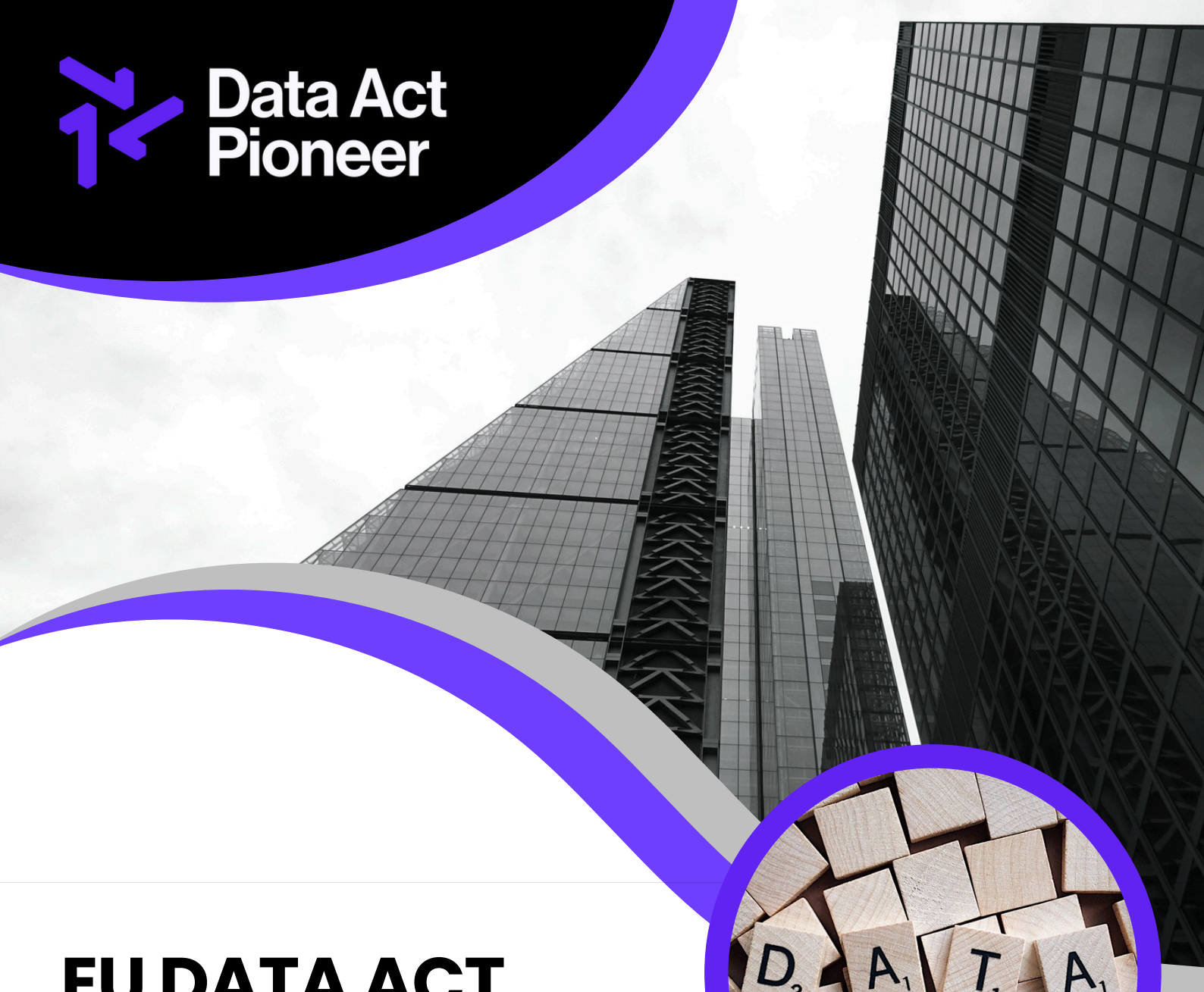
Data Act Pioneer



EU DATA ACT

Auswirkungen, Handlungsmöglichkeiten und Potenziale

29.08.2025

funded by:

Interreg Alpenrhein-Bodensee-Hochrhein

Kofinanziert von der Europäischen Union

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

HTWG Hochschule Konstanz Technik, Wirtschaft und Gestaltung

Zürcher Hochschule für Angewandte Wissenschaften zhaw

OST Ostschweizer Fachhochschule

FHV Vorarlberg University of Applied Sciences

Der EU Data Act – Auswirkungen, Handlungsmöglichkeiten und Potenziale

Ein Whitepaper

im Rahmen des Forschungsprojekts
Interreg VI ABH030 **„Data Act Pioneer“**

Prof. Dr. Marc Strittmatter, Johanna Meyer, LL.B., Eileen Gladis
Hochschule Konstanz Technik, Wirtschaft und Gestaltung (HTWG)

Dr. Jürg Meierhofer, Susana Soriano Ramírez
ZHAW School of Engineering (ZHAW SoE)

Prof. Dr. Petra Kugler
Ostschweizer Fachhochschule (OST)

Dr. Helen Vogt
ZHAW School of Management and Law (ZHAW SML)

Martin Dobler, BSc MSc
Fachhochschule Vorarlberg (FHV)

Veröffentlichungsdatum: 29.08.2025

Management Summary

Der EU Data Act ist ein zentraler Baustein der europäischen Datenstrategie. Er zielt darauf ab, bislang ungenutzte Datenpotenziale für Innovation und Wettbewerb zu erschließen. Im Fokus steht die Schaffung fairer Zugangs- und Nutzungsrechte für Daten. Das neue europäische Regelwerk ordnet die beteiligten Akteure den Rollen Dateninhaber, Nutzer und Datenempfänger (Dritte) zu. Damit schafft der Data Act die Grundlage für eine neue Form der Datenwertschöpfung, stellt Unternehmen jedoch zugleich vor erhebliche rechtliche, technische und strategische Herausforderungen.

Das **Forschungsprojekt „Data Act Pioneer“** analysiert diese Veränderungsdynamiken in vier komplementären Forschungsperspektiven:

1. Rechtliche Rahmenbedingungen und Compliance-Ansätze

Da der Data Act den Vertrag als maßgebliches Steuerungsinstrument für die Datenallokation statuiert, ergeben sich neue Verpflichtungen für Dateninhaber und Datenempfänger z.B. im Hinblick auf Bereitstellungspflichten, technische Gestaltung (Data Access by Design), Informationspflichten und Schutzinteressen. Gleichzeitig treten Zielkonflikte zwischen dem verpflichtenden Datenzugang und dem Schutz von Geschäftsgeheimnissen sowie personenbezogener Daten auf. Während der Data Act den Zugang priorisiert, erlaubt er eine Verweigerung in Fällen unzureichender Schutzmaßnahmen oder drohender wirtschaftlicher Schäden. Zur Umsetzung empfiehlt sich zudem eine unternehmensinterne gestufte Data-Governance-Strategie, bestehend aus Dateninventur, Klassifizierung, rechtlicher Bewertung und Schutzmaßnahmen. Unternehmen sind daher gefordert, die gesetzlichen Datenzugangsansprüche mit ihren Schutzinteressen in ein ausgewogenes Verhältnis zu bringen und zugleich Prozesse zur Risikobewertung und zum Umgang mit potenziellen Sanktionsrisiken umzusetzen.

2. Open Data Innovation

Der Data Act verleiht bislang verschlossenen industriellen Daten einen quasi offenen Charakter und ermöglicht dadurch neue Formen der Innovationspartnerschaft zwischen Dateninhabern, Nutzern und Datenempfängern. Für eine erfolgreiche Nutzung ist jedoch zu klären, welche Datenarten im Ökosystem geteilt werden, wie der neue Datenzugang den Innovationsprozess verändert und welche organisatorischen Voraussetzungen – insbesondere im Bereich Data Literacy – geschaffen werden müssen. Der Schwerpunkt untersucht, wie datengetriebene Innovationen gezielt ermöglicht und potenzielle Hürden abgebaut werden können.

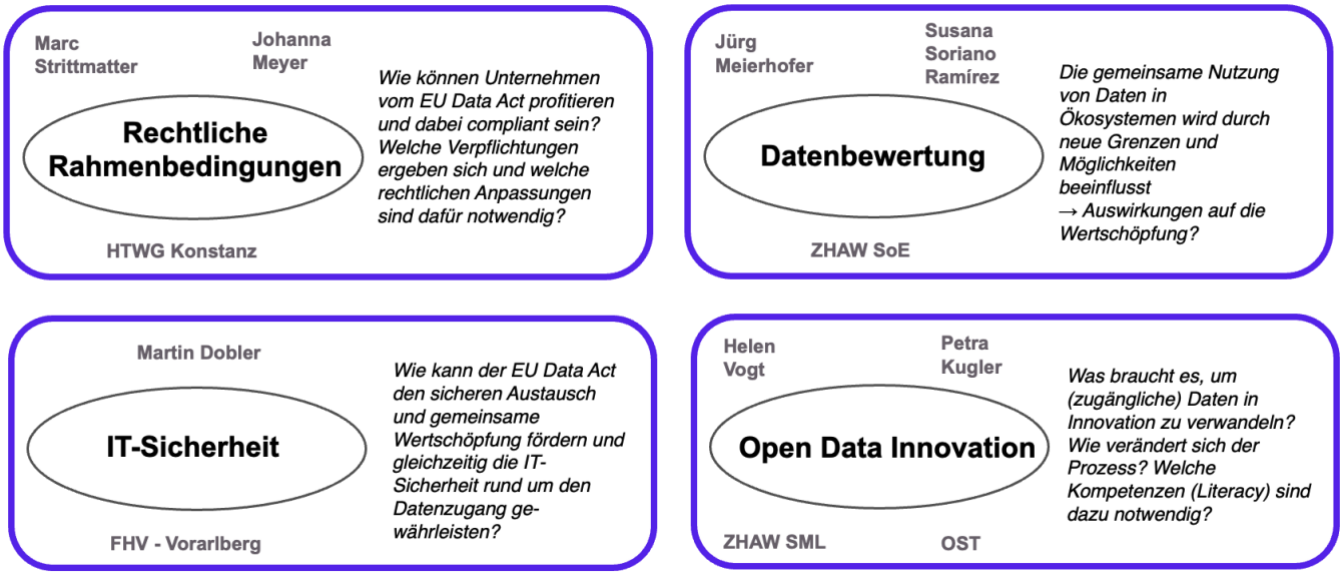
3. IKT-Sicherheit und Schutzmaßnahmen

Der erweiterte Datenzugang geht mit einer Zunahme von Angriffsflächen in industriellen Netzwerken einher. Daher analysiert das Projekt typische Angriffsvektoren im industriellen Umfeld und erarbeitet strategische Sicherheitskonzepte sowie technische und organisatorische Schutzmaßnahmen (TOMs). Darüber hinaus werden neue sicherheitsbezogene Dienstleistungen und Geschäftsmodelle identifiziert, die sich aus dem Data Act heraus entwickeln lassen.

