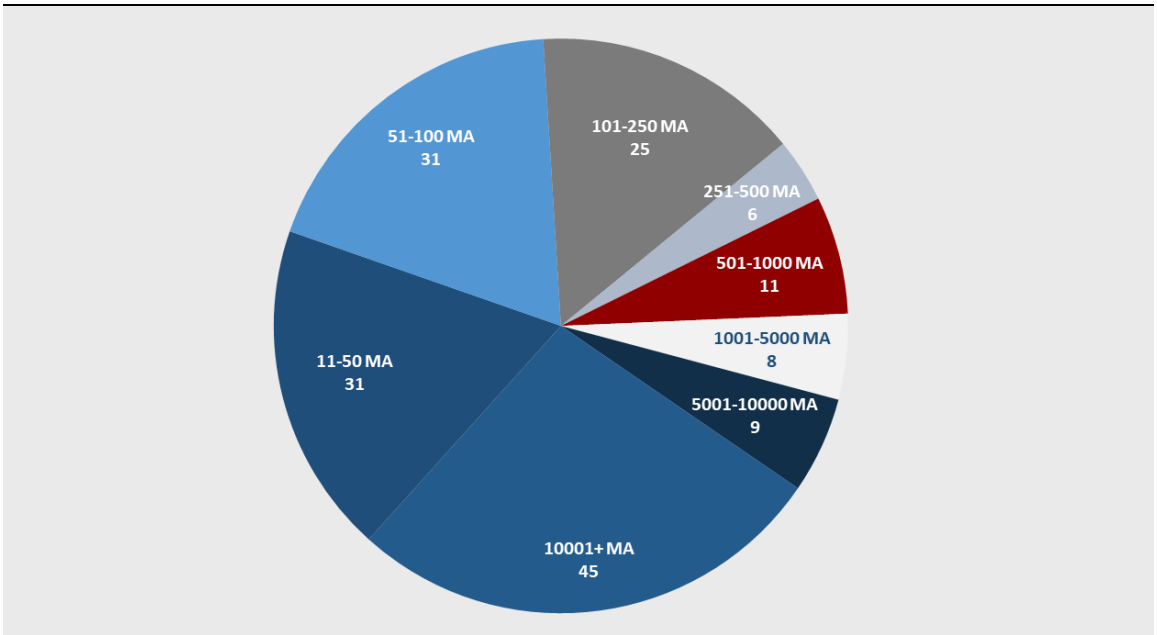
Abbildung 20: Unternehmen nach Geschäftsbeziehung (absolute Anzahl)



Quelle: Eigene Darstellung. Mehrfachnennung möglich.

Etwa 52 % der von uns identifizierten Unternehmen beschäftigen bis zu 250 Personen. 48 % der Unternehmen haben eine Belegschaft von mehr als 250 Personen (vgl. Abbildung 21). Unternehmen mit weniger als 11 Mitarbeitenden sind nicht berücksichtigt, da sie aufgrund ihrer geringen Unternehmensgröße als wenig relevant eingestuft wurden. Die 45 analysierten größten Unternehmen sind überwiegend dem Sektor Information und Kommunikation und/oder dem verarbeitenden Gewerbe zuzuordnen. Ihre Hauptsitze liegen dabei mehrheitlich außerhalb Europas.

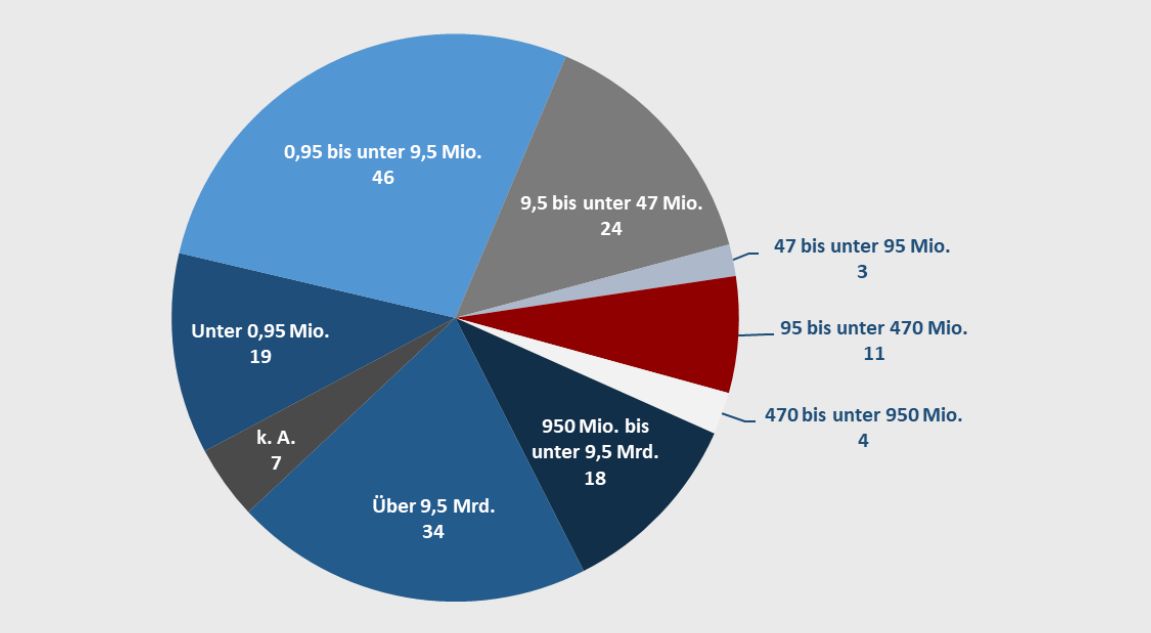
Abbildung 21: Unternehmen nach Mitarbeiterzahl (absolute Anzahl)



Quelle: Eigene Darstellung.

Rund die Hälfte der von uns identifizierten Unternehmen verzeichnen einen Umsatz von 0,95 bis 9,5 Mio. bzw. über 9,5 Mrd. Euro. Unternehmen mit über 9,5 Mrd. Euro können meist dem Sektor verarbeitendes Gewerbe und / oder Information und Kommunikation zugeordnet werden. Anteilig betrachtet, weist der Sektor Handel und Gesundheit jedoch nach unserer Analyse den höchsten Anteil an Unternehmen mit einem Umsatz von über 9,5 Mrd. Euro auf. Der Sektor Landwirtschaft stellt den einzigen betrachteten Sektor dar, der nach unserer Analyse keine Unternehmen mit einem Umsatz von über 9,5 Mrd. Euro umfasst.

Abbildung 22: Unternehmen nach Umsatz (in Euro) (absolute Anzahl)



Quelle: Eigene Darstellung

8 Zwischenfazit zum Teil II

Der Data Act als horizontale Regulierung ist für alle 21 Wirtschaftszweige von Bedeutung. Unsere Analyse zeigt, dass Unternehmen in 11 Sektoren aufgrund ihrer ökonomischen und datenbezogenen Relevanz besonders von der Verordnung betroffen sind. Insgesamt kann auf Basis der European Data Market Study davon ausgegangen werden, dass in Deutschland bis zu 50.000 Unternehmen vom DA betroffen sind.

- Eine hohe IoT-Durchdringung ist insbesondere im verarbeitenden Gewerbe zu verzeichnen, insbesondere in den Bereichen Industrielles IoT als auch im Bereich Automotive IoT.
- Darüber hinaus sticht der IKT-Sektor in seiner Relevanz für den Data Act hervor, hier insbesondere im Bereiche Consumer IoT.
- Im Bereich des öffentlichen Sektors ist vor allem der Bereich Smart City von Bedeutung. Dieser weist im Hinblick auf die IoT-Verbindungen eine der höchsten prognostizierten Wachstumsraten im Zeitraum von 2024-28 auf. Damit gehört der Smart City-Sektor zu einer der wichtigsten Segmente im IoT-Markt und hat somit auch für den Data Act eine besondere Bedeutung.
- Auch der Gesundheitssektor zeigt eine hohe Relevanz, was u.a. daran abgelesen werden kann, dass der Medizinbereich den höchsten Umsatzanteil im deutschen Robotik-Markt erzielt.
- Neben den bisher genannten Branchen kann gezeigt werden, dass auch den Sektoren Verkehr und Lagerei, Energie(versorgung), Handel & Instandhaltung und Reparatur von Kfz sowie dem Bereich Landwirtschaft. Forstwirtschaft und Fischerei eine besondere Bedeutung im Hinblick auf den Data Act zukommt.

Neben den Sektoren wurde im Zuge der Anbieteranalyse auch eine Stichprobe von 500 als potentiell relevant eingeschätzten Unternehmen in diesen Sektoren näher untersucht. Dabei wurden relevante Unternehmen identifiziert, die sich in den 11 ermittelten Sektoren bewegen. Hierzu wurde sowohl auf qualitative als auch quantitative Indikatoren zurückgegriffen.

- Die Analyse zeigt, dass die Relevanz im Kontext des DA für ca. ein Drittel der Unternehmen in der betrachteten Stichprobe bereits mit öffentlich verfügbaren Informationen nachgewiesen werden konnte.
- Mehr als die Hälfte dieser Unternehmen sind dem IKT-Sektor zuzuordnen.
- Mehr als ein Drittel dieser Unternehmen fallen in den Bereich des verarbeitenden Gewerbes.

Die Anbieteranalyse untermauert damit die besonders hervorgehobene Rolle dieser beiden Sektoren für die Relevanz des Data Act. Ca. 80 % der identifizierten Unternehmen sind hauptsächlich im Business-to-Business-Umfeld (B2B) unterwegs.

TEIL III: Ausgewählte Anwendungsherausforderungen des Data Act

In diesem Teil werden ausgewählte Anwendungsherausforderungen des Data Sharing gemäß DA einer Analyse unterzogen. Die Anwendungsherausforderungen wurden in Absprache mit dem Auftraggeber ausgewählt. Zunächst werden in Kapitel 9 mögliche Herausforderungen analysiert, die aus der Überschneidung der Anwendungsbereiche des DA und der DSGVO resultieren. In Kapitel 10 wird anschließend der Umgang mit Geschäftsgeheimnissen im DA näher betrachtet und das daraus resultierende Spannungsfeld zwischen Innovationsanreizen und Geheimnisschutz.

9 Der weite Datenbegriff des Data Acts – eine Herausforderung bei Erfüllung von Datenzugangsansprüchen in Ansehung des Datenschutzrechts aus der DSGVO

9.1 Überblick

Der DA definiert Daten als „jede digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen auch in Form von Ton-, Bild- oder audiovisuellem Material“ (Art. 2 (1) DA). Diese Daten können sich entsprechend des Erw.-Gr. (34) DA auch auf natürliche Personen beziehen, d. h. personenbezogene Daten im Sinne der DSGVO darstellen. Bei der Definition personenbezogener Daten nimmt der DA in Art. 2 (3) DA ausdrücklich auf die Definition in Art. 4 (1) DSGVO Bezug, womit „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“ vom DA mit umfasst sind.[143]

Damit können Gegenstand der Datenzugangsansprüche aus dem DA auch personenbezogene Daten sein, weshalb sich die Anwendungsbereiche von DA und DSGVO mit ihren von Haus aus unterschiedlichen Zielrichtungen überschneiden. Während der DA das Datenwirtschaftsrecht fokussiert und den Zugang ganz allgemein zu *allen* Daten – und damit auch zu den personenbezogenen – eröffnen will, schränkt die DSGVO den Zugriff auf personenbezogene Daten zum Schutz der Betroffenen ein bzw. stellt die Zugriffsmöglichkeit unter enge, den Eingriff in das Persönlichkeitsrecht rechtfertigende Bedingungen. Hieraus resultiert ein erhebliches Spannungsverhältnis zwischen den beiden Rechtsakten und führt den Dateninhaber – wie aufzuzeigen sein wird – in eine Dilemmasituation, weshalb in der Zukunft weitere Konkretisierungen erforderlich werden, um ihm die Wahrung seiner Pflichten aus dem DA und der DSGVO zu ermöglichen.

143 Siehe auch Kap. 3 zum Anwendungsbereich des DA.

9.2 Normatives Verhältnis des Data Act zur DSGVO am Beispiel eines Use Case

Der Gesetzgeber hat im DA normiert, dass dieser unbeschadet des europäischen und nationalen Datenschutzrechts gilt (Art. 1 (5 S. 1) DA) und weiter, dass der DSGVO in Konfliktsituationen, namentlich im Falle eines „Widerspruchs" zwischen dem DA und dem „Schutz personenbezogener Daten bzw. der Privatsphäre", ein Vorrang einzuräumen ist (vgl. Erw.-Gr. (7 S. 5) DA; Art. 1 (5 S. 3) DA). Außerdem, dass der DA die DSGVO in Einzelbereichen zwar ergänzen kann (vgl. Erw.-Gr. (7) i.V.m. Art. 1 (5 S. 3) DA; z. B. bezüglich des Auskunftsrechts nach Art. 15, 20 DSGVO), sich aber eine Abschwächung oder Einschränkung des Datenschutzes in Anwendung und Auslegung des DA jedenfalls verbietet (vgl. Erw.-Gr. (7 S. 5) DA).