4. Datenbewertung und industrielle Datenwertschöpfung

Durch die neuen Rechte der Nutzer zur Weitergabe industrieller Daten an Datenempfänger entstehen neue Datenwertströme und Marktmechanismen. Dies eröffnet Chancen für effizientere Services durch Drittparteien, erzeugt aber auch neue Wettbewerbs- und Finanzierungsfragen für Dateninhaber. Das Projekt analysiert unter anderem diese ökonomischen Auswirkungen, entwickelt Bewertungsmodelle für Datenzugänge und erarbeitet Vorschläge für faire Vergütungsmechanismen zwischen den beteiligten Akteuren.

Mit diesen vier Forschungslinien zeigt das Projekt „Data Act Pioneer“ umfassende Grundlagen und Ansätze auf, um die Auswirkungen des EU Data Acts ganzheitlich zu beleuchten:



Inhaltsverzeichnis

1 Über dieses Whitepaper

Eine Orientierungshilfe zur Einordnung, Auswirkungsanalyse und Strategien im Umgang mit dem neuen europäischen Rechtsrahmen.

Dieses Paper richtet sich an Unternehmen und Berater, die sich mit einem der ambitioniertesten Digitalgesetze Europas auseinandersetzen wollen und damit vor der Frage stehen: *Was bedeutet der Data Act für unser Unternehmen und unser Geschäftsmodell - wie können wir darauf reagieren und was ist zu tun?*

Ab 12.September 2025 anzuwenden, ist der EU Data Act (nachfolgend: Data Act, Datengesetz) für viele Unternehmen eher ein Sprung ins kalte Wasser. Unklar ist nur, wie tief es ist, wie stark die Strömung sein wird und wer überhaupt auf das Schwimmen vorbereitet ist.

Dieses Whitepaper richtet sich an Unternehmen, insbesondere im produzierenden Gewerbe, die vernetzte Produkte und Dienste im Einsatz haben oder Kunden von Unternehmen sind, deren Produkte und Dienste Daten sammeln. Das Papier soll Verständnis schaffen, Orientierung bieten und die Unternehmen in die Lage versetzen, die zur Implementierung des Datengesetzes relevanten Fragen für sich zu stellen.

Ziel dieses Papers ist es daher, Ansätze zu bieten und unterschiedliche fachliche Perspektiven auf zentrale Fragestellungen zusammenzuführen. Es zeigt erste Herangehensweisen und strategische Überlegungen auf, aus verschiedenen Blickwinkeln, aber mit einem gemeinsamen Ziel: die Handlungssicherheit und Bewusstsein im Umgang mit diesem komplexen, neuen Rechtsrahmen zu erhöhen. Dieses Paper ist ein interdisziplinärer Orientierungsrahmen, der Unternehmen dabei unterstützt, die Tragweite und Komplexität des Data Acts zu erfassen und daraus erste strategische Überlegungen für die eigene Praxis abzuleiten. Es ist kein juristischer Kommentar, kein technischer Leitfaden und keine allgemeingültige Handlungsempfehlung für alle Situationen, die Unternehmen vorfinden werden, die im Anwendungsbereich des Data Act sind. Vielmehr versteht es sich als strukturierte Annäherung an ein hochkomplexes Regelwerk, das in Unternehmen unterschiedlichste Fachbereiche betrifft; von Rechtsfragen und Compliance über IT-Sicherheit und Produktentwicklung bis hin zu Geschäftsmodellanpassung und -entwicklung und Erkenntnissen für die eigene Datenstrategie. Ziel des Whitepapers ist es, das notwendige Bewusstsein für die kommenden Anforderungen zu schaffen, zentrale Begriffe, Mechanismen und Herausforderungen zu beleuchten und praktische Fragestellungen aufzugreifen, die sich jetzt – mit Blick auf den September 2025 – konkret stellen.

Im Laufe dieses Paper werden diese unterschiedliche Forschungsschwerpunkte beleuchtet:

> **Schwerpunkt HTWG Konstanz – Rechtliche Aspekte:** Es sollen die Grundlagen des Data Act und seinen rechtlichen Rahmen nachvollziehbar aufgezeigt werden: von den Anforderungen und Pflichten, die unterschiedliche Akteure betreffen werden, über den Umgang mit Spannungsverhältnissen zwischen Datennutzung und Geschäftsgeheimnisschutz und Datenschutz,

bis hin zu den Auswirkungen auf Data Governance Strukturen im Unternehmen, die wichtig sind, mit dem Data Act umzugehen.

Schwerpunkt ZHAW SML und OST – Open Data Innovation: Es soll die neue gesetzliche Regelung als eine strategische Chance begriffen werden, die den Zugang zu bisher kaum zugänglichen Ressourcen (Daten) ermöglicht und so zu innovativen Geschäftsideen führen kann. Letztlich geht es darum, Daten in innovative Produkte, Services und Geschäftsmodelle zu überführen, um so Vorteile im sich rasch entwickelnden Wettbewerb zu erzielen.

Schwerpunkt FHV Vorarlberg - IT-Security: Es sollen die vielschichtigen Teilbereiche der Cybersicherheit beleuchtet werden, die im Zuge des Data Acts um ein weiteres Spezifikum reicher werden. Es wird daher die strategische Rolle der IT-Sicherheit und das Bedrohungsmanagement behandelt, typische Angriffsvektoren im industriellen Umfeld analysiert und effektive technische sowie organisatorische Schutzmaßnahmen (TOMs) diskutiert. Neue Geschäftsfelder und Dienstleistungen können spezifisch aus den Anforderungen rund um die Sicherheit entstehen.

Schwerpunkt ZHAW SoE – Datenbewertung und Monetarisierung: Es sollen die tiefgreifende Veränderungen des Data Act in der industriellen Datennutzung für die Wertschöpfung aufgezeigt werden: Kunden erhalten neue Rechte, auf Anlagendaten zuzugreifen und diese weiterzugeben. Dadurch entstehen Chancen für externe Dienstleister, effizientere Angebote zu entwickeln und zu monetarisieren. Gleichzeitig ergeben sich Risiken für Hersteller. Vor diesem Hintergrund werden die neuen Datenströme und ihre Auswirkungen auf die Wertschöpfung analysiert. Modelle zur Bewertung wirtschaftlicher Effekte und fairer Vergütung werden erarbeitet.

Das vorliegende Paper baut auf den Erkenntnissen und Diskussionen auf, sowie die im Rahmen der Forschung des Projekts Data Act Pioneer (Interreg ABH 030) in Fachkreisen, Konferenzen und Workshops entstanden sind. Die vielen Rückmeldungen aus Wirtschaft und Wissenschaft haben gezeigt, wie groß der Bedarf an strukturierter Information, fachübergreifender Perspektive und praxisnaher Einordnung dieses Gesetzes ist. Dieses Paper ist ein erster Schritt, dem Bedarf nach Orientierung im Umgang mit dem Data Act zu begegnen. Was zunächst wie eine klare rechtliche Ordnung erscheint, wirft bei näherer Betrachtung zahlreiche Fragen zu den Auswirkungen auf Geschäftsmodelle, Wertschöpfungsketten, Innovationsprozesse und IT-Sicherheitsarchitekturen auf; zugleich eröffnet die Verordnung auch neue Chancen für den Markteintritt neuer Akteure.

2 Die wichtigsten Eckpunkte, Ziele und Mechanismen des EU Data Act

2.1 Von ungenutzten Potenzialen zu neuen Pflichten

Bis zu 80 Prozent der Maschinendaten, die in vernetzten Geräten, IoT-Systemen und Produktionsanlagen anfallen, bleiben bislang weitestgehend ungenutzt (*European Kommission, 2023; Podszun/Pfeifer, 2023)*. Das liegt nicht nur an technischen Hürden, sondern vor allem an fehlenden rechtlichen Rahmenbedingungen für den Zugang und die Nutzung dieser Daten *(Specht-Riemenschneider, 2023).*

Der EU-Gesetzgeber hat sich bereits weit über ein zwingend gebotenes Maß hinaus in ein *„market design"* begeben *(Strittmatter et al.).* Der Rechtsrahmen wird so eine erhebliche Weiterentwicklung erfahren. Der Data Act zielt darauf ab, bestehende Datensilos aufzubrechen, um den Zugang zu und die gemeinsame Nutzung von Daten zu erleichtern und damit neue Innovations- und Wertschöpfungsmöglichkeiten in der digitalen Wirtschaft zu schaffen *(Heinzke, 2023).* Während in den vergangenen Jahren der Fokus auf dem Schutz personenbezogener Daten lag, etwa durch die DSGVO, schafft der Data Act erstmals einen umfassenden gesetzlichen Rahmen für den Zugang zu und die Weitergabe von nicht-personenbezogenen Daten.

Daten unterscheiden sich grundlegend von physischen Gütern: Anders als etwa ein mechanisches Bauteil, können sie gleichzeitig und mehrfach verwendet werden und das für verschiedenste Zwecke und ohne Qualitätsverlust. Zudem lassen sich Daten beliebig oft vervielfältigen, ohne dass sie sich abnutzen oder verbrauchen. Hier setzt der EU Data Act an und markiert einen Paradigmenwechsel in der europäischen Datenpolitik *(Hennemann et al., 2025).* Auf diese zentrale Eigenschaft digitaler Güter weist der europäische Gesetzgeber bereits im ersten Erwägungsgrund des Data Act hin. Gleichzeitig wird in der Nutzung von Daten ein erhebliches Potenzial für Innovation, Wettbewerbsfähigkeit und nachhaltiges Wirtschaftswachstum gesehen. Vor diesem Hintergrund verfolgt der Data Act das Ziel, eine *„optimale Verteilung der Daten zum Nutzen der Gesellschaft"* zu ermöglichen *(Erwägungsgrund 2 Data Act).*

Insbesondere Unternehmen im produzierenden Gewerbe und datengetriebene Geschäftsmodelle werden von den neuen Regelungen betroffen sein; sei es als Anbieter, Nutzer oder Verwalter von Maschinendaten. Dazu wird im Folgenden der Anwendungsbereich näher beleuchtet.

Am 6. September 2024 veröffentlichte die EU-Kommission ein erstes FAQ-Dokument zum Data Act, um der Praxis auch nach dessen Inkrafttreten Orientierung zu geben. Die am 3. Februar 2025 vorgelegte aktualisierte Fassung sieht inzwischen 74 Einzelfragen vor, die insbesondere Erläuterungen zur Reichweite und den Anwendungsbereich zentraler Verordnungsvorschriften betreffen *(vgl. PM der EU-Kommission v. 6.9.2024, abrufbar unter: https://digital-strategy.ec.europa.eu/de/library/commission-publishes-frequently-asked-questions-about-data-act*).

2.2 Gegenstand und Anwendungsbereich

Art. 1 Data Act beschreibt den Gegenstand und den Anwendungsbereich des Datengesetzes. Die Vorschrift differenziert dabei zwischen Regelungsschwerpunkten, erfassten Daten und Adressaten, bzw. Akteure im Spielfeld des Data Act. An dieser Stelle werden auf die unterschiedlichen Datenarten und damit einhergehende Datenbegriffe eingegangen, um diese besser einordnen zu können.

Der umfassende Begriff „Daten" des Data Act:

Im Kern adressiert der Data Act **nicht-personenbezogene Daten**. Dabei handelt es sich um alle Arten von Daten, die keine Rückschlüsse auf natürliche Personen zulassen. Dazu gehören vor allem Daten, die durch den Betrieb von vernetzten Geräten im **Internet der Dinge (IoT)** generiert werden. Diese Daten können sowohl Rohdaten als auch vorverarbeitete Daten umfassen, die direkt oder indirekt durch den Betrieb der Geräte erzeugt werden.

Darüber hinaus regelt der Data Act den Zugang zu bestimmten **personenbezogenen Daten**, sofern diese im Rahmen von nicht-personenbezogenen Datensätzen verarbeitet werden. In solchen gemischten Datensätzen, die sowohl personenbezogene als auch nicht-personenbezogene Daten enthalten, gilt weiterhin der Datenschutz der DSGVO.

Der Data Act richtet jedoch besonderes Augenmerk auf Daten, die im Zusammenhang mit **vernetzten Produkten** *(vgl. Art. 2 Nr. 5 Data Act)* und damit **verbundenen Diensten** *(vgl. Art. 2 Nr. 6 Data Act)* entstehen. Diese Produkte reichen von Maschinen in der industriellen Fertigung über intelligente Haushaltsgeräte bis hin zu vernetzten Fahrzeugen *(Erwägungsgrund 14 Data Act).* Demnach sind Daten im Sinne des Data Act etwa Daten zur Leistung (z.B. Reichweite), Nutzung (z.B. Tageszeiten, Insassen während der Fahrt) oder Umgebung (z.B. Standorte, Temperatur). Festhalten lässt sich: Sobald solche Produkte Daten generieren, z.B. durch entsprechende Sensoren, stellt sich die Frage, wer diese Daten nutzen darf.

Die vom Data Act erfassten Daten lassen sich wie folgt einteilen:

- **Daten aus vernetzten Geräten:** Daten, die von Maschinen, Fahrzeugen oder IoT-Geräten gesammelt werden und Einblicke in deren Nutzung oder Zustand ermöglichen.
- **Daten aus verbundenen Diensten:** Daten, die durch Dienste erfasst werden, die mit vernetzten Produkten interagieren, beispielsweise im Rahmen von Wartungs- oder Optimierungsprozessen.
- **Maschinell erzeugte Daten:** Hierbei handelt es sich vor allem um Daten aus Produktionsprozessen, die zur Steigerung der Effizienz und zur besseren Zusammenarbeit entlang der Wertschöpfungskette genutzt werden können.

Der Data Act regelt unter anderem die Bereitstellung von Produktdaten und verbundenen Dienstdaten für den Nutzer des vernetzten Produkts oder verbundenen Dienstes, die Herausgabe von Daten durch den **Dateninhaber** für **Datenempfänger (Dritter)** und die Einführung von Schutzmaßnahmen gegen den

unrechtmäßigen Zugang Dritter zu nicht-personenbezogenen Daten und Maßnahmen zum Schutz von Geschäftsgeheimnissen *(s. dazu 3.1.2 u. 3.1.3).*

Um KMU nicht übermäßig zu belasten, nimmt der Data Act Kleinst- und Kleinunternehmen grundsätzlich von den Pflichten des Kapitels II der Verordnung aus, sofern sie vernetzte Produkte entwickeln oder verbundene Dienste anbieten.

Die Ausnahme greift allerdings nur, wenn diese Unternehmen keine weiteren Partner- oder verbundenen Unternehmen haben, die nicht selbst als Kleinst- oder Kleinunternehmen gelten.

Auch mittlere Unternehmen genießen einen zeitlich befristeten Schutz: Werden sie erst seit weniger als einem Jahr als mittlere Unternehmen eingestuft, gelten die Pflichten ebenfalls noch nicht. Darüber hinaus gilt für von mittleren Unternehmen in Verkehr gebrachte Produkte, dass die entsprechenden Pflichten erst ein Jahr nach der Markteinführung greifen *(Hennemann & Steinrötter, 2022; Schreiber et al. 2024).*

Diese drei Hauptakteure *(s. dazu ausführlich 3.1.3)* und der Daten-Zugangsmechanismus des Data Act werden im folgenden Grundschema deutlich:

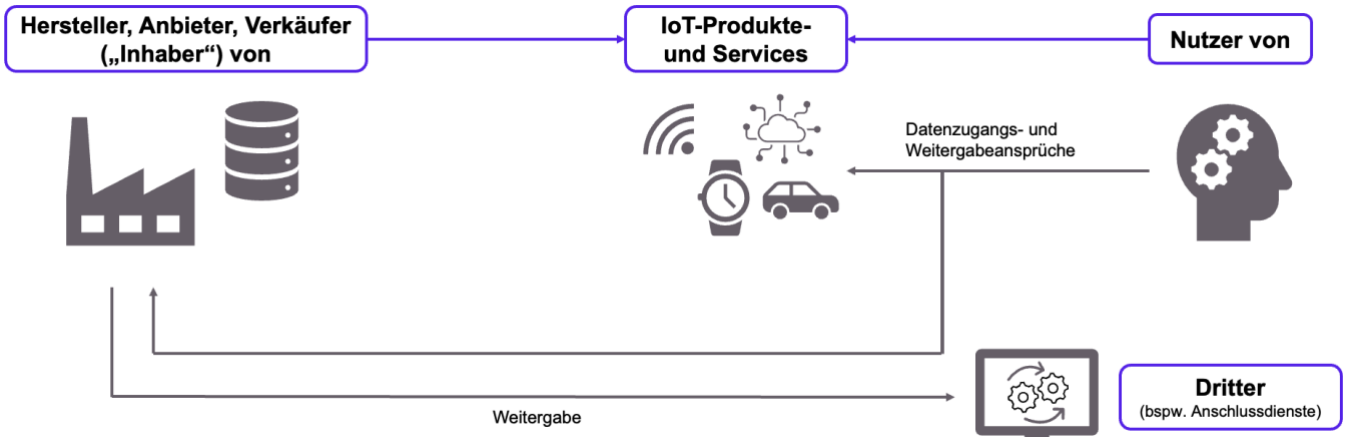


Abbildung 2

Vereinfachtes Schema: Datenzugangsmechanismus des Data Act, mit den wesentlichen drei Rollen: Dateninhaber, Nutzer und Datenempfänger (Dritter)

Beispielhafter Anwendungsfall:

Ein Agrarunternehmen nutzt vernetzte Landmaschinen eines Herstellers, die während des Betriebs kontinuierlich Daten über Bodenqualität, Maschinenleistung oder Umwelteinflüsse erfassen. Wenn diese Daten vom Hersteller erfasst oder ausgelesen werden, liegen diese Daten zunächst in der Sphäre des Herstellers; er ist Dateninhaber im Sinne des Data Act (Art. 2 Nr. 13 Data Act).