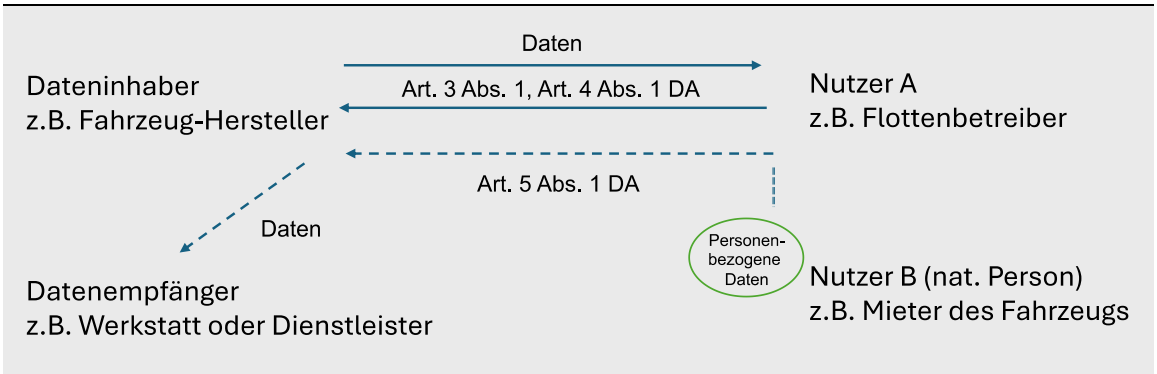
Trotz dieser scheinbar eindeutigen Festlegungen betreffend die Unberührbarkeit des Datenschutzrechts verbleiben in der Praxis Schwierigkeiten. Dabei entstehen besondere Spannungen zwischen dem Recht des Nutzers auf Datenzugang und Nutzbarmachung von Daten einerseits (vgl. Art. 4 und 5 DA) und der Verpflichtung zur Heraus- und Weitergabe der Daten auf Seiten des Dateninhabers andererseits, sofern dieser einem präventiven Verbot zur Weitergabe von personenbezogenen Daten des Nutzers oder eines Dritten aus der DSGVO unterworfen ist (vgl. Art. 6 und Art. 9 DSGVO), welches zudem von den datenschutzrechtlichen Grundsätzen der Zweckbindung und Datenminimierung (Art. 5 (1 lit. b) und (lit. c) DSGVO) sowie den datenschutzrechtlichen Löschpflichten nach Art. 17 DSGVO flankiert wird. Konkret könnte ein Nutzer etwa Datenzugangsansprüche nach Art. 4 oder 5 DA gegenüber dem Dateninhaber geltend machen, bei deren Erfüllung (auch) personenbezogene Daten des Nutzers selbst oder eines Dritten (der ggf. ebenfalls Nutzer iSv Art. 2 (12) DA ist) betroffen sein könnten (angedeutet in Erw.-Gr. (34 S. 1)), so dass die Bereitstellung der personenbezogenen Daten (z. B. an einen Drittempfänger) in den Anwendungsbereich der DSGVO fiele und dabei entweder verboten wäre oder weitere Handlungen erfordern würde (siehe auch Erw.-Gr. (34 S. 6 ff.)).

Beispielhaft kann die Situation eines Fahrzeugflottenbetreibers benannt werden, der als Nutzer A im Sinne des Art. 2 (12) DA seine Datenzugangsansprüche gegenüber dem Fahrzeughersteller als Dateninhaber geltend macht (z. B. bezüglich der Daten zu Betriebsstunden oder bezüglich des Zustands wichtiger Komponenten wie Motor, Getriebe und Bremsen für die Wartungsplanung eines Drittempfängers) und bei deren Weitergabe an einen Datenempfänger (z. B. eine Werkstatt) auch personenbezogene Daten der jeweiligen Fahrzeugführer als Dritte (natürliche Person und Nutzer B als Mieter) betroffen sind (z.B. Klardaten der Dritten; Nutzerkonten der Dritten oder technische Identifier des Nutzers B, wie Strecken-Profil oder Informationen über verbundene Begleit-Apps). In einem solchen Fall kollidiert dann die Erfüllung der Datenzugangs- bzw. Weitergabeansprüche des Nutzers A aus Art. 4 (1), Art. 5 (1) DA mit den Restriktionen der DSGVO, die der Dateninhaber sowie der Nutzer A gegenüber dem Nutzer B zu berücksichtigen haben.[144] Gerade diese Konstellation, in der Nutzer

144 *Martini/ Roeingh,* NJW 2024, 2379.

(Nutzer A) und Betroffener (Nutzer B) personenverschieden sind, kann dann erhebliche Verwerfungen im Verhältnis DA zur DSGVO verursachen (siehe Abbildung 23).

Abbildung 23: Beziehungsgeflecht am Beispiel eines Use Case



Quelle: Eigene Darstellung

Sind hingegen Nutzer und betroffene Person identisch (nur der Nutzer A), bleibt das Datenschutzrecht zwar ebenfalls im vorgenannten Sinne anwendbar, allerdings ist diese Konstellation datenschutzrechtlich eher unproblematisch, da der Nutzer A schon in eigenem Interesse eine rechtfertigende Einwilligung zum Datentransfer i.S. des Art. 6 (1) oder Art. 9 (1) DSGVO gewähren wird. Dabei wird nach herrschender Meinung[145] das Datenherausgabeverlangen als datenschutzrechtliche Einwilligung angesehen (vgl. auch unter 9.3.3).

In der Situation (siehe Abbildung 23), in der Nutzer A und Nutzer B personenverschieden sind, werden allerdings weitere Festlegungen / Konkretisierungen vorzunehmen sein, um Dilemmasituationen insbesondere für den Dateninhaber – die zudem mit beträchtlichen Haftungsrisiken verbunden sein können (Art. 40 DA; Art. 83 DSGVO) – zu vermeiden. Solche Dilemmasituationen sind jedenfalls präsent. Denn kennt der Dateninhaber die datenschutzrechtliche Betroffenheit des Dritten (Nutzer B) nicht oder schätzt die Qualität der Daten fälschlicherweise als nicht-personenbezogen ein, liegt im Erfüllen der Datenzugangs- und Weitergabeansprüche unter Missachtung datenschutzrechtlicher Vorgaben ein Verstoß gegen die DSGVO. Geht er hingegen irrtümlich vom Personenbezug der Daten aus und verneint die Datenzugangs- und Weitergabeansprüche, gerät er zwar jetzt nicht mehr mit der DSGVO in Konflikt, verstößt allerdings gegen den Data Act.[146] Dabei ist – darauf wurde bereits an anderer Stelle hingewiesen[147] – die Qualität der Daten als personenbezogen oder nicht-personenbezogen nicht einfach zu entscheiden,[148] klare Kriterien gibt es derzeit nicht. Der Begriff des personenbezogenen Datums soll vielmehr weit zu verstehen sein und die Bestimmung des Personenbezugs

145 *Hennemann/Steinrötter* NJW 2024, 1, 4; *Paal/Cornelius/Seeland* RDV 2024, 5, 10; *Wiebe* GRUR 2023, 1569, 1574; *Götz/Blöink*, MMR 2024, 541, 543.
146 *Götz/Bloink*, MMR 2024, 451.
147 Siehe ausführlich zur Abgrenzung personenbezogener und nicht-personenbezogener Daten Kap. 3.2.1.
148 *Bomhard/Merkle*, RDi 2022, 168 Rn. 27; *Bomhard*, MMR 2024, 71, 74.

einem abstrakten Maßstab „nach allgemeinem Ermessen wahrscheinlich für die Identifizierung“[149] folgen, was einer klaren Konturierung nicht zuträglich ist. Insofern wirkt sich die seit Jahren bekannte Problematik aus dem Datenschutzrecht, nämlich ob und wann Daten einen Personenbezug aufweisen (können), auch auf den Data Act aus und ist jedenfalls mitursächlich für die vorbeschriebene Dilemmasituation.[150] Die im Umgang mit der DSGVO praktizierte Herangehensweise, nämlich im Zweifel vom Vorliegen personenbezogener Daten auszugehen, um das Risiko eines Verstoßes gegen die DSGVO zu vermeiden, funktioniert unter dem Damoklesschwert des DA ebenfalls nicht mehr, denn der Dateninhaber würde mitunter sanktionsbewährt gegen den DA verstoßen. Ferner würde eine solche Zweifelsregel die Ziele des DA, nämlich möglichst viele Daten zu teilen, konterkarieren.

9.3 Identifizierte Problembereiche

Nachfolgend sollen nun zunächst die Problembereiche benannt werden, die sich aus der Konstellation des oben angeführten Use Case ergeben, bevor im Anschluss erste Lösungsansätze vorgestellt werden.

9.3.1 Abgrenzung personenbezogene / nicht personenbezogene Daten

Wie zuvor dargestellt ist ein Grundproblem der DSGVO und jetzt auch des DA, dass sich Daten (IoT-Daten oder gemischte Datensätze) nicht eindeutig in die Kategorien mit und ohne Personenbezug klassifizieren lassen. Dieser Umstand schränkt die möglichen Reaktionen des Dateninhabers erheblich ein oder verpflichtet ihn zu Maßnahmen (z. B. eine unerwünschte und sanktionsbehaftete Flucht in die DSGVO), die bei zutreffender und vorausschauender Einordnung nicht notwendig würden.

Inwieweit in der Zukunft klare Hinweise zur Kategorisierung der Daten von den Datenschutzbehörden oder den Gerichten erwartet werden darf, ist derzeit vollkommen offen. Der Europäische Datenschutzausschuss (EDSA) hat Anfang des Jahres Pseudonymisierungsguidelines veröffentlicht[151] und darüber hinaus sog. Anonymisierungsguidelines angekündigt, die die Operationalisierbarkeit des Datentransfers insgesamt erhöhen sollen, weshalb man sich dort auch Hinweise auf eine rechtssichere Abgrenzung zum „Personenbezug“ im Kontext DSGVO/DA erhofft. Ferner wird in der Rechtssache *Deloitte* ein Urteil des EuGH erwartet (C 413/23 P[152]), das ebenfalls die Abgrenzungsproblematik thematisieren wird und – so die Erwartung in der Rechtswissenschaft – vertiefte Ausführungen zum Verständnis des Personenbezugs liefern wird.

---

149 Zuletzt EuGH, Urt. v. 9.11.2023, C-319/22 - FIN kann personenbezogenes Datum sein.
150 Ausf. *Sattler*, CR 2024, 383 ff.
151 Guidelines 1/2025 on Pseudonymisation – puplic consultation ongoing: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-012025-pseudonymisation_de
152 EuGH (Präsident), Beschluss vom 29.11.2023 – C-413/23 P, BeckRS 2023/47866.

9.3.2 Zuordnung von Verantwortung

Eine weitere Fragestellung, die aus dem o.g. Use Case folgt, ist die nach der Verantwortlichkeit. Wer wäre für die Preisgabe der personenbezogenen – u. U. auch besonders sensiblen personenbezogenen – Daten des Nutzers B verantwortlich? Ist es der Dateninhaber, der die Möglichkeit zur Übermittlung der personenbezogenen Daten eröffnet oder ist es der Nutzer A, der die Datenweitergabe an den Datenempfänger (z. B. eine Werkstatt) veranlasst, u. U. auch erwünscht.

Die DSGVO bestimmt als Verantwortliche im Sinne des Art. 4 (7) DSGVO „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet …“, weshalb sich die datenschutzrechtliche Verantwortlichkeit bei Übermittlung personenbezogener Daten je nach Einzelfall zwar unterschiedlich darstellen kann, die DSGVO aber zumindest auch die gemeinsame bzw. gemeinschaftliche Verantwortung („joint controllership“) sowie ein Auftragsverarbeiterverhältnis kennt. In diesen Fällen müssen nach der DSGVO Vereinbarungen gemäß Art. 26 (1 S. 2) DSGVO oder, bei Auftragsverarbeiterverträge, gemäß Art. 28 (3) DSGVO abgeschlossen werden, welche sicherstellen, dass die Datenverarbeitung durch alle am Verarbeitungsprozess Beteiligten im Einklang mit der DSGVO erfolgt. Dabei normieren Art. 26 (3) und Art. 28 (3) DSGVO die inhaltlichen Mindestanforderungen an einen solchen Vertrag.[153] Nur wenn der Datenempfänger (im Use Case die Werkstatt) ausschließlich eigene Zwecke verfolgt, ist er nach der DSGVO auch als alleiniger, eigenständiger Verantwortlicher zu qualifizieren; Dateninhaber und Nutzer wären dann nicht mehr angesprochen.

Im DA gibt es eine derart klare Bestimmung zur gemeinschaftlichen Verantwortung nicht. Erw.-Gr. (34 S. 6) deutet lediglich eine ähnliche Vorgehensweise an. Danach kann auch der Nutzer, der nicht zugleich der datenschutzrechtlich Betroffener ist (im Use Case wäre das Nutzer A; Nutzer B wäre Betroffener), Verantwortlicher sein, „wenn dieser ein Unternehmen ist und das betreffende Produkt nicht gemeinsam in einem Haushalt verwendet wird“. Insofern ist auch nach dem DA eine gemeinschaftliche Verantwortung vorstellbar, wobei die Verantwortlichen sodann „in einer Vereinbarung in transparenter Form festlegen [sollen], wer von ihnen die einschlägigen Pflichten zur Einhaltung der genannten Verordnung erfüllt.“ (Erw.-Gr. (34 S. 9)).

Insofern kennen sowohl der DA als auch die DSGVO die gemeinsame Verantwortlichkeit und überlassen deren Ausgestaltung einer gemeinsamen Vereinbarung im Innenverhältnis. Es ist naheliegend die Mindestanforderungen, die in der DSGVO an eine solche Vereinbarung gerichtet sind, auch einer Vereinbarung im Rahmen des DA zugrunde zu legen (siehe auch unten 9.4.2 zum „Datenvertrag“).

153 Ausf. u. a. BeckOK Datenschutz R/*Spoerr*, 50. Ed. 1.8.2024, DSGVO Art. 28 Rn. 50 ff.

9.3.3 Vorliegen von Rechtsgrundlagen für den Datentransfer

Unabhängig von der Verantwortung bedarf es für den Datentransfer bzw. der Bereitstellung der Daten des Nutzer B an den Datenempfänger einer rechtlichen Grundlage (Art. 4 (12), Art. 5 (7) DA). Denn die Verarbeitung personenbezogener Daten ist nach der DSGVO nur gestattet, wenn eine datenschutzrechtliche Rechtsgrundlage für die Weitergabe der Daten vorliegt. Die rechtliche Grundlage ist dabei in der DSGVO zu suchen.

Art. 4 (12) sowie Art. 5 (7) DA lauten: Handelt es sich bei dem Nutzer nicht um die betroffene Person, deren personenbezogene Daten verlangt werden, so darf der Dateninhaber personenbezogene Daten, die bei der Nutzung eines vernetzten Produktes oder verbundenen Dienstes generiert werden, dem Nutzer nur dann bereitstellen, wenn es für die Verarbeitung eine gültige Rechtsgrundlage gemäß Artikel 6 der Verordnung (EU) 2016/679 gibt und gegebenenfalls die Bedingungen des Artikels 9 jener Verordnung sowie des Artikels 5 (3) der Richtlinie 2002/58/EG erfüllt sind.