Da das Agarunternehmen durch die Nutzung der Maschine diese Daten generiert, steht ihm ein Datenzugangsrecht (Art. 4 Data Act) zu. Er kann außerdem verlangen, dass diese Daten einem Dritten, z.B. einem spezialisierten Anbieter für agrarische Datenanalyse, übermittelt werden, um darauf aufbauend beispielsweise präzisere Ernteprognosen oder Düngeempfehlungen zu erhalten.

Dieses Zusammenspiel verdeutlicht den zentralen Mechanismus des Data Act: Die faktische Kontrolle über Daten bleibt beim Dateninhaber, die dispositive Entscheidungsmacht über deren Weitergabe liegt jedoch beim Nutzer. Der Dritte hat die Möglichkeit, an für sein Geschäftsmodell strategisch wertvolle Daten zu gelangen.

2.3 Marktortprinzip des Data Act

Das Marktortprinzip in Art. 1 Data Act stellt sicher, dass sich die Anwendbarkeit der Verordnung nicht nach dem Sitz der beteiligten Akteure, sondern nach dem Ort der Nutzung oder Bereitstellung richtet. Entscheidend ist danach, ob vernetzte Produkte, verbundene Dienste oder damit zusammenhängende Daten in der Europäischen Union angeboten oder genutzt werden. Damit unterwirft der Data Act auch außereuropäische Anbieter den europäischen Regeln, sofern ihre Leistungen auf den EU-Markt ausgerichtet sind. Das Marktortprinzip trägt somit maßgeblich zur Reichweite des Data Act bei und schützt den europäischen Datenraum vor regulatorischen Schlupflöchern *(Specht-Riemenschneider et. al. 2025).* Das Marktortprinzip liegt z.B. auch der Datenschutzgrundverordnung (DSGVO) zugrunde.

Durch dieses Prinzip wird festgelegt, dass auch Dateninhaber und Anbieter entsprechender Dienste mit Sitz außerhalb der Union, wie etwa in der Schweiz, vom Anwendungsbereich des Data Act erfasst werden, sofern ihre Angebote auf den europäischen Markt abzielen *(Strittmatter et al. 2024; Weinhold et al. 2024).* Offen bleibt jedoch, wessen Handlung für das Inverkehrbringen des Produkts in der EU maßgeblich ist und ob die Pflichten bereits dann Anwendung finden, wenn ein Dritter das Produkt ohne Kenntnis des Herstellers in Verkehr gebracht hat.

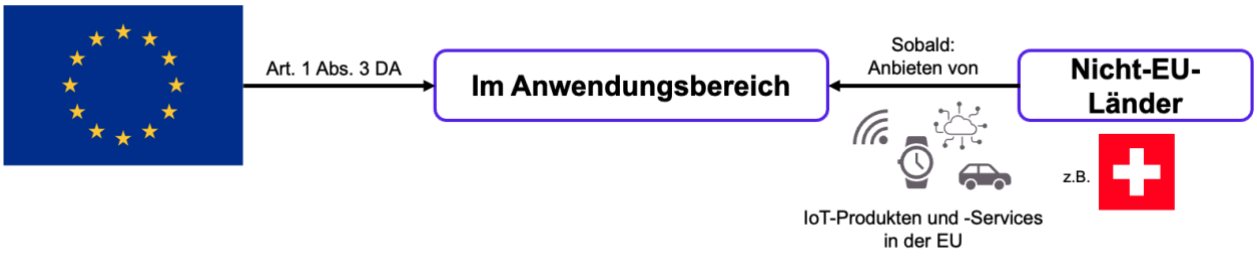


Abbildung 2

Visualisierung und Länderbeispiel des Marktortprinzips des Data Act

3 Die unterschiedlichen Perspektiven des Forschungsprojekts „Data Act Pioneer“

Das Forschungsprojekt „Data Act Pioneer“ erforscht die zentralen regulatorischen Neuerungen des EU Data Act und deren Auswirkungen auf datengetriebene Unternehmen in unterschiedlichen Disziplinen: Darunter rechtliche Aspekte, Verpflichtungen und Auswirkungen auf Data Governance Strukturen, Open Data Innovation, Datenmonetarisierung und IT-Sicherheit.

Durch die Neudefinition von Zugangs- und Nutzungsrechten an Daten fördert der Data Act die Entwicklung neuer Geschäftsmodelle, Produkte und Services, stellt jedoch zugleich erhebliche Herausforderungen in diesen Bereichen dar.

Das Forschungsprojekt konzentriert sich bewusst auf vier zentrale Perspektiven. Das Besondere an dieser Initiative ist es, dass der Data Act nicht allein aus juristischer Sicht beleuchtet wird, sondern weitere Aspekte und unterschiedliche Forschungsdisziplinen einbezogen werden.

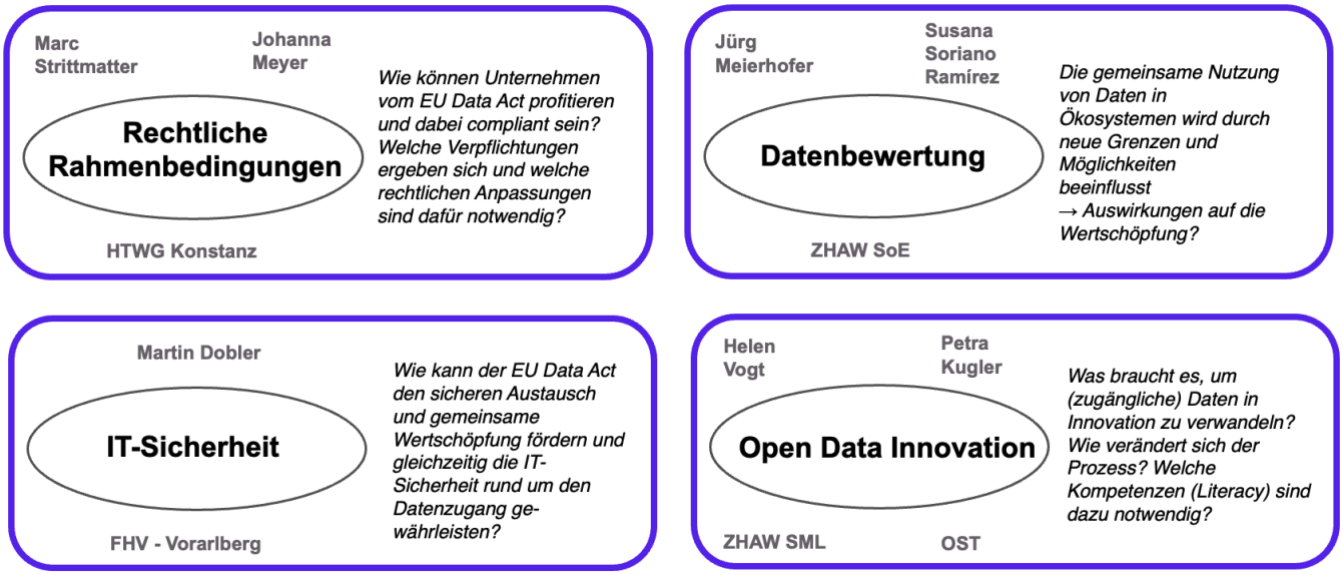


Abbildung 3

Forschungspartnerinnern und Forschungspartner und deren Forschungsschwerpunkte

Wer die damit verbundenen Potenziale nutzen und Risiken einschätzen will, muss also verschiedene Perspektiven zusammenführen: rechtlich, wirtschaftlich, technisch und innovationsbezogen. Ausführungen in nachfolgender Tabelle.

Forschungsperspektive	**Erläuterung**
Rechtliche Aspekte und wichtige Felder der Data Governance (Kapitel 3.1)	Dieses Teilprojekt analysiert sowohl den aktuellen Stand in Unternehmen; im Hinblick auf das Bewusstsein und Vorbereitung auf die Anforderungen des Gesetzes, als auch die Maßnahmen, die ergriffen werden sollten, um bis zur Anwendung des Data Act (12.09.2025) gerüstet zu sein. Zu dieser Forschungsperspektive gehört etwa die Anpassung und Weiterentwicklung von Vertrags- und unternehmensinterne Data Governance Prozesse. Zudem werden die Spannungsfelder beleuchtet, die sich zwischen dem verpflichteten Datenzugang und dem Schutz von Geschäftsgeheimnissen, datenschutzrechtlichen Anforderungen, und wettbewerbsrechtliche Aspekte aufbauen.
Open Data Innovation (Kapitel 3.2)	Das Teilprojekt fokussiert sich auf die Chancen, die sich aus dem nun möglichen Zugriff auf bisher kaum zugängliche Daten ergeben, um innovative Produkte, Services und Geschäftsmodelle zu generieren und so Vorteile im Wettbewerb zu erzielen. Was braucht es dazu, welche Hindernisse müssen überwunden werden? Vor diesem Hintergrund ist zu erwarten, dass sich sowohl der Innovationsprozess als auch die dafür erforderlichen Kompetenzen (Literacy) verändern werden, unklar ist jedoch noch, wie.
IKT-Sicherheit (Kapitel 3.3)	Dieses Teilprojekt befasst sich mit den vielschichtigen Aspekten der Cybersicherheit. Es werden die strategische Beratung und das Bedrohungsmanagement beleuchten, typische Angriffsvektoren im industriellen Umfeld analysiert und effektive technische sowie organisatorische Schutzmaßnahmen (TOMs) diskutiert. Zudem wird ein Blick auf die Entwicklung neuartiger Dienstleistungen und Geschäftsmodelle unter dem Aspekt Sicherheit geworfen.
Datenbasierte Wertschöpfung (Kapitel 3.4)	Das Teilprojekt fokussiert sich auf die Auswirkungen des EU Data Acts auf die industrielle Wertschöpfung basierend auf Daten. Durch neue Nutzungsrechte für Kunden an ihren Anlagendaten entstehen Potenziale für innovative Dienstleistungen durch Drittanbieter. Gleichzeitig stellen sich Fragen nach fairer Vergütung und wirtschaftlichen Effekten für Hersteller. Welche neuen Wertesströme entstehen, wie lassen sie sich bewerten und welche Modelle sind dafür geeignet? Ziel ist es, die Chancen und Herausforderungen dieser regulatorischen Veränderungen in Bezug auf Wertschöpfung systematisch zu analysieren und zu quantifizieren.