In Betracht kommt zuvorderst die **Einwilligung** i.S. des Art. 4 (11), Art. 6 (1 lit. A)) DSGVO bzw. Art. 9 (2 lit. a) DSGVO, welche in Erw.-Gr. (34) DA ausdrücklich benannt wird.

Sofern der Nutzer zugleich Betroffener ist (sofern im Use Case alleine Nutzer A datenschutzrechtlich Betroffener wäre und es keinen Nutzer B gebe), ist es nach ganz herrschender Auffassung in der Literatur[154] vertretbar, in der Aufforderung zur Nutzung / Weitergabe der Daten eine konkludente, informierte und freiwillige Einwilligung i.S. des Art. 6 (1 lit. A) DSGVO anzunehmen, so dass eine datenschutzrechtliche Problemlage ausscheidet.

Im Falle, dass ein Dritter Betroffener i.S. der DSGVO ist (im Use Case Nutzer B) stellt sich die Situation vielschichtiger dar, wobei vorab festzustellen ist, dass sich die Bereitstellungspflichten aus dem DA nicht über Art. 6 (1) lit. c) DSGVO in eine legitimierende Verarbeitungsgrundlage „umwidmen“ lassen. Denn nach Erw. Gr. (7 S. 7) DA stellt „die … *Verordnung keine Rechtsgrundlage für die Erhebung oder Generierung personenbezogener Daten dar*“. Erw. Gr. (7) DA stellt vielmehr klar, dass bei Auseinanderfallen von Nutzer (im Use Case Nutzer A) und dem datenschutzrechtlich Betroffenen (im Use Case Nutzer B) der DA gerade keine datenschutzrechtliche Rechtsgrundlage für die Gewährung des Datenzugangs bzw. der Weitergabe bilden kann.

Insofern kommen als Verarbeitungsgrundlage für die Datenbereitstellung an den Datenempfänger (z. B. die Werkstatt) sowohl im Rahmen des Art. 4 (1) DA, als auch bei Art. 5 (1) DA zunächst die Einwilligung des Betroffenen (im Use Case Nutzer B) nach Art. 6 (1 lit. a) DSGVO in Betracht, wobei die Anforderungen an eine solche Einwilligung hoch sind (Freiwilligkeit, Informiertheit, Zweckbindung und -gerichtetheit). Insbesondere

154 *Hennemann/Steinrötter* NJW 2024, 1, 4; *Paal/Cornelius/Seeland* RDV 2024, 5, 10; *Wiebe* GRUR 2023, 1569, 1574; *Götz/Blöink*, MMR 2024, 541, 543.

das Erfordernis einer hinreichend informierten Einwilligung lässt sich in multipolaren Strukturen, in denen die Datenempfänger mitunter gar nicht frühzeitig bekannt sind, nur schwer umsetzen. Außerdem ist eine Einwilligung jederzeit widerrufbar (Art. 7 (3) DSGVO), was für den Dateninhaber insbesondere in Datenketten oder bei der Echtzeitübermittlung der Daten eine Herausforderung darstellen kann. Ferner fehlt es regelmäßig an einem direkten Kommunikationskanal zwischen Dateninhaber und Betroffenem, weshalb er seine datenschutzrechtliche Rechenschaftspflicht nur unter Einbezug des Nutzers A erfüllen könnte und die Überprüfung der Einwilligungsvoraussetzungen allenfalls mittelbar möglich wäre, obschon er das (Haftungs-)Risiko bezüglich des Vorliegens einer Einwilligung vollumfänglich tragen würde. Sind besondere Arten personenbezogener Daten betroffen, z. B. bei Fitness- und Gesundheitsprodukten oder im Fahrzeug die Fahrer spezifischen Komforteinstellungen, bedürfte es schließlich nach Art. 9 (2 lit. a) DSGVO einer am konkreten Zweck ausgerichteten, ausdrücklichen Einwilligung gegenüber dem Dateninhaber, was angesichts der vorgenannten Aspekte schwierig ist.

Statt der Einwilligung könnte die Datenverarbeitung **zur Erfüllung eines Vertrags** gemäß Art. 6 (1 lit. b) DSGVO in Betracht kommen, eine Möglichkeit, die Erw.Gr. (34) S. 8 DA erwähnt. Allerdings müsste der Betroffene (im Use Case Nutzer B) hierzu Partei eines Vertrags zwischen dem Nutzer A und dem Dateninhaber sein, für dessen Erfüllung die Datenübermittlung „objektiv unerlässlich [ist], um einen Zweck zu verwirklichen, der notwendiger Bestandteil der für die betroffene Person bestimmten Vertragsleistung ist“, was nach der Rspr. des EuGH weiter erfordern würde, dass der Verantwortliche nachweisen kann, dass „der Hauptgegenstand des Vertrags ohne die betreffende Verarbeitung nicht erfüllt werden könnte“, weil „keine praktikablen und weniger einschneidenden Alternativen bestehen”.[155] Da es zumeist schon an einem entsprechenden Vertragsverhältnis fehlen wird und obendrein die Erforderlichkeit des Datentransfers an den Datenempfänger zur Erfüllung des Vertragszwecks nicht hinreichend nachweisbar sein wird, kommt Art. 6 (1 lit. b) als Legitimationsgrundlage ebenfalls nicht in Betracht.

Als Legitimationsgrundlage bliebe noch die Verarbeitung **zur Wahrung von berechtigten Interessen** nach Art. 6 (1 lit. f) DSGVO. Das „berechtigte Interesse“ ist als datenschutzrechtliche Rechtsgrundlage relevant, wenn weder ein Vertrag mit dem Betroffenen besteht, der eine entsprechende Verpflichtung des Dateninhabers zur Herausgabe oder Weitergabe von Daten mit Personenbezug vorsieht, noch eine Einwilligung des Betroffenen vorliegt. Dabei erfordert die nach Art. 6 (1 lit. f) DSGVO notwendige Interessenabwägung eine Prüfung auf drei Stufen: Zunächst muss der Dateninhaber und / oder Nutzer A sein berechtigtes Interesse an der Bereitstellung der Daten bestimmen (1. Stufe), wobei die Anforderungen niedrig sind. Sodann ist festzustellen, ob die Bereitstellung der Daten für die Wahrung dieses Interesses erforderlich ist (2. Stufe). Letzteres entfällt, wenn der Zweck der Verarbeitung in zumutbarer Weise durch andere mildere (d. h. weniger datenintensive) Mittel erreicht werden kann und die Anforderungen an Zweckbindung und Datenminimierung erfüllt sind. In Kenntnis dieser

155 EuGH, Urt. v. 4.7.2023 - C-252/21, CR 2023, 516 Rz. 98 - Meta/BKartA.

Voraussetzungen nimmt die Literatur an, dass der Dateninhaber annehmen darf, dass eine Datenverarbeitung, soweit sie eine gesetzliche Pflicht nach dem DA erfüllt, jedenfalls erforderlich ist.[156] Schließlich muss auf einer 3. Stufe im Einzelfall noch abgewogen werden, ob entgegenstehende Interessen oder Grundrechte und Grundfreiheiten des Betroffenen (im Use Case Nutzer B) bestehen, die das Interesse des Dateninhabers und / oder Nutzer A überwiegen.[157] Hierbei wird es dann darauf ankommen, inwieweit die Datenübertragung für den Nutzer B erwartbar war und welche Daten an den Datenempfänger übermittelt werden – dienen die Daten eher dem wirtschaftlichen Interesse des Dateninhabers oder des Nutzers A, werden die Interessen des Nutzers B an der Wahrung seiner Persönlichkeitsrechte überwiegen. Steht dagegen ein Zugang zu Daten im Raum, die dem Nutzer B eine Besserstellung versprechen, dürfte das Interesse an der Datenübertragung überwiegen. Zudem können in der Interessenabwägung auch die Wertungen des DA einzahlen: Zumindest für weniger sensible Daten lässt sich argumentieren, dass der VO-Geber mit der Normierung des Zugangsanspruch bereits eine Interessenabwägung zugunsten der Datenübermittlung vorgenommen hat.[158] Allerdings bleibt am Ende die Unsicherheit des Dateninhabers und / oder Nutzers A interessengerecht agiert zu haben – Klarheit erfolgt mitunter erst bei einer ex-post-Kontrolle durch die Gerichte oder Aufsichtsbehörden.

9.4 Mögliche Lösungsansätze

9.4.1 Klare Abgrenzung zum Personenbezug von Daten und Anonymisierungskriterien

Um einen Personenbezug bezüglich der zu transferierenden Daten zu vermeiden, kann der Dateninhaber versuchen (was er heute bereits weitgehend macht), die Datenerhebung bereits so zu konfigurieren, dass die Daten zumindest keine Personenklardaten mehr enthalten. Ferner kann er die Daten – zumindest in der Theorie (die praktischen Abgrenzungsschwierigkeiten wurden bereits angesprochen) – kategorisieren (bei gemischten Datensätzen diese zuvor „aussondern“) und sodann die personenbezogenen Daten anonymisieren, was als Lösungsansatz im Erw.-Gr. (7 S. 12 DA) angedeutet wird.

Ein Aussondern personenbezogener Daten des Betroffenen (im Use Case Nutzer B) aus gemischten Datensätzen dürfte jedoch überhaupt nur in wenigen Ausnahmefällen möglich sein, so dass der Schlüssel zum Gelingen der europäischen Datenstrategie unter gleichzeitiger Wahrung des nach Art. 8 (1 GRCh) verfassungsrechtlich verbürgten Rechts auf Datenschutz zunächst in der Anonymisierung personenbezogener Daten liegt. Dabei gelten personenbezogene Daten als anonymisiert, wenn die Identifizierung der jeweiligen natürlichen Person nicht mehr oder nur mit unverhältnismäßig hohem

156 *Baumann/Brunnbauer*, ZD 2025, 132, 135.
157 EuGH, Urt. v. 4.7.2023 - C-252/21, CR 2023, 516 Rz. 106 f. - Meta/BKartA.
158 *Antoine*, CR 2024, 73, 75 Rz. 10 f.

Aufwand möglich ist bzw. mit an Sicherheit grenzender Wahrscheinlichkeit auch unter Hinzuziehung weiterer Daten ein Personenbezug nicht mehr hergestellt werden. [159]

Eine gesetzliche Pflicht zur Anonymisierung sieht der DA für die Datenbereitstellung im Bereich B2C und B2B – im Gegensatz zur Bereitstellung an öffentliche Stellen (Art. 18 (4 DA)) – nicht vor, wenngleich sich der Dateninhaber einer Anonymisierung wohl nicht würde entziehen können, wenn eine rechtssichere Anonymisierung für den Dateninhaber auch technisch sicher umsetzbar wäre.

Bislang aber werden die Anforderungen an die Anonymisierung – sowohl bei der absoluten[160] als auch der faktischen[161] – als hoch beschrieben und es werden zudem diverse Anonymisierungsmethoden vorgestellt,[162] die jedoch für die Rechtspraxis nicht eindeutig und insbesondere im Prozedere der Datenweitergabe unkonkret und wenig erfolgversprechend bleiben.[163] Eine rechtssichere Anonymisierung, bei der eine Re-Identifizierung nicht mehr möglich ist, gilt oftmals als unmöglich oder geht – wie im Falle der Randomisierung – mit einem erheblichen Informationsverlust einher.

Um die Herausforderung aus dem Spannungsverhältnis DA versus DSGVO zu lösen, könnte es daher erforderlich sein, dass der bisher vertretene „Null-Risiko-Ansatz“ der Anonymisierung überdacht werden muss. Eine Herangehensweise könnte sein, dass die Frage, unter welchen Voraussetzungen personenbezogene Daten als hinreichend gewahrt angesehen werden können, künftig risikobasiert beantwortet wird. Hier könnte – je nach Risiko – zur Wahrung der Interessen der Betroffenen auch eine Pseudonymisierung[164] als ausreichend angesehen werden. Dies lehnt zwar die Mehrzahl der datenschutzrechtlich geprägten Aufsichtsbehörden nach wie vor ab. Allerdings hat schon der EuGH in seiner Breyer-Entscheidung festgestellt (und seitdem regelmäßig wiederholt), dass kein Personenbezug vorliegt, wenn „das Risiko einer Identifizierung de facto vernachlässigbar ist“[165] und damit eben genau die vorbezeichnete Risikobetrachtung vorgenommen.

Dieser Pfad sollte in Ansehung des Zusammenspiels DA/DSGVO weiter beschritten werden und er sollte dort, wo die Anonymisierung aufgrund der Interessenlage erforderlich bleibt, zwingend mit klar definierten Kriterien für die Anonymisierung personenbezogener Daten einhergehen. Die EDSA entwickelt nach eigenem Bekunden aktuell Anonymisierungsguidelines, welche in Ansehung der DSGVO und des DA dann auch Szenarien der Datenweitergabe mit behandeln werden. Insofern wird man abwarten

---

159 *Paal/Pauly/Ernst*, 3. Aufl. 2021, DS-GVO Art. 4 Rn. 48, 51.

160 Man spricht von absoluter Anonymisierung, wenn der Personenbezug für jedermann unmöglich wird.

161 Eine faktische Anonymisierung zeichnet sich dadurch aus, dass die Re-Identifizierbarkeit der betroffenen Person nicht gänzlich ausgeschlossen ist. Allerdings scheidet die Re-Identifizierung der betroffenen Person aufgrund der Unverhältnismäßigkeit ihres Aufwands aus.

162 Vgl. u. a. *Stiftung Datenschutz*, Grundsatzregeln für die Anonymisierung personenbezogener Daten, 2022 sowie *dies*., Praxisleitfaden für die Anonymisierung personenbezogener Daten, 2022.

163 *Schemmel*, CB 2024, 301, 306 ff.

164 Die Pseudonymisierung ersetzt die identifizierenden Merkmale durch Pseudonyme, bietet aber keinen vollständigen Schutz vor Re-Identifizierung und kann unter bestimmten Bedingungen rückgängig gemacht werden. Sie ist „ein Weniger“ gegenüber der Anonymisierung.

165 EuGH ZD 2017, 24 Rn. 46 m. Anm. *Kühling/Klar* = MMR 2016, 842 m. Anm. *Moos/Rothkegel*.

müssen, welche Empfehlungen die EDSA hierzu ausspricht und ob sie einen risikobasierten Ansatz verfolgen wird.