Tabelle 1: Vier Forschungsperspektiven im Zusammenhang mit den Herausforderungen und Chancen des EU Data Act

3.1 Der Rechtsrahmen des Data Act

Spannungsfelder zwischen Datenzugang im Verhältnis zum Schutz von Geschäftsgeheimnissen und personenbezogenen Daten

Zusammengefasst: Der Data Act ist ein zentraler Baustein der europäischen Datenstrategie. Er zielt auf die Schaffung fairer Zugangs- und Nutzungsrechte für Daten, insbesondere im industriellen und IoT-Bereich, ab. Ein Eigentumsrecht an Daten besteht nicht, jedoch ergeben sich Schutzpositionen aus dem Datenbankrecht, dem Geschäftsgeheimnisschutz sowie aus vertraglichen Regelungen. Durch den Data Act wird der Vertrag das maßgebliche Instrument der Datenallokation werden. Dazu definiert der Data Act unterschiedliche Rollen: Es gibt Dateninhaber (das wird oft der Hersteller oder Anbieter vernetzter Produkte sein, jedoch werden Hersteller und Dateninhaber nicht immer identisch sein), Nutzer (Inhaber oder berechtigte Verwender) und Datenempfänger (Dritte, die Daten vom Nutzer erhalten). Für Dateninhaber gelten umfangreiche Pflichten bezüglich Bereitstellung, technischer Gestaltung („Data Access by Design"), Informationspflichten, Vertragsbindung und Schutzinteressen. Auch der Dritte unterliegt Verpflichtung aus dem Data Act.

Zentrale Spannungsfelder bestehen zwischen dem vom Data Act festgelegten verpflichtenden Datenzugang und Aspekten von Geschäftsgeheimnisschutz und Datenschutz. Während der Data Act den Zugang priorisiert, erlaubt er in Fällen von unzureichenden Schutzmaßnahmen oder drohenden schweren wirtschaftlichen Schäden eine Verweigerung. Wenn personenbezogene Daten mit Daten des Data Act zusammenfallen, gilt der Vorrang der DSGVO. Unklare Abgrenzungen zwischen personenbezogenen und nicht-personenbezogenen Daten schaffen jedoch praktische Risiken.

Für die Umsetzung empfiehlt sich eine gestufte Data-Governance-Strategie: Dateninventur und Klassifizierung, rechtliche Bewertung und Schutzmaßnahmen für sensible Datensätze sowie strategische Ausgestaltung der Zugangsarten. Zudem sehen sich Unternehmen vor die Entscheidung gestellt, welche Compliance-Strategie sie einschlagen möchten.

3.1.1 Ausgangspunkt: Fragen des Rechtsschutzes für Daten

Die Debatte um den Schutz von Maschinendaten und Datenpools hat über lange Zeit die rechtswissenschaftliche Diskussion geprägt. Inzwischen ist sie jedoch weitgehend abgeklungen, da der europäische Gesetzgeber bewusst auf die Einführung eines Eigentumsrechts an Daten verzichtet und sich mit dem Data Act stattdessen auf die Einführung von **Datenzugangs- und Nutzungsregelungen** geeinigt hat *(Wiebe, 2023; Hennemann & Steinrötter, 2024; Strittmatter, 2025)* Damit hat er sich gleichzeitig auch von der Idee eines Ausschließlichkeitsrechts an Daten, z.B. in der Rechtsfigur des Dateneigentums, verabschiedet *(Weiden, 2022; Denga, 2024).*

Die rechtliche Einordnung von Daten sowie die Bewertung der gesetzlichen Schutzmöglichkeiten bleiben eine Herausforderung der Datenökonomie, denn die **Schutzpositionen an Daten** sind begrenz: Daten sind keine Sachen im Sinne des § 90 BGB und gelten somit als immaterielle Güter. Als Computerprogramme nach § 69a UrhG oder als urheberrechtlich geschützte Datenbankwerke nach § 4 Abs. 2 UrhG scheiden sie regelmäßig aus. Strukturierte Datensammlungen können jedoch unter bestimmten Voraussetzungen als Datenbanken im Sinne des § 87a UrhG anerkannt werden. Der Schutz

erstreckt sich dabei auf die Struktur der Datenbank selbst (das sogenannte Datenbankherstellerrecht) und nicht auf die einzelnen darin enthaltenen Daten *(Antonie, 2024)*.

Voraussetzung für diesen Schutz ist eine wesentliche Investition in die Beschaffung, Überprüfung oder Darstellung der Inhalte; Investitionen in die reine Generierung der Daten führen hingegen nicht zu einem Schutzrecht *(vgl. EuGH, Urt. v. 09.11.2004 – C-444/02, GRUR 2005, 254; vgl. zur Schöpfungshöhe: EuGH, Urt. v. 01.03.2012 - C-604/10, GRUR 2012, 386)*. Ein strafrechtlicher Schutz bezieht sich nicht auf die Daten selbst, sondern primär auf deren Integrität und auf den Schutz vor unbefugtem Zugriff. Ähnlich verhält es sich im Geschäftsgeheimnisschutz: Hier steht der Zugangsschutz im Vordergrund, der durch eine Kombination technischer, organisatorischer und rechtlicher Maßnahmen gewährleistet wird (*Grützmacher, 2024; s. dazu ergänzend Kapitel IKT-Sicherheit 3.3.4).*

In der EU, insbesondere in Deutschland, Österreich und Schweiz, existieren keine Eigentumsrechte an einzelnen Daten, Datensätzen und unstrukturierten Datensammlungen. Da der gesetzliche Schutz insgesamt lückenhaft bleibt, ist der Vertrag das maßgebliche Instrument zur Regelung der Datennutzung (*Wiebe, 2023; Denga, 2024)*. Das führt der Data Act mit seinen Regelungen zur vertraglichen Gestaltung und der Pflicht, Daten nur auf Basis von Datenlizenzverträgen zugänglich und nutzbar zu machen, fort *(Schmidt-Kessel, 2024).*

3.1.2 Einordung des Data Act in die europäische Datenstrategie

Mit ihrer ambitionierten Datenstrategie und einer Vielzahl neuer Rechtsakte hat sich die Europäische Union das ehrgeizige Ziel gesetzt, einen einheitlichen, sicheren und innovationsfördernden Datenbinnenmarkt zu schaffen. In diesem komplexen Regulierungsrahmen nimmt der Data Act eine Schlüsselrolle ein: Er ergänzt den Data Governance Act (DGA) und regelt insbesondere den fairen Zugang zu und die Nutzung von Daten, mit Fokus auf den industriellen und IoT-bezogenen Bereich. Während der DGA auf die Schaffung vertrauensvoller Datenräume und die Förderung freiwilliger Datenteilung abzielt, konkretisiert der Data Act die Rechte und Pflichten von Dateninhabern und –nutzern; vor allem im Verhältnis zwischen Unternehmen, Verbrauchern und öffentlichen Stellen. Gemeinsam mit weiteren Regelwerken wie dem Digital Services Act (DSA), dem Digital Markets Act (DMA) und der KI-Verordnung entsteht ein komplexes Ordnungsgefüge für die digitale Wirtschaft Europas:

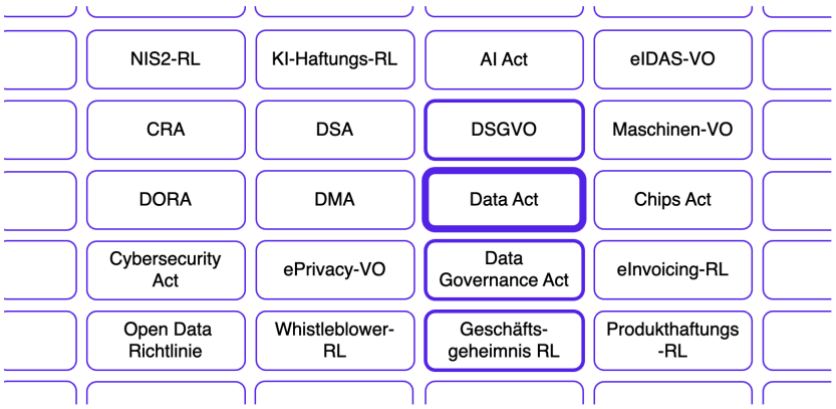


Abbildung 4

Der Data Act und benachbarte Rechtsakte der Europäischen Digitalstrategie der Europäischen Kommission

3.1.3 Überblick der Akteure und wichtigsten Pflichten

Der Data Act verfolgt das Ziel, Datenzugangs- und Datennutzungsrechte zu etablieren und diese durch die verschiedenen Regelungsinhalte sicherzustellen. Dabei entsteht ein Datenzugangsdreieck, das drei zentrale Akteursgruppen umfasst: Dateninhaber, Nutzer und Datenempfänger (Dritte), s. dazu auch das vereinfachte Datenzugangsschema unter 2.2. Da die DSGVO unberührt bleibt (s. dazu auch 3.1.4,) wird die rechtmäßige Nutzung personenbezogener Daten eine Rechtsgrundlage nach DSGVO voraussetzen. Es tritt daher als weiterer Akteur die **betroffene Person** hinzu.

Wer ist Dateninhaber? Der **Dateninhaber** (Art. 2 Nr. 13 Data Act) ist diejenige natürliche oder juristische Person, die kraft Gesetzes oder Vertrages verpflichtet ist, den Zugang zu bestimmten produkt- oder dienstbezogenen Daten zu ermöglichen und deren Weitergabe im Einklang mit dem Data Act zu ermöglichen. Typischerweise handelt es sich dabei um den Hersteller oder Anbieter eines vernetzten Produkts bzw. Dienstes, der durch seine technische oder rechtliche Kontrolle Zugriff auf die entstehenden Daten hat. Es ist dabei zu beachten, dass Hersteller und Dateninhaber weder gleichgesetzt werden können noch im Data Act trennscharf voneinander getrennt werden *(Hennemann et al., 2025).* In der Regel wird jedoch der Hersteller das Recht und die Pflicht innehaben, Daten zugänglich zu machen, da er meist die Person sein wird, die die Daten am ehesten kontrollieren kann. Die Gleichung *Hersteller = Dateninhaber* wird in der industriellen Realität nichtsdestotrotz in mehreren Fällen nicht immer passend sein. Der Dateninhaber ist damit zentrale Schnittstelle im Datenökosystem: Er verwaltet den Zugang zu den Daten und muss Nutzern oder vom Nutzer bestimmten Dritten den Datenzugang ermöglichen *(Schmidt-Kessel, 2024).*

Welche Pflichten gelten für Dateninhaber? (Auszug des Pflichtenprogramms)

Technische Gestaltung vernetzter Produkte und Dienste: **Data Access by Design** Art. 3 Abs. 1 DA Frist zur Umsetzung: 12.09.2026	Vernetzte Produkte müssen so konzipiert und hergestellt, und verbundene Dienste so gestaltet und erbracht werden, dass sie den Nutzer in die Lage versetzen, auf die dabei entstehenden Daten **standardmäßig** zuzugreifen. Dazu zählen sowohl Produktdaten als auch verbundene Dienstdaten, einschließlich aller relevanten Metadaten, die für das Verständnis und die Nutzung der Daten erforderlich sind. Der Zugang muss für den Nutzer einfach, sicher und unentgeltlich erfolgen, und zwar in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format. Soweit technisch möglich und sinnvoll, sollen die Daten zudem unmittelbar und **direkt zugänglich** sein. Dies schafft einen klaren Gestaltungsauftrag für Hersteller und Anbieter digitaler Dienste: Nutzerzentrierter Datenzugang wird zur technischen und rechtlichen Grundanforderung.
Datenhinweise zum vernetzten Produkt Art. 3 Abs. 2 DA Frist zur Umsetzung: 12.09.2025	Vor dem Abschluss eines Kauf-, Miet- oder Leasingvertrags über ein vernetztes Produkt muss der Nutzer über die datentechnischen Eigenschaften des Produkts informiert werden. Der Verkäufer, Vermieter oder Leasinggeber, wobei es sich auch um den Hersteller handeln kann, muss mindestens folgende Angaben bereitstellen: Art, Format und geschätzter Umfang der durch das Produkt generierten Daten, ob das Produkt Daten kontinuierlich und in Echtzeit erzeugen kann, ob und wo Daten gespeichert werden (lokal oder auf einem Server), inklusive Speicherdauer

	sowie Informationen zum Zugriff, Abruf und ggf. zur Löschung der Daten – einschließlich der technischen Mittel, Nutzungsbedingungen und Dienstqualität.
Datenhinweise zum verbundenen Dienst Art. 3 Abs. 3 DA Frist zur Umsetzung: 12.09.2025	Anbieter verbundener Dienste müssen vor Vertragsabschluss dem Nutzer darlegen, wie mit den entstehenden Daten umgegangen wird. Die **Pflichtinformationen** umfassen insbesondere: Art, Umfang und Häufigkeit der Datenerhebung sowie Informationen zu Zugriff, Speicherung und Aufbewahrungsdauer von Produkt- und Dienstdaten, Verwendungszwecke der Daten durch den künftigen Dateninhaber und ggf. durch Dritte, Identität und Kontaktdaten des potenziellen Dateninhabers sowie etwaiger weiterer Datenverarbeiter, Verfahren, wie der Nutzer Datenweitergabe an Dritte veranlassen oder beenden kann, Hinweise auf das Beschwerderecht bei der zuständigen Behörde gemäß Art. 37 Data Act, Angaben zu eventuell enthaltenen Geschäftsgeheimnissen und deren Inhaber, sowie Informationen zur Vertragsdauer und Bedingungen für eine vorzeitige Beendigung.
Datenherausgabe an Nutzer Art. 4 Abs. 1 DA Frist zur Umsetzung: 12.09.2025	Kann der Nutzer nicht direkt über das vernetzte Produkt oder den verbundenen Dienst auf die Daten zugreifen (by design), müssen ihm die ohne Weiteres verfügbaren Daten inklusive der erforderlichen Metadaten unverzüglich, sicher, unentgeltlich und in einem gängigen, maschinenlesbaren Format bereitgestellt werden. Dies erfolgt auf einfaches elektronisches Verlangen (**Datenzugangsanspruch** des Nutzers), kontinuierlich und in Echtzeit sowie in der gleichen Qualität, wie sie dem Dateninhaber selbst zur Verfügung stehen, soweit dies technisch möglich ist.
Bereitstellung von **personenbezogenen Daten** Art. 4 Abs. 12 DA Anwendung ab: 12.09.2025	Besteht ein Personenbezug, erfolgt die Bereitstellung personenbezogener Nutzungsdaten nur bei Vorliegen einer **gültigen Rechtsgrundlage**, gem. Art. 6 DSGVO sowie gegebenenfalls Art. 9 DSGVO.
Datennutzung nur auf Basis eines Vertrages: **Verpflichtende Datenlizenz** Art. 4 Abs. 13 DA Gilt für Verträge, die nach dem 12.09.2025 geschlossen werden.	Der Dateninhaber darf ohne Weiteres verfügbare, nicht-personenbezogene Daten nur auf Grundlage eines Vertrags mit dem Nutzer nutzen. Dabei ist es ihm ausdrücklich untersagt, diese Daten zur Gewinnung von Einblicken in die wirtschaftliche Lage, Vermögenswerte oder Produktionsmethoden des Nutzers zu verwenden – ebenso wenig in einer Weise, die dessen gewerbliche Position auf relevanten Märkten beeinträchtigen könnte. Vertragsklauseln, die zu Ungunsten einer Partei (insbesondere des Nutzers) von den gesetzlichen Vorgaben abweichen, sind nicht bindend. Zudem unterliegen die Vertragsklauseln einer strengen Kontrolle **(“AGB-Recht" für Datenlizenzen)**, um insbesondere KMU vor unfairen oder unangemessenen Regelungen zu schützen *(vgl. Art. 12,13 Data Act).*

Datenweitergabe an Dritte Art. 5 Abs. 1 DA Anwendung ab: 12.09.2025	**Auf Verlangen des Nutzers** muss der Dateninhaber einem Dritten die ohne Weiteres verfügbaren Daten sowie die nötigen Metadaten unverzüglich, unentgeltlich, sicher und in derselben Qualität bereitstellen. Vorgesehen wird die Bereitstellung in einem gängigen, strukturierten und maschinenlesbaren Format, möglichst kontinuierlich und in Echtzeit. Die Bereitstellung erfolgt gem. den Vorgaben der Art. 8 und 9 Data Act.
Verarbeitungsverbot ohne Weiteres verfügbarer Daten Art. 5 Abs. 6 DA Anwendung ab: 12.09.2025	Der Dateninhaber darf ohne Weiteres verfügbare Daten **nicht zur Analyse** der wirtschaftlichen Lage, Vermögensverhältnisse oder Produktionsmethoden des Dritten verwenden, wenn dies dessen Wettbewerbsposition gefährden könnte. Eine solche Nutzung ist nur zulässig, wenn der Dritte ausdrücklich zustimmt und er diese Zustimmung jederzeit einfach widerrufen kann (Art. 5 Abs. 6 Data Act).

Wer ist Nutzer? Der **„Nutzer“** (Art. 2 Nr. 12 Data Act) ist eine natürliche oder juristische Person, die ein vernetztes Produkt besitzt oder berechtigt (durch Vertrag) nutzt oder verbundene Dienste in Anspruch nimmt. Nutzer sind zentrale Anspruchsberechtigte des Data Act und profitieren von den wesentlichen Datenzugangs- und Datenbereitstellungspflichten nach Art. 3, 4 und 5 Data Act *(Hennemann et al., 2025).*

Sie haben nicht nur das Recht, auf die beim Einsatz eines Produkts oder Dienstes entstehenden Daten zuzugreifen, sondern können auch darüber entscheiden, ob diese vom Dateninhaber an einen Dritten weitergegeben werden sollten. Zudem dürfen Dateninhaber nicht-personenbezogene Daten nur dann selbst nutzen, wenn der Nutzer dem zuvor vertraglich zugestimmt hat. Damit hält der Nutzer die zentrale Entscheidungsgewalt über die Verwendung der Daten und wird zum Schlüsselakteur im Datenzugangsdreieck.