Etwas rigoroser ist ein Lösungsvorschlag, den *Steinrötter*[166] vorbringt. Er geht davon, dass viele Dateninhaber bereits überobligatorisch in Grau- bzw. Grenzbereichen die Anforderungen der DSGVO erfüllen, weshalb man personenbezogene und nicht-personenbezogene Daten im DA von vorn herein gleichbehandeln könnte, was gerade im Hinblick auf gemischte Datensätze besonders sinnvoll erscheinen würde. Dieser Ansatz ist zwar erfreulich klar, wird aber angesichts der zuvor dargestellten Haltung der Datenschutzbehörden („Null-Risiko-Ansatz“) nicht zu realisieren sein. Zudem ist die Annahme, dass alle Unternehmen überobligatorisch die DSGVO erfüllen, eine idealistische und bislang auch nicht weiter belegte Vorstellung.

9.4.2 Überwinden insbesondere des Fehlens einer datenschutzrechtlichen Rechtsgrundlage durch einen Datenvertrag

Wenn weder eine Anonymisierung der Daten noch eine Absonderung der personenbezogenen Daten möglich ist, verbleibt dem Dateninhaber nurmehr – wie dargestellt – eine datenschutzrechtliche Rechtsgrundlage i.S. des Art. 6 (1) DSGVO zu bemühen, was – wie aufgezeigt – Schwierigkeiten bereiten kann.

Selbst wenn man sich eine Legitimation über die „berechtigten Interessen“ herstellen ließe (Art. 6 (1 lit. f) DSGVO), fehlt es bezüglich der 3. Stufe – Abwägung – an Leitprinzipien, an denen sich die Beteiligten im Abwägungsprozess orientieren könnte. Hier könnte sich ggf. für die Zukunft ein Aufgabenbereich der überwachenden Behörde ergeben, eine Orientierung für das „Legitimate Interests Assessment“ zu schaffen – ggf. in Form von Leitlinien mit Szenarien / Fallbeispielen, die eine Orientierung für den Abwägungsprozess geben.

In der Literatur[167] wird wegen der derzeit eher unklaren Lage zu den Legitimationsgrundlagen ein **Datenvertrag** zwischen dem Dateninhaber und dem Nutzer (im Use Case Nutzer A) vorgeschlagen, welcher Letzteren dazu verpflichtet, das Vorliegen der datenschutzrechtlichen Erfordernisse gegenüber dem Dateninhaber sicherzustellen. Das entbindet zwar den Dateninhaber nicht von seinen datenschutzrechtlichen Pflichten, erlaubt ihm aber im Falle, dass der Nutzer die Festlegungen des Datenvertrags verletzt, diesen im Innenverhältnis in Regress zu nehmen. Auf diese Weise kann er sich von Schadensersatzansprüchen des Betroffenen und/oder Bußgeldern der Marktaufsicht freistellen. Soweit Dateninhaber und Nutzer gemeinsam Verantwortliche sein sollten, sind diese nach Art. 26 (1 S. 2) DSGVO ohnehin dazu verpflichtet, in einer Vereinbarung festzulegen, wer von ihnen welche Verpflichtungen nach der DSGVO zu erfüllen hat (vgl. 9.3.2).

---

166 Steinrötter, GRUR 2023, 216, 226.

167 *Götz/Blöink*, MMR 2024, 451, 454; *Antoine*, CR 2024, 73, 75 Rz. 12 f.; *Baumann/Brunnbauer*, ZD 2025, 132, 137; *Frank/von Imhoff*, RInPrax 2025, 51, 58;

Kernelement eines solchen Datenvertrags wäre daher das Festlegen der datenschutzrechtlichen Rollenverteilung mit der Verpflichtung des Nutzers (im Use Case Nutzer A), das Vorliegen einer datenschutzrechtlichen Rechtsgrundlage gegenüber den (möglicherweise) Betroffenen (z. B. der Einwilligung des Nutzers B) sicherzustellen. Da es sich um ein privatautonomes schuldrechtliches Rechtsverhältnis handelt, kann der Inhalt der Vereinbarung frei ausgestaltet werden. In der Literatur werden – angelehnt an die vertraglichen Vereinbarungen zu Art. 26, 3 und 28) (3) DSGVO – die folgenden Regelungsgegenstände vorgeschlagen:

- Arten der betroffenen personenbezogenen Daten
- Rollen der Beteiligten, insbesondere Dateninhaber, Nutzer und Datenempfänger
- Wahrnehmung von datenschutzrechtlichen Informationsverpflichtungen
- Sicherstellung der Anforderungen aus Art. 6 (1) DSGVO sowie beweissichernde Dokumentation; im Falle einer Interessenabwägung nach Art. 6 (1 lit. f) DSGVO sollte eine Dokumentation zum zugrundeliegenden Legitimate Interests Assessment (LIA) vorhanden sein.
- Umgang mit Widerruf und Löschungsbegehren des Betroffenen
- Haftungsklauseln / -quoten bei Vertragsverletzung

Selbst wenn der Datenvertrag in der Literatur derzeit als „Königsweg“ gilt, besteht die Herausforderung für die am Datentransfer Beteiligten darin, dass es noch keine belastbaren praxistauglichen Vorgaben gibt, an denen sie sich orientieren könnten. Insofern könnte es eine Aufgabe der Überwachungsbehörden sein, Szenarien-orientierte Mustervereinbarungen zu entwickeln und diese online abrufbar zu stellen. Das wäre nicht ungewöhnlich, schließlich hat man auch in anderen Sachzusammenhängen den Unternehmen solche Mustervereinbarungen an die Hand gegeben (z. B. Mustervereinbarung des LfDi BW zur gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO[168] oder des BfDi zur Auftragsdatenverarbeitung[169]).

168 Vgl. https://www.baden-wuerttemberg.datenschutz.de/mehr-licht-gemeinsame-verantwortlichkeit-sinnvoll-gestalten/

169 Vgl. https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Muster/Muster_zur_Auftragsverarbeitung.pdf?__blob=publicationFile&v=2

9.5 Fazit

Die Vorgaben der DSGVO und der Umgang mit personenbezogenen Daten bleiben eine große Herausforderung bei der Etablierung einer europäischen Datenwirtschaft. Daher muss klarer festgelegt werden, wann ein Personenbezug von Daten vorhanden ist und wie man ihn ohne einen Verstoß gegen den DA oder einer – den Zielen des DA zuwiderlaufenden – Flucht in die DSGVO vermeiden kann.

Dabei spielt die Anonymisierung der Daten eine entscheidende Rolle, mit der der Personenbezug von Daten ausgeschlossen werden kann. Allerdings sind die Anforderungen an eine Anonymisierung entsprechend dem geltenden Null-Risiko-Ansatz zu hoch, um als praktikabel zu gelten. Daher scheint ein risikobasierter Ansatz untersetzt mit Hinweisen als vorzugswürdig.

Ferner ist die Dilemmasituation des Dateninhabers bei Überschneiden der Anwendungsbereiche von DA und DSGVO in den Blick zu nehmen, die den Dateninhaber mitunter in eine schwierige Situation bringen, wenn er die Vorgaben beider Rechtsakte zu berücksichtigen hat. Um die widerstreitenden Interessen zu versöhnen, bedarf es zur Weitergabe personenbezogener Daten einer Legitimationsgrundlage. Sofern Nutzer und Betroffener personenidentisch sind, kann bereits das Datenherausgabeverlangen als Einwilligung i.S. des Art. 6 DSGVO angesehen werden. Anderes gilt jedoch, wenn Nutzer und Betroffener personenverschieden sind. In dieser Konstellation bedarf es der Synchronisierung von DA und DSGVO über Rechtfertigungstatbestände. Neben dem Erfüllen eines „berechtigten Interesses“ (Art. 6 (1 lit. f) DSGVO), das hohe Anforderungen an den notwendigen Abwägungsprozess stellt, kann ein Datenvertrag zwischen Dateninhaber und Nutzer helfen. Er kann die Interessen aller Beteiligten (Nutzer, Dateninhaber, Betroffener und Datenempfänger) aufnehmen und austarieren sowie die Verantwortlichkeiten zur Sicherstellung der datenschutzrechtlichen Anforderungen festlegen.

10 Der Schutz von Geschäftsgeheimnissen im Data Act als Spannungsfeld zwischen der Gewährung des Datenzugangs und der Aufrechterhaltung von Innovationsanreizen

Im vorliegenden Kapitel werden die im Data Act getroffenen Regelungen zum Data Sharing von als Geschäftsgeheimnis eingestuften Daten tiefergehend analysiert. Dabei wird untersucht, welche Auswirkungen die im Data Act getroffenen Regelungen auf das Spannungsfeld zwischen der Gewährung des Datenzugangs und der Aufrechterhaltung von Innovationsanreizen hat. In einem ersten Schritt werden dazu die im Data Act getroffenen Regelungen im Umgang mit Geschäftsgeheimnissen vorgestellt. Anschließend wird ausgeführt, wie Geschäftsgeheimnisse definiert sind, welche Eigenschaften sie von verwandten Maßnahmen wie bspw. Patente abheben und welche empirischen Aussagen sich zum Einsatz von Geschäftsgeheimnissen in der Wirtschaft treffen lassen. Dies bildet die Grundlage, um im Folgenden drei Anwendungsherausforderungen des Umgangs mit Geschäftsgeheimnissen gemäß DA herauszuarbeiten und zu analysieren. Zum Schluss wird ein Fazit gezogen und potenzielle Lösungsansätze aufgezeigt.

10.1 Die Rechtsgrundlage im Data Act: Regelungen zum Data Sharing von Geschäftsgeheimnissen

Grundsätzlich gelten gemäß DA auch für Daten, die der Dateninhaber als Geschäftsgeheimnis einstuft, die Datenzugangsrechte der Nutzer. Dies wird im Erw.-Gr 31 des DA explizit ausgeführt:

„[…] Grundsätzlich können Dateninhaber ein Datenzugangsverlangen gemäß dieser Verordnung nicht allein aufgrund dessen ablehnen, dass bestimmte Daten als Geschäftsgeheimnisse gelten, da dies die beabsichtigte Wirkung dieser Verordnung untergraben würde. […]“[170]

Geschäftsgeheimnisse sind also von den Datenzugangsansprüchen ***nicht*** per se ausgenommen. Es gelten jedoch spezifische Regelungen bzw. Anforderungen zum Data Sharing von Geschäftsgeheimnissen, die im Folgenden skizziert werden:

Vereinbarung von TOMs zum Vertraulichkeitsschutz der Geschäftsgeheimnisse

Wie in Art. 4 (6) dargelegt wird, muss beim Teilen der Geschäftsgeheimnisse deren Vertraulichkeit, insbesondere gegenüber Dritten gewahrt bleiben. Dazu sollen Dateninhaber und Nutzer angemessene technische und organisatorische Maßnahmen (TOMs) zum Schutz der Vertraulichkeit der Geschäftsgeheimnisse vereinbaren. Die Weitergabe der Daten durch den Dateninhaber muss erst dann erfolgen, wenn diese Maßnahmen

170 Erw.-Gr. [31] DA.

eingehalten werden. Als mögliche Maßnahmen werden in Art. 4 (6) explizit die in Tabelle 8 dargestellten Maßnahmen genannt.[171]

Tabelle 8: Im DA genannte TOMs mit Nennung möglicher Beispiele

Im DA genannte Maßnahmen	Mögliche(s) Beispiel(e)
Mustervertragsklauseln	Verwendung der offiziellen EU-Musterklauseln, z. B. mit spezifischen Regelungen zur Nutzung, Löschung und Zweckbindung der Daten.
Vertraulichkeitsvereinbarungen	Abschluss eines NDA (Non-Disclosure Agreement) vor Beginn der Datenweitergabe, z. B. mit festen Vertragsstrafen bei Verstoß.
Strenge Zugangsprotokolle	Einrichtung eines rollenbasierten Zugriffssystems mit Zwei-Faktor-Authentifizierung und detaillierten Zugriff-Logs.
Technische Normen	Einsatz von Ende-zu-Ende-Verschlüsselung (z. B. TLS 1.3), Datenverarbeitung nach ISO/IEC 27001 oder Nutzung zertifizierter Cloud-Dienste.
Anwendung von Verhaltenskodizes	Orientierung an einem anerkannten Branchenkodex, z. B. dem „Code of Conduct on Data Sharing in Agriculture“ oder einem internen Datenschutzleitfaden.

Dem Erw.-Gr. (57) ist darüber hinaus zu entnehmen, dass sich die erforderlichen TOMs zum Schutz der Geschäftsgeheimnisse beim Teilen derselben Daten zwischen verschiedenen Datenempfängern nicht unterscheiden sollen. Alle potenziellen Datenempfänger sollen also unter gleichen Bedingungen auf die Daten zugreifen können. Zudem dürfen die TOMs den Zugang zu Daten sowie deren Nutzung für die Datenempfänger und Nutzer nicht einschränken.[172] Die Zugangsrechte zwischen Nutzern und Dritten / Datenempfängern zu Geschäftsgeheimnissen des Dateninhabers unterscheiden sich insofern, als dass Dritte gemäß Art. 5 (9) DA lediglich dann einen Zugangsanspruch auf diese Daten haben, wenn sie für den Zweck der Vereinbarung mit dem Nutzer erforderlich sind.

Aussetzen der Datenweitergabe aufgrund nicht umgesetzter TOMs zum Schutz der Geschäftsgeheimnisse

Kann keine Einigung über die TOMs erzielt werden oder werden die vereinbarten TOMs vom Nutzer nicht adäquat umgesetzt, so dass die Vertraulichkeit der Geschäftsgeheimnisse in Gefahr ist, kann der Dateninhaber gemäß Art. 4 (7) die Weitergabe der als Geschäftsgeheimnis eingestuften Daten verweigern bzw. aussetzen. In diesem Fall muss der Dateninhaber dies dem Datennutzer unverzüglich und inklusive Begründung schriftlich mitteilen. Gleichzeitig muss er die zuständige nationale Aufsichtsbehörde darüber in Kenntnis setzen, welche Maßnahmen nicht vereinbart oder umgesetzt wurden

171 Siehe DA Art. 4 (6).
172 Siehe DA Erw.-Gr. 57.

und wieso daraus ein Risiko für die Vertraulichkeit des Geschäftsgeheimnisses resultiert.[173]

Verweigern der Datenweitergabe aufgrund eines erheblichen wirtschaftlichen Schadens

Wenn trotz möglicher TOMs vom Teilen der Daten für den Dateninhaber ein schwerer wirtschaftlicher Schaden mit hoher Wahrscheinlichkeit zu erwarten ist, kann der Dateninhaber gemäß Art. 4 (8) das Teilen der betreffenden Daten im Einzelfall ablehnen. Durch die Präzisierung in Erw.-Gr. (31), dass mit dem hohen wirtschaftlichen Schaden schwere irreparable wirtschaftliche Verluste einhergehen müssen, um die Weitergabe der Daten zu verweigern, werden die Hürden für das Nutzen dieser Ausnahmeregelung bewusst hoch gelegt. Die Inanspruchnahme dieser Regelung muss durch den Dateninhaber gegenüber dem Datennutzer unverzüglich schriftlich begründet werden. Im Erw.-Gr. (31) wird hier zudem eine direkte Verbindung zum Thema Cybersicherheit hergestellt: Negative Auswirkungen auf diese können als Begründung zur Inanspruchnahme der Ausnahmeregelung herangezogen werden, ebenso wie die Durchsetzbarkeit des Schutzes von Geschäftsgeheimnissen in Drittländern, der Art und des Vertraulichkeitsgrads der verlangten Daten sowie der Einzigartigkeit und Neuartigkeit des vernetzten Produkts (siehe Art. 4 (8) DA).

Die Möglichkeit des Aussetzens bzw. Verweigerns der Datenweitergabe aufgrund unzureichender TOMs oder eines zu erwartenden erheblichen wirtschaftlichen Schadens wird von der EU-Kommission auch als „Trade Secrets Handbrake“ bezeichnet.[174]

Kann vom Teilen der Daten eine Gefahr für die Sicherheit natürlicher Personen ausgehen, indem durch das Data Sharing für bestimmte vernetzte Produkte Sicherheitsanforderungen nicht mehr erfüllt werden können, die (sektorspezifisch) im nationalen oder europäischen Recht kodifiziert sind, kann die Datenweitergabe durch den Dateninhaber ebenfalls verweigert werden – unabhängig davon, ob es sich bei den Daten um Geschäftsgeheimnisse handelt oder nicht. Dies ist die sogenannte „Security and Safety Handbrake“.[175]

Dateninhaber muss ex ante Transparenz über das Anfallen als Geschäftsgeheimnis eingestufter Daten schaffen

Zu den in Art. 3 DA definierten Transparenzpflichten des Dateninhabers gehört, dass dieser vor Abschluss einen Kauf-, Miet- oder Leasingvertrages für ein vernetztes Produkt bzw. verbundenen Dienst dem potenziellen Datennutzer anzeigt, ob und welche Daten, die durch die Nutzung des Produktes / Dienstes generiert werden, vom Dateninhaber als Geschäftsgeheimnis eingestuft werden. Die Einstufung von bestimmten Daten als

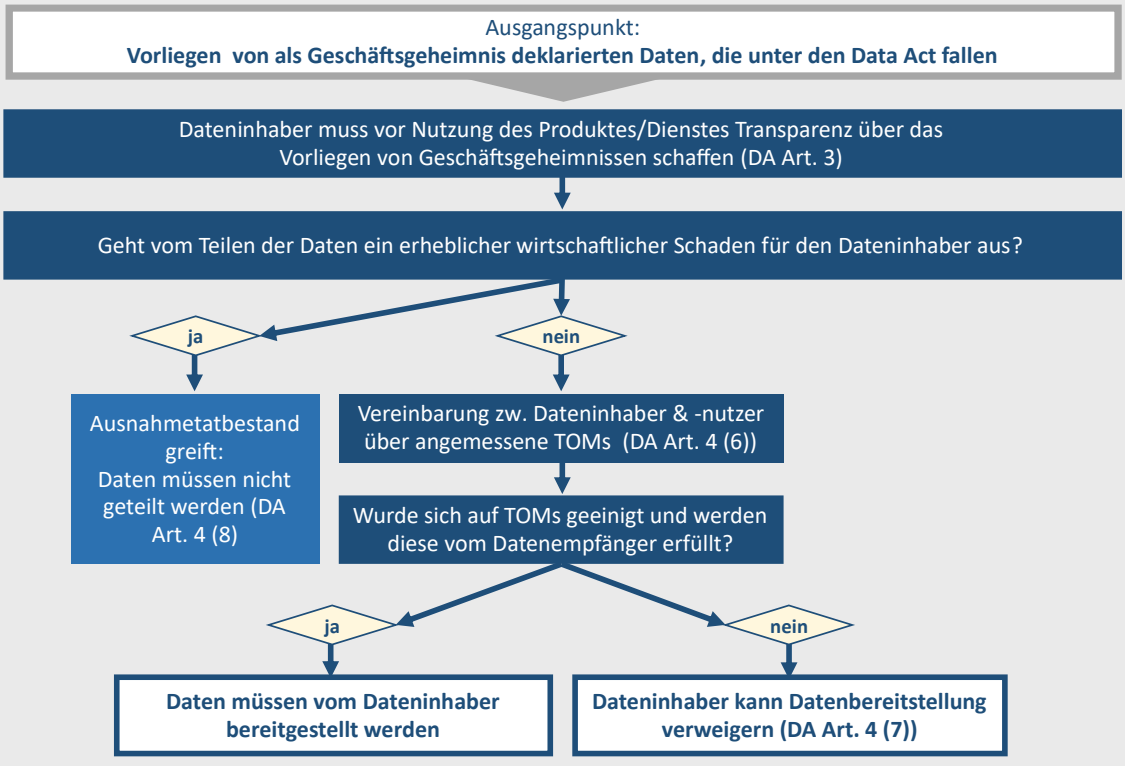
173 Siehe DA Art. 4 (7).
174 Siehe FAQ-Dokument der EU-Kommission zum Data Act.
175 Siehe hierzu Art. 4 (2) DA sowie Frage 25 in den FAQs der EU-Kommission zum Data Act (Version vom 3.2.2025).

Geschäftsgeheimnis muss also ex ante erfolgen und kann nicht ex post, also erst nach dem Anfallen der Daten, geschehen.

Fazit zur Rechtsgrundlage

Zusammenfassend ist die Rechtsgrundlage zum Data Sharing beim Vorliegen von Geschäftsgeheimnissen in Abb. 24 in Form eines Fließdiagramms dargestellt. Es lässt sich festhalten, dass für Datennutzer in der Regel auch Datenzugangsrechte an denjenigen Daten bestehen, die vom Dateninhaber als Geschäftsgeheimnis eingeordnet wurden. Bedingung ist, dass angemessene TOMs zur Sicherstellung der Vertraulichkeit der Geschäftsgeheimnisse ergriffen werden. Ausgenommen von den Datenzugangsansprüchen sind die Daten lediglich, wenn das Teilen der Daten einen irreparablen wirtschaftlichen Schaden beim Dateninhaber verursachen würde oder wenn keine Einigung über die erforderlichen TOMs erzielt wird, bzw. wenn vom Nutzer die vereinbarten TOMs nicht umgesetzt werden oder die Vertraulichkeit der Geschäftsgeheimnisse verletzt wird

Abbildung 24: Schematische Prüfstruktur beim Vorliegen von Geschäftsgeheimnissen



Quelle: Eigene Darstellung.

10.2 Theoretische und empirische Einordnung von Geschäftsgeheimnissen als unternehmerisches Mittel

Da für die Analyse entscheidend ist, wie Geschäftsgeheimnisse definiert sind, welche Charakteristika sie aufweisen und welche empirische Bedeutung sie als unternehmerisches Mittel haben, wird hierauf im vorliegenden Kapitel eingegangen.

10.2.1 Definition von Geschäftsgeheimnissen und daraus folgende Implikationen

Die gemeinsame Grundlage zum Schutz von Geschäftsgeheimnissen in allen WTO-Mitgliedsstaaten wird durch die Verankerung im TRIPS-Abkommen[176] aus dem Jahr 1994 gewährleistet. Dort werden in Art. 39 Geschäftsgeheimnisse als **Informationen** definiert, welche die folgenden drei Anforderungen erfüllen:

- Die Informationen sind **geheim** (d. h. sie sind nicht allgemein bekannt oder allgemein zugänglich)
- Die Informationen haben einen **Wert**, da sie geheim sind.
- Die Informationen werden **angemessen geschützt**.[177]

Auf europäischer Ebene wurden diese Anforderungen an Geschäftsgeheimnisse in die **Trade Secrets Directive** (2016) übernommen, welche im Jahr 2019 mit dem **Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)** in nationales Recht umgesetzt wurde.

In Art. 2 DA wird darauf verwiesen, dass die in der Trade Secrets Directive getroffene Definition von Geschäftsgeheimnissen auch für den DA Gültigkeit besitzt. Demnach gelten die gerade angeführten Anforderungen an ein Geschäftsgeheimnis auch für den Geltungsbereich des DA.

Unterschiede von Geschäftsgeheimnissen im Vergleich zu klassischen Rechten zum geistigen Eigentum

Obwohl Geschäftsgeheimnisse im TRIPS-Abkommen den Rechten zum Schutz geistigen Eigentums zugeordnet werden (IPR – Intellectual Property Rights), unterscheiden sie sich von klassischen IPR (wie bspw. Patente oder Copyright-Schutz). Im Gegensatz zu den klassischen IPR werden durch Geschäftsgeheimnisse keine Eigentumsrechte definiert. Der Schutz beschränkt sich auf die Verhinderung der unrechtmäßigen Aneignung der Informationen durch Dritte.[178] Geschäftsgeheimnisse definieren dementsprechend kein exklusives Recht an den Informationen. So bieten Geschäftsgeheimnisse beispielsweise keinen Schutz vor Reverse Engineering: Gelangen Dritte durch

176 TRIPS steht für *Trade-Related Aspects of Intellectual Property Rights.* Mit dem Abkommen werden Minimalstandards für den Schutz geistigen Eigentums definiert, die von allen WTO-Staaten einzuhalten sind.
177 Siehe Art. 39 TRIPS-Abkommen.
178 Vgl. Radauer (2022).

Untersuchen, Rückbauen oder Testen eines Produktes / Dienstes zu der als Geschäftsgeheimnis klassifizierten Information, ist dies zulässig. Sie lassen aus diesem Grund mehr Raum für Wettbewerb als klassische IPR wie bspw. Patente.[179]

Vorteile von Geschäftsgeheimnissen als unternehmerisches Mittel

Als unternehmerisches Mittel, dass zwischen einem formalen und informalen Schutzmechanismus liegt[180], bedürfen Geschäftsgeheimnisse keiner Registrierung. Im Vergleich zu Patenten ist der administrative Aufwand bei Geschäftsgeheimnissen für das Unternehmen damit deutlich geringer. Es fallen lediglich die Kosten für den angemessen Schutz des Geschäftsgeheimnisses an. Im Gegensatz zu Patenten sind Geschäftsgeheimnisse zeitlich nicht begrenzt und die geschützte Information muss auch nicht offengelegt werden, um den Schutzstatus zu erhalten. Zudem ist die Schwelle für den Schutzstatus geringer als bei klassischen IPR. Sie stellen somit ein sehr flexibles Schutzrecht dar.[181]

Nachteile von Geschäftsgeheimnissen als unternehmerisches Mittel

Der gewichtigste Nachteil von Geschäftsgeheimnissen als unternehmerisches Tool im Vergleich zu anderen klassischen IPR besteht darin, dass der Schutz schwächer ausfällt. Wie weiter oben bereits ausgeführt, stellen sie kein exklusives Recht an den Informationen dar. Es ist zulässig, dass Dritte durch Reverse Engineering oder auch unabhängige Entdeckung an die Informationen gelangen und diese nutzen und dadurch der Status der Information als Geschäftsgeheimnis obsolet wird.[182]

Zudem ist für den Fall, dass eine unrechtmäßige Aneignung der Geschäftsgeheimnisse durch Dritte erfolgt (bspw. durch einen Cyber-Angriff o.Ä.), die rechtliche Durchsetzbarkeit der eigenen Schutzrechte schwieriger. Dies folgt daraus, dass die Informationen vorher geheim waren (und nicht registriert). Es muss also in einem Rechtsprozess zunächst nachgewiesen werden, dass es sich bei den relevanten Informationen um Geschäftsgeheimnisse gehandelt hat[183], was eine weitere Offenlegung der Informationen und damit eine weitere Aufweichung der Vertraulichkeit der Information zur Folge hat. Zudem sind die möglichen Kompensationen für den Inhaber der Geschäftsgeheimnisse bei einem Verletzten der Schutzrechte schwer zu prognostizieren, da hierfür der Wert der unrechtmäßig erlangten Information bestimmt werden muss.[184]

Abschließend zu den Eigenschaften von Geschäftsgeheimnissen erfolgt in Tabelle 9 eine Gegenüberstellung wesentlicher Merkmale mit denen von Patenten um die spezifischen

179 Siehe hierzu GeschGehG, Art. 3, (1), Nr. 2.
180 Vgl. Radauer et al. (2022).
181 Vgl. Mylly (2024).
182 Vgl. Mylly (2024).
183 In Deutschland beträgt gemäß des EUIPO-Reports (2023) der Anteil der Prozesse, die erfolgreich für den Inhaber des Geschäftsgeheimnisses ausgehen, bspw. nur 19% („infringement claim success rate“).
184 Vgl. Searle (2021).

Charakteristika von Geschäftsgeheimnissen als unternehmerisches Mittel plakativ herauszuarbeiten.

Tabelle 9: Gegenüberstellung von Geschäftsgeheimnissen und Patenten

	Geschäftsgeheimnis	Patent
Offenlegung der Information	nein	ja
Dauer des Schutzes	Potenziell unbegrenzt	i.d.R. 20 Jahre
Exklusives Nutzungsrecht	nein	ja
Kosten	Kosten für angemessene Schutzmaßnahmen	Hoher administrativer und finanzieller Aufwand zum Erlangen des Schutzes

Quelle: In Anlehnung an EUIPO (2017).