Wer ist Datenempfänger (Dritter)? Der **„Datenempfänger“** (Art. 2 Nr. 14 Data Act) ist eine natürliche oder juristische Person, die im Rahmen ihrer beruflichen oder wirtschaftlichen Tätigkeit handelt, aber selbst kein Nutzer eines vernetzten Produkts oder verbundenen Dienstes ist. Diese erhält Daten vom Dateninhaber auf ausdrückliches Verlangen des Nutzers.

Datenempfänger sind damit typische Akteure der Datenweiterverwertung: Sie können z. B. als Wartungsdienstleister, Plattformbetreiber oder Analyseanbieter agieren, sofern der Nutzer den Zugang zu den entsprechenden Daten freigegeben hat. Entscheidend ist: Ohne die Zustimmung des Nutzers ist der Datenzugang für diese nicht möglich.

Welche Pflichten gelten für Datenempfänger (Dritte)? (Auszug des Pflichtenprogramms)

Vereinbarung von **TOMs zum Schutz von Geschäfts-geheimnissen** Art. 6 Abs. 9 DA Anwendung ab: 12.09.2025	Geschäftsgeheimnisse werden nur soweit offengelegt, wie es für den vertraglich vereinbarten Zweck mit dem Dritten unbedingt notwendig ist. Der Dateninhaber oder der Geschäftsgeheimnisinhaber identifiziert schützenswerte Daten einschließlich relevanter Metadaten und stimmt mit dem Dritten geeignete technische und organisatorische Maßnahmen ab, um deren Vertraulichkeit sicherzustellen. Dazu zählen beispielsweise Mustervertragsklauseln, Vertraulichkeitsvereinbarungen, strenge Zugangsprotokolle und die Anwendung anerkannter Sicherheitsstandards.
Zweckbindung und Nutzungsbeschränkung Art. 6 Abs. 1 DA Anwendung ab: 12.09.2025	Der Datenempfänger ist verpflichtet, die ihm bereitgestellten Daten ausschließlich zu den vertraglich mit dem Nutzer vereinbarten Zwecken zu verarbeiten. Sobald die Daten für den vereinbarten Zweck nicht mehr benötigt werden, müssen sie gelöscht werden – es sei denn, der Nutzer hat hinsichtlich nicht-personenbezogener Daten etwas anderes mit dem Dritten vereinbart.
Beachtung **Nutzungsverbote** Art. 6 Abs. 2 DA Anwendung ab: 12.09.2025	Datenempfänger dürfen die vom Nutzer erhaltenen Daten ausschließlich im Rahmen des vereinbarten Zwecks und gesetzeskonform nutzen. **Verboten** ist insbesondere: die Einschränkung von Nutzerrechten, unerlaubtes Profiling, Weitergabe an Dritte ohne Nutzervertrag, Übermittlung an sogenannte Torwächter (z. B. große Plattformen), Nutzung zur Entwicklung konkurrierender Produkte, sicherheitsgefährdende Verwendungen sowie die Verletzung von Geschäftsgeheimnissen. Wenn es sich beim Nutzer um einen Verbraucher handelt, darf dieser außerdem nicht daran gehindert werden, seine Daten weiteren Partien weiterzugeben (keine Exklusivvereinbarungen).
Pflichten bei **unrechtmäßiger Daten-verwendung** Art. 11 Abs. 2 DA Anwendung ab: 12.09.2025	Kommt es zu einer rechtswidrigen Nutzung oder Weitergabe von Daten, ist der Dritte oder Datenempfänger verpflichtet, den Aufforderungen des Dateninhabers, des Inhabers von Geschäftsgeheimnissen oder des Nutzers unverzüglich nachzukommen. Dazu zählen u.a. die Löschung aller erhaltenen Daten, das Einstellen und ggf. Vernichten daraus abgeleiteter Produkte oder Dienstleistungen, die Information des Nutzers über die erfolgte Datenverletzung sowie eine angemessene Entschädigung für entstandene Schäden. Diese Pflichten greifen insbesondere dann, wenn die Daten durch Täuschung, unbefugte Nutzung, Weitergabe, Missachtung technischer Schutzmaßnahmen oder Sicherheitslücken erlangt oder verarbeitet wurden.

3.1.4 Spannungsfeld Datenzugang zum Schutz von Geschäftsgeheimnissen und personenbezogenen Daten

Der Data Act etabliert Datenzugangsrechte und bringt damit zwangsläufig Spannungsverhältnisse im Verhältnis zu Geschäftsgeheimnissen und dem Schutz personenbezogener Daten mit sich *(Antoine, 2024)*. In den folgenden Abschnitten wird skizziert, welche Anforderungen Unternehmen in Bezug auf diese Thematiken im Blick behalten sollten.

3.1.4.1 Spannungsfeld Datenzugang und Schutz von Geschäftsgeheimnissen

Das Ziel des europäischen Gesetzgebers, über den Data Act den bislang einseitigen Datenzugang der Hersteller durch gesetzlich verankerte Bereitstellungs- und Zugangsrechte zugunsten der Nutzer aufzubrechen, kollidiert in zentralen Punkten mit dem Schutz von Geschäftsgeheimnissen (*Grützmacher, 2024)*. Das Nutzungsrecht an diesen Daten ist sowohl für Nutzer als auch für Dritte von Interesse, z.B. wenn es darum geht, ergänzende Dienstleistungs- und Datenmärkte zu erschließen. Für den Dateninhaber kann dies auf diesen Märkten unerwünschten Wettbewerb bedeuten und die Sorge auslösen, dass im Rahmen des Datenzugangs oder der Weitergabe der Daten wertvolles Know-how an Nutzer oder Dritte gelangen könnte.

Was sind Geschäftsgeheimnisse im Sinne des Data Act? Vor diesem Hintergrund stellt sich die Frage, in welchem Umfang der Schutz von Geschäftsgeheimnissen durch die Datenzugangsansprüche ausgehöhlt wird oder ob der Data Act den Geheimnisschutz ausreichend berücksichtigt.

Ein Geschäftsgeheimnis liegt nach Art. 2 Nr. 18 Data Act vor, wenn es den Kriterien der EU-Geschäftsgeheimnis-Richtlinie (umgesetzt im deutschen Recht in § 2 Nr. 1 GeschGeh = Gesetz zum Schutz von Geschäftsgeheimnissen) entspricht. Konkrete Voraussetzungen sind, dass Informationen vorliegen müssen, die (a) weder allgemein bekannt noch leicht zugänglich sind und daher wirtschaftlichen Wert besitzen, (b) durch angemessene Geheimhaltungsmaßnahmen geschützt werden und (c) ein berechtigtes Interesse an der Geheimhaltung besteht.

Ob die im Data Act erfassten, ohne Weiteres verfügbaren Daten, also unverarbeitete Rohdaten vom Schutz des GeschGehG erfasst werden, ist in der Literatur umstritten (*Grützmacher, 2024*.) So äußerte sich unter anderem die EU -Kommission mit Verweis auf eine Studie, dass gerade dies nicht der Fall sei (*European Commission/European Innovation Council and SMEs ExecutiveAgency/Radauer/Bader/Aplin u.a., Study on the legal protection of tradesecrets in the context of the data economy - Final report, Publications Office of the European Union, 2022, S. 89*). Dieser Sichtweise steht jedoch eine Vielzahl konträrer Meinungen gegenüber, nach denen auch Rohdaten (zumindest unter bestimmten Voraussetzungen) als Geschäftsgeheimnisse im Sinne des GeschGehG qualifiziert werden können. Hinzuweisen ist auf die Rechtsprechung des Bundesverwaltungsgerichts (*BVerwG, Beschl. v. 5.3.2020 – 20 F 3.19*), die anerkennt, dass auch Daten als Geschäftsgeheimnisse geschützt sein, sofern aus diesen Daten Geschäftsgeheimnissen abgeleitet werden können. Man könnte also annehmen, dass durch die Zusammenführung von Daten oder technischen Parametern, wie etwa Temperaturen und Bewegungsdaten vernetzter Produkte, Rückschlüsse auf deren technische Funktionsweise möglich sind *(Pauly et al., 2024).* Weiter könnte das

auch für Datensätze gelten, aus denen sich leicht auf besonders relevante Geschäftsgeheimnisse schließen lässt, beispielsweise weil sie ein Reverse Engineering gemäß § 3 Abs. 1 Nr. 2 GeschGehG ermöglichen.

Der Gesetzgeber hat diese Spannungsverhältnisse zwar erkannt, doch ob dies im Zusammenspiel mit den Regelungen des Data Act in der Praxis tatsächlich funktioniert, bleibt abzuwarten. Für den Dateninhaber entsteht ein Zielkonflikt: Er muss einerseits den Verlust seiner Datenschätze fürchten, andererseits droht ihm ein hohes Bußgeld (Art. 40 Data Act), wenn er den Zugang unrechtmäßig verweigert, weil er die Anforderungen an den Geheimnisschutz falsch einschätzt *(Grützmacher, 2024)*.