Ökonomische Logik des Schutzes von Geschäftsgeheimnissen

Der ökonomische Hintergrund des in Rechtsakten verankerten Schutzes von Geschäftsgeheimnissen sowie von IPR allgemein besteht darin, dass man ein innovationsfreundliches Investitionsklima in der Volkswirtschaft schaffen möchte. Durch die staatlich garantierten einzelwirtschaftlichen Schutzrechte für wettbewerbsrelevante Informationen schafft man bei den Unternehmen Anreize, in innovative Lösungen zu investieren. Durch die garantierten Schutzrechte für den Innovator, welche den Wettbewerb einschränken, wird der Erwartungswert der Investitionserlöse erhöht, so dass sich Investitionen schneller amortisieren. Mit den staatlich garantierten Schutzrechten nimmt der Gesetzgeber folglich bewusst statische Ineffizienzen durch die Einschränkung des Wettbewerbs in Kauf, um dynamische Effizienzen durch mehr Innovation in der Volkswirtschaft zu heben.[185]

Die ökonomische Logik dieser Schutzrechte hat demnach die langfristige Entwicklung der Volkswirtschaft im Blick. Wie bereits weiter oben erwähnt, weisen Geschäftsgeheimnisse im Vergleich zu anderen Mitteln wie bspw. Patente eine geringere Schutzintensität auf, dafür ist die Dauer des Schutzes jedoch unbegrenzt.

10.2.2 Empirische Befunde zur Relevanz von Geschäftsgeheimnissen als unternehmerisches Mittel

Um einen Eindruck von der Relevanz von Geschäftsgeheimnissen in der unternehmerischen Praxis zu erhalten, werden im Folgenden Ergebnisse aus empirischen Studien zum Einsatz von Geschäftsgeheimnissen präsentiert.

Geschäftsgeheimnisse sind als Mittel inzwischen weiter verbreitet als Patente

Empirisch lässt sich beobachten, dass die Bedeutung von Geschäftsgeheimnissen als unternehmerisches Mittel im Vergleich zu Patenten zunimmt. Wurden Patente in den

185 Vgl. Searle (2021).

vorangegangenen Jahrzehnten gewissermaßen als der „Goldstandard“ der IPR angesehen, so haben sich Geschäftsgeheimnisse inzwischen als das am weitesten verbreitete Mittel etabliert (siehe hierzu auch Tabelle 10). Als Ausdruck dieses Bedeutungszuwachses von Geschäftsgeheimnissen als unternehmerisches Mittel kann auch gesehen werden, dass sowohl die USA (Defend Trade Secrets Act 2016) als auch die EU (Trade Secrets Directive 2016) und Japan (Unfair Competition Prevention Act 2019) den Rechtsrahmen für Geschäftsgeheimnisse im vergangenen Jahrzehnt maßgeblich angepasst und aktualisiert haben.[186]

Ein möglicher Erklärungsgrund für die dynamische Entwicklung von Geschäftsmodellen als unternehmerisches Mittel ist, dass Geschäftsgeheimnisse flexibler, schneller und kostengünstiger als „klassische“ IPR eingesetzt werden können und somit für eine digitalisierte Wirtschaft mit schnelllebigen Innovationszyklen besser geeignet erscheinen.

Gleichzeitig werden Geschäftsgeheimnisse häufig ergänzend zum Patenschutz eingesetzt. Geschäftsgeheimnisse und Patente stellen also nicht immer Substitute dar, sondern können auch Komplementäre sein. Dies gilt auch insbesondere für eine digitalisierte Wirtschaft, indem man bspw. ein innovatives Produkt als Patent schützen lässt und die dazugehörigen Daten zum Produkt unter den Geschäftsgeheimnisschutz stellt.[187]

Geschäftsgeheimnisse vor allen bei Prozessinnovationen

Dazu passt die empirische Erkenntnis, dass Geschäftsgeheimnisse stärkere Verbreitung bei Prozess- als bei Produktinnovationen finden. Searle (2021) führt hier als mögliche Begründung an, dass im Allgemeinen die Patentierbarkeit von Prozessen schwieriger sei als von Produkten. Zudem sei bei Produkten die Gefahr des Reverse Engineering höher als bei Prozessen, so dass bei Produkten ein stärkerer Anreiz bestehen könnte, diese besser durch Patente zu schützen und somit Reverse Engineering zu verhindern.

Dienstleistungs- und Produktionsbereich als sektorale Schwerpunkte für den Einsatz von Geschäftsgeheimnissen

Da Prozessinnovationen vor allem im Dienstleistungssektor eine wichtige Rolle spielen, sind Geschäftsgeheimnisse als unternehmerisches Mittel in diesem Bereich stark vertreten. Ähnliches zeigt für den Produktionsbereich, wo (patentierte) Produktinnovationen häufig komplementär durch Geschäftsgeheimnisse begleitet werden.[188] Da der Produktionssektor auch für den DA von hoher Relevanz ist, zeigt sich hier die praxisrelevante Bedeutung der Regelungen zum Umgang mit Geschäftsgeheimnissen im DA.

186 Vgl. Searle (2021).
187 Vgl. Radauer et al. (2022).
188 Vgl. Searle (2021).

Unterschiedliche Nutzung und Einschätzung zwischen Groß- und Kleinunternehmen

Richtet man den Blick auf die Größe der Unternehmen, dann zeigt sich, dass Großunternehmen im Vergleich zu KMU sowohl mehr Geschäftsgeheimnisse als auch Patente einsetzen. Auffällig ist dabei, dass der Unterschied zwischen Großunternehmen und KMU bei Patenten deutlich größer ist als bei Geschäftsgeheimnissen (siehe Tabelle 10)

Tabelle 10: Anteil der innovativen Unternehmen in Deutschland, die Geschäftsgeheimnisse oder Patente als unternehmerisches Mittel nutzen

	Geschäftsgeheimnisse	Patente
Großunternehmen	82,4 %	72,8 %
KMU	73,5 %	45,9 %

Quelle: EUIPO (2017).[189]

Eine weitere Studie zeigt, dass Großunternehmen Patente als effektiver als Geschäftsgeheimnisse einstufen. Bei kleinen Unternehmen ist es genau umgekehrt: Hier werden Geschäftsgeheimnisse effektiver als Patente eingestuft. Diese Einschätzung mag daran liegen, dass der administrative Aufwand für Patente für Kleinunternehmen zu hoch ist, so dass Patente als Tool für diese Unternehmen weniger in Frage kommt.[190]

Relativ betrachtet haben Geschäftsgeheimnisse für den Schutz von IPR für kleine und mittlere Unternehmen (KMU) folglich eine größere Bedeutung als für Großunternehmen, da für KMU Patente weniger in Betracht kommen.

Zusammenfassend lässt sich zum empirischen Befund sagen, dass Geschäftsgeheimnisse als unternehmerisches Mittel stark verbreitet in der Wirtschaft sind. Vor allem KMU sind auf dieses Mittel angewiesen, da die Patentanmeldung insbes. für kleinere Unternehmen zu aufwendig und komplex ist. Geschäftsgeheimnisse kommen vor allem bei Prozessinnovationen zum Einsatz. Insbesondere im Produktions- und Dienstleistungsbereich scheinen Geschäftsgeheimnisse als Mittel stark vertreten zu sein.

10.3 Anwendungsherausforderungen im Data Act hinsichtlich des Umgangs mit Geschäftsgeheimnissen inkl. möglicher Lösungsansätze

Nachdem die Regelungen zum Umgang mit Geschäftsgeheimnissen im Data Act aufgezeigt wurden (Kapitel 10.1) und Geschäftsgeheimnisse als unternehmerisches Mittel theoretisch und empirisch eingeordnet wurden (Kapitel 10.2), werden im vorliegenden Kapitel mögliche Anwendungsherausforderungen analysiert, die aus dem Data Act im Umgang mit Geschäftsgeheimnissen resultieren könnten.

189 Da für die Unterscheidung nach Unternehmensgröße nach unserer Kenntnis keine aktuelleren Zahlen vorliegen, muss hier auf eine Quelle aus dem Jahr 2017 zurückgegriffen werden.
190 Vgl. Radauer (2022).

10.3.1 Fragliche Qualifizierung von Rohdaten als Geschäftsgeheimnis

Eine erste Anwendungsherausforderung besteht in der Frage, ob sich die vom DA erfassten Daten überhaupt für die Einordnung als Geschäftsgeheimnis eignen. Die im DA definierten Datenzugangsrechte beziehen sich auf ***Rohdaten*** *(inkl. zugehörigen Metadaten)* sowie ***vorverarbeitete Daten.*** Gemäß Definition der Geschäftsgeheimnisse im TRIPS-Abkommen sowie der Trade Secrets Directive muss es sich beim Schutzgegenstand allerdings um ***Informationen*** handeln (siehe Kapitel 10.1). Die zu klärende Frage ist folglich, ob Rohdaten bzw. vorverarbeitete Daten Informationen darstellen können und sich damit für den Geschäftsgeheimnisschutz qualifizieren.

Rohdaten stellen die fundamentalste Form von Daten dar. Dabei handelt es sich um den direkten Output der Datenquelle, ohne weitere Verarbeitung oder Kontext, bspw. eine bloße Reihe an numerischen Werten.[191] Sie bilden somit den Ursprung der Datenwertschöpfungskette. Erst durch die Kontextualisierung und weitere Verarbeitung bekommen die Daten eine Bedeutung und damit einen steigenden Wert. Der syntaktischen Ebene der Rohdaten (bspw. Numerik) wird durch die Verarbeitung der Daten eine semantische Ebene hinzugefügt.[192] Erst die semantische Ebene, also gewissermaßen die „Verstehbarkeit“ von Daten durch Kontext und ggf. Analyse, macht diese aus wissenschaftlicher Sicht zu einer Information.[193] Rohdaten sind somit isoliert gesehen noch keine Information, sondern eine Vorstufe, woraus folgt, dass sich reine Rohdaten nicht für den Geschäftsgeheimnisschutz qualifizieren.

Dadurch, dass der Gesetzgeber aber explizit Regelungen im Umgang mit Geschäftsgeheimnissen in den DA aufgenommen hat, ist aber davon auszugehen, dass der Gesetzgeber die in den Geltungsbereich des DA fallenden Daten als potenziell schutzwürdig ansieht. Dieser scheinbare Widerspruch wird durch Art. 3 (1) DA abgeschwächt, indem klargestellt wird, dass mit dem Teilen der Rohdaten stets auch diejenigen Metadaten mitgeliefert werden müssen, die zur Interpretation und Nutzung der Daten notwendig sind. Es wird entsprechend der grundlegende Kontext zu den Daten mitgeliefert aber keine Analyse / Auswertung.

Dementsprechend bewegt man sich hier am Übergang zwischen syntaktischer und semantischer Ebene der Daten und damit vom Übergang von losen Daten zu einer Information. Der Data Act trifft folglich keine klare Abgrenzung zwischen Informationen mit potenziellem Geschäftsgeheimnisschutz und (Roh-)Daten bzw. vorverarbeitete Daten ohne Schutzanspruch.[194] Hieraus können sich Konflikte zwischen Dateninhaber und Datennutzer bezüglich der Zugangsbedingungen zu den Daten ergeben. Die durch diese Konflikte resultierenden Transaktionskosten können das Ausschöpfen der mit dem DA verbundenen Wohlfahrtspotenziale schmälern. Dies leitet direkt über zum nächsten

191 Vgl. World Intellectual Property Organisation (2025).
192 Vgl. Fellah (2024).
193 Vgl. Senaratna (2024).
194 Vgl. Mylly (2024).

Anwendungsherausforderung: Die mögliche Überbeanspruchung von Geschäftsgeheimnissen durch den Dateninhaber.

10.3.2 Potenzielle Überbeanspruchung des Geschäftsgeheimnisschutzes durch den Dateninhaber („Overclaiming“)

Eine Anwendungsherausforderung, welche sich aus der nicht ganz eindeutigen Abgrenzung im DA zwischen Information (als potenziell schutzbedürftig) und Daten (als nicht schutzbedürftig) ergibt, besteht darin, dass hierdurch beim Dateninhaber ein Anreiz zur Überbeanspruchung des Geschäftsgeheimnisschutzes resultiert („Overclaiming“).[195]

Die Deklaration von Informationen als Geschäftsgeheimnis hat durch den Dateninhaber selbst zu erfolgen. Dieser hat im Einzelfall zu beurteilen, ob die Anforderungen an ein Geschäftsgeheimnis erfüllt sind. Wenngleich die Beurteilung durch den Dateninhaber selbst aus wettbewerblicher Sicht nicht optimal erscheint, so ergibt sich die Notwendigkeit daraus, dass Geschäftsgeheimnisse per Definition geheim sind. Würde die Einschätzung, ob es sich bei der Information um ein Geschäftsgeheimnis handelt, durch eine andere Partei als den Dateninhaber vorgenommen, wäre dies mit einer Offenlegung der Information / Daten verbunden. Gleichzeitig wäre es für eine Drittpartei auch schwierig zu beurteilen, ob es sich um ein Geschäftsgeheimnis handelt, ohne dass diese Partei Einblick in alle Vorgänge des Unternehmens hat.

Aus dem Umstand, dass der Dateninhaber die Deklaration von Geschäftsgeheimnissen selbst vornimmt, folgt in Kombination mit der nicht eindeutigen Unterscheidung im DA zwischen Daten bzw. Informationen mit und ohne Anspruch auf Geschäftsgeheimnisschutz, dass beim Dateninhaber ein Anreiz besteht, Daten, die unter den Anwendungsbereich des Data Acts fallen, großzügig als Geschäftsgeheimnisse zu erklären. Dies wird als „Overclaiming“ bezeichnet. Die großzügige Auslegung von Daten als Geschäftsgeheimnis ist für den Dateninhaber nur mit geringem Risiko verbunden.[196] Für den Datennutzer erhöht dieses Vorgehen jedoch die Zutrittsschranken zu den Daten, da sich der Zugriff auf die Daten verzögert. Der Datennutzer hat die Wahl, ob er gegen die Einordnung der Daten als Geschäftsgeheimnis qua Beschwerde bei der zuständigen Aufsichtsbehörde bzw. gerichtlich vorgeht oder aber Schutzmaßnahmen ergreift, die vom Dateninhaber verlangt werden.[197] In beiden Fällen steigen die Transaktionskosten für das Data Sharing. Wird dies durch den Datennutzer antizipiert, sinkt bei ihm der Anreiz, seine Datenzugangsrechte überhaupt wahrzunehmen. Die Deklaration von Daten als Geschäftsgeheimnis kann folglich vom Dateninhaber strategisch genutzt werden, um die Kosten des Data Sharing für den Dateninhaber bewusst in die Höhe zu treiben. Dabei ist es unerheblich, wie viele Datenkategorien im Datensatz vom Dateninhaber als Geschäftsgeheimnis eingestuft werden. Sobald mind. eine Datenkategorie im Datensatz

195 Zum Overclaiming, vgl. Aplin et al. (2023) sowie Mylly (2024).
196 Das Risiko für den Dateninhaber besteht in Kosten, die aus einem möglichen Rechtsstreit mit dem Nutzer resultieren können.
197 Greift der Dateninhaber auf den Ausnahmetatbestand des erheblichen wirtschaftlichen Schadens zurück und verweigert so die Weitergabe der Daten gänzlich, bleibt dem Datennutzer nur die Beschwerde bei der zuständigen Aufsichtsbehörde.

als Geschäftsgeheimnis eingestuft wird, müssen vom Nutzer entsprechende TOMs eingehalten werden. Ein weiterer Anreiz für das Overclaiming beim Dateninhaber resultiert daraus, dass ein Geschäftsgeheimnis gemäß TRIPS-Abkommen auch vertraulich / geheim sein muss (siehe Kap. 10.1). Daraus folgt, dass die Möglichkeit, Daten zum Geschäftsgeheimnis zu erklären, verloren geht, wenn man die Daten mit Datennutzern bereits geteilt ohne für diese den Status als Geschäftsgeheimnis in Anspruch zu nehmen.[198] Die Vertraulichkeit als Voraussetzung an ein Geschäftsgeheimnis gemäß TRIPS-Abkommen ist dann nicht mehr gegeben. Volkswirtschaftlich ist zu erwarten, dass diese Anreize zum Overclaiming dazu führen, dass das Ausschöpfen der mit dem DA verbundenen Wohlfahrtspotenziale geschmälert wird , da das Data Sharing weiterhin unter dem volkswirtschaftlich optimalen Niveau verbleibt.

10.3.3 Spielraum bei Angemessenheit der Schutzmaßnahmen (TOMs)

Eine weitere Anwendungsherausforderung der Regelungen im DA zum Umgang mit Geschäftsgeheimnissen besteht darin, die Angemessenheit der technischen und organisatorischen Maßnahmen (TOMs) zu beurteilen, auf welche sich Dateninhaber und Datennutzer im Falle des Data Sharing von Geschäftsgeheimnissen gemäß DA einigen sollen. Zur Angemessenheit der Maßnahmen selbst werden im DA keine weiteren Aussagen getroffen. Es werden lediglich die in Kapitel 10.1 aufgelisteten Musterkategorien für TOMs genannt und es wird klargestellt, dass sich die vom Dateninhaber eingeforderten TOMs für dieselben Daten nicht zwischen verschiedenen Datennutzern unterscheiden dürfen.

Damit ist klar, dass die Beurteilung der Angemessenheit der TOMs keinen Bezug zum konkreten Nutzer bzw. Datenempfänger hat, sondern lediglich zu den Daten selbst, die geteilt werden sollen. Entscheidend für die Beurteilung der Angemessenheit der TOMs ist hier vor allem der Wert der Daten. Dieser ist bei Geschäftsgeheimnissen jedoch schwer zu validieren, da die Daten vertraulich sind.[199] Die Folge ist, dass dem Dateninhaber ein Ermessenspielraum für die Beurteilung der Angemessenheit der TOMs verbleibt. Es ist zu erwarten, dass aus diesen Informationsasymmetrien zuungunsten der Nutzer bzw. Datenempfänger beim Dateninhaber ein Anreiz entsteht, TOMs auf hohem Niveau einzufordern, um so den Datenzugang für den Datennutzer und -empfänger zu erschweren. Dies kann auch als eine Form des „Overclaiming“, hier nun bezogen auf die TOMs, angesehen werden. Der Anreiz wird für den Dateninhaber noch dadurch verstärkt, dass er für alle Datenempfänger die gleichen TOMs für die Daten einfordern muss. Sobald dieser für einen Datenempfänger weniger bzw. schwächere TOMs verlangt, muss er dies auch allen anderen Datenempfängern der gleichen Daten einräumen.

Aus Sicht des Dateninhabers ist das „Overclaiming“ von TOMs besonders effektiv, wenn sich dieses insbesondere auf IT-Sicherheitsmaßnahmen bezieht, da diese für den Nutzer bzw. Datenempfänger aufwendiger und damit kostspieliger umzusetzen sind als bspw.

198 Vgl. Mylly (2024).
199 Vgl. Searle (2021).

Vertraulichkeitserklärungen, etc.. Im Nachteil sind hier dann vor allem KMU, da für diese aufgrund begrenzterer personeller und technischer Kapazitäten die TOMs und hier auch insbesondere die IT-Sicherheitsanforderungen schwieriger umzusetzen sind.[200] Dies könnte darin resultieren, dass vor allem KMU häufiger auf ihre Datenzugangsansprüche verzichten. Dies hätte wiederum Wohlstandseinbußen zur Folge und stände der Intention des DA entgegen.[201]

10.4 Fazit & mögliche Lösungsansätze

Mit der prinzipiellen Inklusion von Geschäftsgeheimnissen der Dateninhaber in die Datenzugangsansprüche der Datenempfänger hat der Gesetzgeber versucht, mögliche Schlupflöcher für Dateninhaber zum Umgehen des Data Sharing zu schließen. Über das Tool der TOMs wird versucht, die Interessen der Dateninhaber und Datenempfänger beim Vorliegen von Geschäftsgeheimnissen auszutarieren. Beim Dateninhaber verbleiben jedoch Ermessensspielräume im Hinblick auf die Deklaration von Geschäftsgeheimnissen sowie die Einforderung von TOMs zum Schutz dieser. Diese Ermessensspielräume entstehen insbesondere dadurch, dass der Dateninhaber aufgrund der Vertraulichkeit der Geschäftsgeheimnisse einen Informationsvorsprung gegenüber den Datenempfängern (und der Aufsichtsbehörde) hat. Grundlage des Ermessensspielraum ist zudem, dass die Vorgaben im Data Act (bzw. in der Trade Secrets Directive) zum Vorliegen eines Geschäftsgeheimnisses als auch zur Angemessenheit der TOMs ausreichend unkonkret sind. Aus diesen Informationsasymmetrien resultiert für den Dateninhaber ein zweifacher Anreiz zum „Overclaiming“: Sowohl im Hinblick auf das Vorliegen eines Geschäftsgeheimnisses selbst als auch in einem weiteren Schritt im Hinblick auf das Einfordern von TOMs. Dieses Overclaiming steht der Intention des Data Act entgegen und ist mit Einbußen des dem DA ausgehenden Wohlfahrtspotenzials verbunden.

Zur Abschwächung der Overclaiming-Problematik kann es zielführend sein, dass der Gesetzgeber Unternehmen, und hier insbes. KMU, bei der Implementierung von TOMs unterstützt, insbes. im Hinblick auf IT-Sicherheitsmaßnahmen. Diese Unterstützung könnte über die Sensibilisierung und den Wissensaufbau durch Innovationszentren bis hin zu Investitionszuschussprogrammen oder vergünstigten Krediten für die notwendigen Investitionen der TOMs reichen. Dies würde die Transaktionskosten der Inanspruchnahme der Datenzugangsrechte senken und Overclaiming als Strategie für den Dateninhaber unattraktiver machen. Gleichzeitig würde mit der Förderung von IT-Sicherheitslösungen in den Unternehmen die Resilienz und Souveränität des Wirtschaftsstandorts Deutschland gestärkt.

200 Vgl. Searle (2021).
201 Zu den Auswirkungen des DA auf KMU siehe auch Märkel et al. (2024).

11 Gesamtfazit

Mit dem DA verfolgt der Gesetzgeber u. a. das Ziel, zu einer verstärkten Mehrfachnutzung von Daten, die durch die Nutzung vernetzter Produkte oder verbundener Dienste anfallen, zu gelangen. Auf diesem Weg soll die Datenökonomie gestärkt und Wohlfahrtspotenziale realisiert werden. Um dies zu erreichen, stärkt der DA die Nutzer von vernetzten Produkten und verbundenen Diensten, indem er für diese Zugangsrechte für die Daten schafft, die durch ihre Nutzung der vernetzten Produkte oder verbundenen Dienste generiert wurden. Gegenwärtig besitzen die Hersteller bzw. Dateninhaber häufig eine de facto-Kontrolle über die Daten. Diese soll durch die im DA verankerten Datenzugangsansprüche für die Nutzer aufgebrochen werden. Gerechtfertigt wird die Stärkung der Position der Nutzer der vernetzten Produkte und verbundenen Dienst damit, dass nicht nur die Hersteller / Dateninhaber (durch die Konzeption der Produkte) sondern auch die Nutzer (durch die Nutzung der Produkte) zur Datengenerierung beitragen.

Ungeachtet der branchenübergreifenden Relevanz des DA als horizontale Regulierung konnte im Rahmen der in dieser Studie durchgeführten empirische Sektorenanalyse gezeigt werden, dass 11 Sektoren vom DA besonders stark betroffen sind. Dabei stechen insbesondere das Verarbeitende Gewerbe und hier insbes. die Bereiche industrielles IoT und Automotive IoT sowie die IKT-Branche und hier insbes. der Bereich Consumer IoT hervor. Daneben weist die Analyse daraufhin, dass auch die Bereiche Energie(versorgung) sowie Verkehr & Lagerei, Handel & Instandhaltung von Kfz sowie der Bereich Landwirtschaft, Forstwirtschaft & Fischerei überdurchschnittlich stark vom DA betroffen sind. Aus dem öffentlichen Sektor kommt insbesondere noch der Bereich Smart City hinzu.

Insgesamt kann auf Basis der European Data Market Study davon ausgegangen werden, dass in Deutschland bis zu 50.000 Unternehmen vom DA betroffen sind. Neben den Sektoren wurde im Zuge der Anbieteranalyse auch eine Stichprobe von 500 als potentiell relevant eingeschätzten Unternehmen in diesen Sektoren näher untersucht. Dabei wurden relevante Unternehmen identifiziert, die sich in den 11 ermittelten Sektoren bewegen. Hierzu wurde sowohl auf qualitative als auch quantitative Indikatoren zurückgegriffen.

Die Analyse ausgewählter möglicher Anwendungsherausforderungen hat exemplarisch anhand der Überschneidung der Anwendungsbereiche des DA und der DSGVO sowie anhand des Umgangs mit Geschäftsgeheimnissen im DA gezeigt, dass mit der Implementierung des DA noch unklare Fragen einhergehen, welche gegebenenfalls die Realisierung der Wohlfahrtspotenziale, die vom DA ausgehen könnten, einschränken können. Hier gilt es, die Implementierung des DA eng zu begleiten und zu beobachten, um bei etwaigen Fehlentwicklungen mit geeigneten Maßnahmen rechtzeitig gegensteuern zu können.

12 Literaturverzeichnis

acatech (2019): „Neue autoMobilität II - Kooperativer Straßenverkehr und intelligente Verkehrssteuerung für die Mobilität der Zukunft.

Allied Market Research (2023). IoT in der Landwirtschaft. https://www-alliedmarketresearch-com.translate.goog/internet-of-things-iot-in-agriculture-market?_x_tr_sl=en&_x_tr_tl=de&_x_tr_hl=de&_x_tr_pto=sc

Apel, S. / Huber, C. (2024): "Das neue Datenrecht in der EU – Eine Übersicht". In: JuS 2024, S. 410ff.

Aplin, T. et al. (2023): The Role of EU Trade Secrets Law in the Data Economy: An Empirical Analysis, *IIC* 54, 826–858

Arioli, M. (2024): "Der EU Data Act: werden damit die «Datenschatztruhen» geöffnet?"; iusnet 15.07.2024; abrufbar unter: https://www.arioli-law.ch/site/assets/files/1178/iusnet_beitrag_eu_data_act_martina_arioli_202407.pdf

Bitkom & Fraunhofer-Institut für System- und Innovationsforschung ISI (2012): Gesamtwirtschaftliche Potenziale intelligenter Netze in Deutschland.

Bitkom (2020). Schon 8 von 10 Landwirten setzen auf digitale Technologien. https://www.bitkom.org/Presse/Presseinformation/Schon-8-von-10-Landwirten-setzen-auf-digitale-Technologien

BMDV (2023): "EU verabschiedet Data Act"; Artikel vom 22.12.2023; abrufbar unter: https://bmdv.bund.de/DE/Themen/Digitales/Digitale-Gesellschaft/EU-Data-Act/eu-data-act.html

BMWK (2023). Digitalisierungsindex: Interaktives IndikatorenTool. https://www.de.digital/DIGITAL/Navigation/DE/Lagebild/Indikatorentool/indikatorentool.html

BMWK (2025). Smart City Navigator. https://www.de.digital/SiteGlobals/DIGITAL/Forms/Listen/Smart-City-Navigator/smart-city-navigator_Formular.html

Bomhard, D. (2024): "Der Anwendungsbereich des Data Act", in: MMR 2024, S. 71ff.

Caburn Telecom (2024). IoT in Germany: Driving Innovation, https://caburntelecom.com/iot-in-germany/; Jäger (2020): Smarte IoT-Lösungen für die Energiewirtschaft.

Crass, D. et. al. (2019): Protecting Innovation Through Patents and Trade Secrets: Evidence for Firms with a Single Innovation; International Journal of the Economics of Business, 26(1), 117–156. https://doi.org/10.1080/13571516.2019.1553291

Dannhausen, E. / Abel, D. (2024): Spotlight auf den Nutzer – Wer ist Anspruchsberechtigter nach dem DA?; in: MMR 2024; S.931ff.

Demary, V. (2022): "Der Data Act – Welchen Rahmen Unternehmen für Data Sharing wirklich brauchen"; IW-Policy Paper 02/2022.

DIGI (2024). IoT im Baugewerbe: Anwendungsfälle und Vorteile. https://de.digi.com/blog/post/iot-in-construction

Eckardt, M. / Kerber, W. (2023): "Property Rights Theory, Bundles of Rights on IoT Data, and the EU Data Act"; in: European Journal of Law and Economics, Vol. 57, Nr. 1-2, S.113-143, Special Issue: The Law and Economics of the Data Economy,

Ehlen, T. / Sebulke, P. (2024): "Der Data Act: Zwischen Markt- und Vertragsgestaltung — Auswirkungen auf die Ausgestaltung von Datenüberlassungsverträgen aus der Perspektive von Nutzern"; in: Computer und Recht. Band 40, Heft 2.

eco – Verband der Internetwirtschaft e. V. und Arthur D. Little GmbH (2020): Die Internetwirtschaft in Deutschland 2020–2025.

eco – Verband der Internetwirtschaft e.V. (2023): „Urban Mobility: Zusammenspiel von IoT und Mobility zur Umsetzung von Mobilitätslösungen – Recap“, abrufbar unter:. https://www.eco.de/news/urban-mobility-zusammenspiel-von-iot-und-mobility-zur-umsetzung-von-mobilitaetsloesungen-recap/.

EU-Kommission (2020): The European Data Market Study 2017-2020. Studie erstellt durch IDC, The Lisbon Council. https://digital-strategy.ec.europa.eu/en/library/results-2017-2020-european-data-market-study

EU-Kommission (2022): Impact Assessment Report – Accompanying the document: Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). Commission Staff Working Document. SWD(2022) 34 final.

EU-Kommission (2023): European Data Market Study 2021-2023 – D2.4 Second Report on Facts and Figures.

EU-Kommission (2024a): “A European Strategy for data”, Version vom 10.10.24; abrufbar unter: https://digital-strategy.ec.europa.eu/de/policies/strategy-data

EU-Kommission (2024b): “Data Act explained”; Version vom 06.09.2024; abrufbar unter: https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained

EU-Kommission (2024c): “Frequently Asked Questions – Data Act”; Version 1.2.

EU-Kommission (2024d): The European Data Market Study 2024-2026. Studie erstellt durch IDC, CARSA, The Lisbon Council. https://digital-strategy.ec.europa.eu/en/library/european-data-market-study-2024-2026.

EU-Kommission (2024e): The European Data Market Study 2024-2026 – EU Data Landscape report. Studie erstellt durch IDC, CARSA, The Lisbon Council. https://digital-strategy.ec.europa.eu/en/library/european-data-market-study-2024-2026.

Etzkorn, P. (2024): (Vertragliche) Datenzugangsansprüche nach dem Data Act RDi 2024, 116, 118.

Expert Market Research (2024): Global Smart Cities Market Size and Share Outlook - Forecast Trends and Growth Analysis Report (2025-2034).

EUIPO (2017): Protecting Innovation through Trade Secrets and Patents: Determinants for European Union Firms; https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/Trade%20Secrets%20Report_en.pdf

EUIPO (2023): „Trade Secrets litigation trends in the EU“; abrufbar unter: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2023_Trade_Secrets_Litigation_Trends_in_the_EU/2023_Trade_Secrets_Litigation_Trends_Study_FullR_en.pdf“

Expert Market Research (2024): Global Smart Cities Market Size and Share Outlook - Forecast Trends and Growth Analysis Report (2025-2034).

Fellah, S. (2024): Unlocking Data Understanding: The Syntax vs. Semantics Challenge; abrufbar unter: https://medium.com/@stephanef/unlocking-data-understanding-the-syntax-vs-semantics-challenge-a4a80bb55075

Fortune Business Insights (2024): Internet of Things (IoT) in Healthcare Market Size, Share & Industry. https://www.fortunebusinessinsights.com/internet-of-things-iot-in-healthcare-market-102188.

Fortune Business Insights (2025). Hardware- und Software-IT-Dienste: Predictive Maintenance Markt. https://www.fortunebusinessinsights.com/de/predictive-maintenance-markt-102104.

Frank, C./ Freifrau von Imhoff, J. (2025): „Die Bereitstellung von Daten im Data Act“, in: RInPrax 2025, 51.

Fraunhofer-Institut für Offene Kommunikationssysteme Fokus (o.J.): Public IoT – Das Internet der Dinge im öffentlichen Raum.

Gkotsis, P. & Puglies, E. & Vezzani, A. (2018): A Technology-Based Classification of Firms: Can We Learn Something Looking Beyond Industry Classifications? Entropy 2.018, 20(11), 887.

Götz, M. (2023): Data Act-Entwurf und Ansprüche auf den Zugang zu Fahrzeugdaten; in: RAW 2023, S.98-104..

Gries, C-I; Tenbrock, S. (2023). Internet of Things (IoT): Vernetzte Geräte und Maschinen im Mittelstand. Eine Erhebung der Mittelstand-Digital Begleitforschung im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz. WIK-Consult. https://www.wik.org/fileadmin/user_upload/Unternehmen/Veroeffentlichungen/Studien/2022/WIK-Kurzstudie_IoT-Internet-of-things.pdf

Grand View Research (2025). Germany Predictive Maintenance Market Size & Outlook. https://www.grandviewresearch.com/horizon/outlook/predictive-maintenance-market/germany.

Happ, M & Hilllebrand, A (2023). CDO-Forum Digitale Kaffeerunde für Digitalisierungsverantwortliche aus deutschen Kommunen, Mai bis Juni 2023. Initiative Stadt.Land.Digital. https://www.de.digital/DIGITAL/Redaktion/DE/Publikation/bericht-zu-den-cdo-foren-mai-juni-2023-stadtlanddigital.html

Human, S. (2019). IoT-Statistiken für Industrie und Bauwesen. Industry of Things Mission Manufacturing. https://www.industry-of-things.de/iot-statistiken-fuer-industrie-und-bauwesen-a-858799/.

Jäger, C. (2020): Smarte IoT-Lösungen für die Energiewirtschaft.

Krämer, J. (2023) “Improving the Economic Effectivness of the B2B and B2C Data Sharing Obligations in the proposed Data Act; in: CERRE (2023): “Data Act: Towards a balanced EU Data Regulation”; S. 37-57.

Locke (2021). IoT im Gesundheitswesen: Anwendungen und Anwendungsfälle. DIGI. https://de.digi.com/blog/post/iot-in-healthcare-applications.

Lommatzsch / Albrecht (2024), Der "Data Act" der EU als Rechtsrahmen für Daten - Überblick über wichtigste Regelungen für Unternehmen, GWR 2024, S. 302ff.

Mittelstand-Digital Zentrum Bau (2021). IoT im Bauwesen. https://www.digitalzentrumbau.de/kos/WNetz?art=News.show&id=954

Mylly (2024): “Trade Secrets and the Data Act”, in: *IIC* **55**, 368–393

PWC (2016). Smart Farming: Landwirtschaft nimmt Vorreiterrolle bei der Digitalisierung ein https://www.pwc.de/de/handel-und-konsumguter/studie-zu-smart-farming-landwirtschaft-nimmt-vorreiterrolle-bei-der-digitalisierung-ein.html

Radauer et al. (2022): Study on the Legal Protection of Trade Secrets in the Context of the Data Economy Final Report, Publications Office of the European Union, 2022.

Rammer, C et al. (2024): Innovationen in der deutschen Wirtschaft: Indikatorenbericht zur Innovationserhebung 2023. ZEW – Leibniz-Zentrum für Europäische Wirtschaftsforschung GmbH.*Martini/ Roeingh,* NJW 2024, 2379.

Ravin (2021). LoRaWAN-Projekte und Use Cases. Urban Digital. https://urban-digital.de/lorawan-projekte-use-cases/.

Report Prime (2025). IoT in der Landwirtschaft Markt. https://www.reportprime.com/de/IoT-in-der-Landwirtschaft-r14249.

Searle, **N. (2021)** "The economic and innovation impacts of trade secrets"; Report for the British Intellectual Property Office, https://op.europa.eu/en/publication-detail/-/publication/c0335fd8-33db-11ed-8b77-01aa75ed71a1/language-en

Senaratna, N. (2024): Data vs. Information - How they are different; abrufbar unter: https://medium.com/on-technology/data-vs-information-d4596dbfcaf8

Statista (2021). Branche im Fokus: Wachstumsmarkt Smarte Mobilität. https://de.statista.com/infografik/25953/umsatz-im-smart-mobility-markt-in-deutschland/.

Statista (2022). Smart Mobility – The future is digital, greener, and more efficient.

Statista (2024a). Internet der Dinge – Deutschland. https://de.statista.com/outlook/tmo/internet-der-dinge/deutschland

Statista (2024b). Internet der Dinge – Deutschland – Umsatz. https://de.statista.com/outlook/tmo/internet-der-dinge/deutschland#umsatz

Statista (2024c). Internet der Dinge – Deutschland – Anzahl IoT-Verbindungen. https://de.statista.com/outlook/tmo/internet-der-dinge/deutschland#volumen.

Statista (2024d). Smart Home – Deutschland. https://de.statista.com/outlook/cmo/smart-home/deutschland.

Statista (2024e). Internet der Dinge – Consumer IoT – Deutschland. https://de.statista.com/outlook/tmo/internet-der-dinge/consumer-iot/deutschland

Statista (2024f). Smart Grid: Das intelligente Stromnetz in Deutschland. https://de.statista.com/themen/1964/smart-grid/#topicOverview

Statista (2024g). IoT im Gesundheitswesen – Deutschland. https://de.statista.com/outlook/tmo/internet-der-dinge/iot-im-gesundheitswesen/deutschland.

Statista (2024h). IoT im Gesundheitswesen – Deutschland – Umsatz. https://de.statista.com/outlook/tmo/internet-der-dinge/iot-im-gesundheitswesen/deutschland#umsatz.

Statista (2024i). Robotics – Germany – Revenue. https://www.statista.com/outlook/tmo/robotics/germany#revenue.

Statista (2024j). Logistik-Servicerobotik – Deutschland. https://de.statista.com/outlook/tmo/robotik/servicerobotik/kommerzielle-servicerobotik/logistik-servicerobotik/deutschland.

Statista (2024k). Marktwert des industriellen Internets der Dinge (IIoT) in der Landwirtschaft weltweit nach Region in den Jahren 2020 bis 2025. https://de.statista.com/statistik/daten/studie/1337452/umfrage/landwirtschaftlich-industriell-internet-der-dinge-weltweit-markwert/.

Statista (2024l). Anteil der wichtigsten technologischen Innovationen am Gesamtmarkt in der Landwirtschaft weltweit im Jahr 2022. https://de.statista.com/statistik/daten/studie/1337057/umfrage/agritech-wichtigste-innovationen-weltweit/.

Statista (2024m). Smart Finance – Germany. https://www.statista.com/outlook/tmo/internet-of-things/smart-finance/germany.

Statista (2024n). Internet der Dinge – Industrielles IoT – Deutschland. https://de.statista.com/outlook/tmo/internet-der-dinge/industrielles-iot/deutschland

Statista (2024o). Internet der Dinge – Smarte Städte – Deutschland. https://de.statista.com/outlook/tmo/internet-der-dinge/smarte-staedte/deutschland

Statista (2025a). Umsatz der Branche Verarbeitendes Gewerbe in Deutschland von 2012 bis 2019 und Prognose bis zum Jahr 2025. https://de.statista.com/prognosen/924735/verarbeitendes-gewerbe-umsatz-in-deutschland.

Statista (2025b). Prognose zur Anzahl der Smart Home Haushalte in Deutschland für die Jahre 2020 bis 2028.https://de.statista.com/prognosen/885611/anzahl-der-smart-home-haushalte-in-deutschland.

Statista (2025c). Anzahl der Carsharing-Fahrzeuge in Deutschland nach Varianten in den Jahren 2014 bis 2025. https://de.statista.com/statistik/daten/studie/219139/umfrage/anzahl-der-carsharing-fahrzeuge-in-deutschland/.

Statista (2025d). Carsharing – Deutschland – Umsatz. https://de.statista.com/outlook/mmo/shared-mobility/carsharing/deutschland#umsatz.

Statistisches Bundesamt (Destatis) (2022). Mehr als jedes dritte deutsche Unternehmen nutzt das Internet der Dinge. https://www.destatis.de/DE/Presse/Pressemitteilungen/2022/01/PD22_035_52911.html#:~:text=Diese%20kommen%20bei%2021%20%25%20der,in%20den%20Tabellen%2052911%20verf%C3%BCgbar.

Statistisches Bundesamt (Destatis) (2025). Input-Output-Rechnung 2021 (Revision 2024; Stand: August 2024). Statistischer Bericht. https://www.destatis.de/DE/Themen/Wirtschaft/Volkswirtschaftliche-Gesamtrechnungen-Inlandsprodukt/Publikationen/Downloads-Input-Output-Rechnung/statistischer-bericht-input-output-rechnung-2180200217005-rev-2024-august-2024.xlsx?__blob=publicationFile&v=2.

Steffen, N., Wiewiorra, L., Kroon, P. (2021): "Wettbewerb und Regulierung in der Plattform- und Datenökonomie"; WIK Diskussionsbeitrag, No. 481.Sylla/Wendlinger (2023). Der Smart Meter Rollout in Deutschland und Europa. FfE. https://www.ffe.de/veroeffentlichungen/smart-meter-rollout-in-deutschland-und-europa/.

Staudenmayer, D. (2024): „Der Data Act im Gefüges des europäischen digitalen Privatrechts"; in: Neue Juristische Wochenschrift (NJW) 2024, S. 1377ff.

Sylla / Wendlinger (2023): „Der Smart Meter Rollout in Deutschland und Europa"; abrufbar unter: https://www.ffe.de/veroeffentlichungen/smart-meter-rollout-in-deutschland-und-europa/.

TU München (2022): Smart Cities in Deutschland 2022. Technologien, Anwendungsfälle und Partizipation.

Weinhold, R. / Schröder, C. (2024): „(R)Evolution oder vergebene Chance - Mehr Wettbewerb in Bezug auf und besserer Zugang zu Daten"; in: Zeitschrift für Datenschutz (ZD) 2024, S. 306ff.

WIK (2023): Energieeffizienz in öffentlichen Liegenschaften steigern: Gute Beispiele für LoRaWAN-Anwendungen.

Wörrle (2024). Smart Meter: Verpflichtender Einbau startet 2025. DHZ Deutsche Handwerks Zeitung. https://www.deutsche-handwerks-zeitung.de/smart-meter-wer-baut-sie-ein-wann-und-warum-ueberhaupt-300206/.