Welche Schutzmaßnahmen im Lichte des Geschäftsgeheimnisschutzes sieht der Data Act vor? Der Data Act sieht vor, dass Geschäftsgeheimnisse geschützt bleiben. Der Data Act sieht hierfür verschiedene Schutzmechanismen vor oder legt sie zumindest nahe, etwa die Mustervertragsklauseln (der Europäischen Kommission *(vgl. Art. 41 Data Act)*, NDAs, strenge Zugriffsregelungen, technische Sicherheitsvorgaben und Verhaltenskodizes. Zum Schutz gehört auch die Implementierung von Berechtigungskonzepten, die eine beschränkte Nutzung sicherstellen sowie Geheimhaltungsverpflichtungen bei Drittzugriffen. Es empfiehlt sich daher, der Datenzugang auf eine „Need-to-Know"-Basis zu beschränken. Fehlen solche Schutzmaßnahmen (wie z.B. einem passwortgeschützten Berechtigungskonzepts) und haben Mitarbeiter weit über die Entwicklungsabteilung hinaus Zugriff auf die relevanten Daten, wird man sich auf den Geschäftsgeheimnisschutz wohl kaum berufen können *(Pauly et al., 2024).* Dreh und Angelpunkt des Schutzes geschäftsgeheimnishaltiger Daten werden vertragliche Vereinbarungen zwischen Dateninhabern und Nutzern bzw. Dritten (Datenempfängern) sein. Diese Vereinbarungen werden entlang der gesamten Wertschöpfungskette vernetzter Produkte und Dienste eine zentrale Rolle spielen, vor allem auch dann, wenn mehrere Geschäftsgeheimnisinhaber für die betroffenen Daten bestehen. Zum einen beugt die vertragliche Absicherung einem „Overclaiming" von Geschäftsgeheimnissen vor. Dies ist notwendig, da der Begriff des Geschäftsgeheimnisses nicht eindeutig abgegrenzt ist und der Data Act (anders als etwa Art. 20 Abs. 4 DSGVO) keine Abwägungsvorschrift enthält, die Datenzugangsrechte relativieren würde.

Eine genauere Betrachtung zeigt, dass der EU-Gesetzgeber dem Datenzugang spürbar mehr Gewicht beimisst als dem Schutz von Geschäftsgeheimnissen, obwohl weite Teile der europäischen Industrie, etwa der Anlagen- und Maschinenbau, die Fahrzeugbranche oder die Medizintechnik, gerade auf letzteren angewiesen sind *(Antoine, 2024).* Diese Feststellung wird noch intensiv diskutiert werden; dazu sind auch dementsprechende Ausformungen und Leitsätze durch die Rechtsprechung des EuGH zum Verhältnis von Daten und Geschäftsgeheimnisschutz zu erwarten.

Zugleich wird nochmal mehr deutlich: Der Vertrag ist das zentrale Instrument zur Umsetzung des Data Act (*Wiebe, 2023)*. In sämtlichen Konstellationen, ob zwischen Nutzer und Dateninhaber oder gegenüber Dritten, sind vertragliche Regelungen zum Schutz von Geschäftsgeheimnissen angesagt. Um dem Dateninhaber Kontrolle im Umgang mit seinen Geschäftsgeheimnissen einzuräumen, sieht Art. 4 Abs. 6 – 7 und Art. 5 Abs. 9 Data Act – 12 Regelungen zum Geheimnisschutz vor und die Möglichkeit den Datenzugang bzw. die Datenweitergabe im Einzelfall für spezielle Daten abzulehnen (Art. 4 Abs. 8 und Art. 5 Abs. 11 Data Act).

Welche Schranken und Verweigerungsrechte bestehen zu Gunsten des Geheimnisschutzes nach dem Data Act? Liegt ein Geschäftsgeheimnis vor, kann der Dateninhaber dem Anspruch des Nutzers auf Datenzugang oder Weitergabe an Dritte entgegentreten. Das ist dann möglich, wenn ein Geschäftsgeheimnis vorliegt, aber der Schutz des Geheimnisses (trotz der in Art. 4 Abs. 7 und Art. 5 Abs. 10 Data Act vorgesehenen Maßnahmen) nicht gewährleistet werden kann. Selbst wenn sich die Parteien auf Schutzmaßnahmen geeinigt haben, darf der Dateninhaber den Zugang so lange zurückhalten, bis ein ausreichender Schutz tatsächlich gewährleistet ist. Sind die erforderlichen Maßnahmen technisch oder organisatorisch besonders anspruchsvoll, kann dies die Bereitstellung der Daten entsprechend verzögern *(Pauly et al., 2024).* Darüber hinaus ist eine Verweigerung auch dann denkbar, wenn außergewöhnliche Umstände vorliegen und mit hoher Wahrscheinlichkeit mit schwerwiegenden wirtschaftlichen Schäden zu rechnen wäre (Art. 4 Abs. 8 und Art. 5 Abs. 11 Data Act; *Schulz, 2024*).

Ein **Verweigerungsrecht** des Dateninhabers besteht demensprechen dann, wenn sich die beteiligten Parteien nicht auf angemessene Schutzmaßnahmen einigen konnten, vereinbarte Maßnahmen nicht umgesetzt wurden oder es zu einer Verletzung der Vertraulichkeit gekommen ist. Selbst wenn Nutzer oder Dritte ausreichende Maßnahmen zum Schutz von Geschäftsgeheimnissen ergreifen, kann der Dateninhaber den Zugang nach Art. 4 Abs. 8 bzw. Art. 5 Abs. 11 Data Act verweigern, wenn im Ausnahmefall mit hoher Wahrscheinlichkeit ein schwerer wirtschaftlicher Schaden droht. Laut Erwägungsgrund 31 des Data Act ist ein solcher Schaden gegeben, wenn erhebliche und irreparable wirtschaftliche Verluste zu erwarten sind. Das im Gesetzgebungsverfahren stark umstrittene Verweigerungsrecht wird in den Erwägungsgründen nur vage umschrieben, sodass unklar bleibt, welche konkreten Kriterien in der Praxis und Rechtsprechung künftig maßgeblich sein werden *(Grützmacher, 2024)*. Der Data Act nennt dazu einige Anhaltspunkte, darunter die Durchsetzbarkeit des Geheimnisschutzes in Drittländern (außerhalb der EU), den Vertraulichkeitsgrad und die Art der betroffenen Daten sowie die „Einzigartigkeit und Neuartigkeit“ des vernetzten Produkts. Zusätzlich wird auch auf mögliche negative Auswirkungen für die Cybersicherheit hingewiesen.

Gibt es Hinweise auf praktisch erwartbare Schwierigkeiten und Konfliktpotenziale zum Datenzugang vs. Geschäftsgeheimnisschutz? Schon jetzt ist absehbar, dass die Anwendung der im Data Act festgelegten Kriterien zu erheblichen Streitigkeiten führen wird:

Zum einen stellt der Nachweis, dass es sich bei den betroffenen Daten tatsächlich um ein Geschäftsgeheimnis handelt, eine große Herausforderung dar. Der Dateninhaber muss diese Tatsache darlegen und belegen, um sich gegen einen Datenzugriff zu wehren. Allerdings wird es häufig schon umdie grundsätzliche Frage gehen, ob bestimmte Daten, wie etwa Maschinendaten, überhaupt als Geschäftsgeheimnisse gelten können (s.o.). Pauschale Aussagen, dass solche Daten grundsätzlich kein Geschäftsgeheimnis darstellen, sind dabei nicht haltbar. Darüber hinaus wird es für den Dateninhaber oft schwierig sein, die konkreten Maßnahmen zur Geheimhaltung überzeugend nachzuweisen *(Schulz, 2024).*

Zum anderen ist Streit darüber, welche Schutzmaßnahmen tatsächlich notwendig sind und ob diese bereits ausreichend umgesetzt wurden, absehbar. Die Beteiligten werden hier nicht selten unterschiedlicher Auffassung sein. Eine Antwort auf die Frage, wer im Streitfall die Verantwortung für den

Nachweis der Umsetzung trägt, wird auch abzuwarten sein. Zwar weisen Art. 4 Abs. 7 und Art. 5 Abs. 10 Data Act die Beweislast zunächst dem Dateninhaber zu, doch fehlt diesem in der Praxis oft der nötige Einblick in die Verhältnisse beim Nutzer oder Dritten. Daher dürfte zumindest in Teilen auch Letzteren eine sekundäre Darlegungslast treffen. Ein weiteres Problem stellt die unklare Definition des Begriffs „schwerer wirtschaftlicher Schaden" dar *(Specht-Riemenschneider et al. 2025)*. Wie bereits ausgeführt, bietet Erwägungsgrund 31 des Data Acts nur eine vage Orientierung, sodass unklar bleibt, wann genau ein solcher Schaden angenommen werden kann.

Für Anbieter von Geräten, Systemen oder Diensten ist dies besonders problematisch, da die Hürden für eine Weitergabe an Dritte gering sind. Denn im Grunde lässt sich stets ein Nutzer finden, mit dem eine Zweckvereinbarung gem. Art. 5 Abs. 10 Data Act getroffen werden kann - eine Hürde, die kaum unüberwindbar erscheint. In einem solchen Fall obliegt es dem Inhaber, nachzuweisen, dass der Dritte gegen die getroffenen Vertraulichkeitsvereinbarungen verstoßen hat. Hinzu kommt, dass es äußerst schwierig sein wird zu belegen, dass der Dritte die erhaltenen Informationen zur Entwicklung von Konkurrenzprodukten genutzt hat. Daher wird es in bestimmten Fällen wohl wenig helfen, dass sich Dritte nach Art. 9 Abs. 2 lit. c) Data Act zur Geheimhaltung verpflichtet haben *(Pauly et al., 2024).*

Zwar sieht der Data Act vor, den Datenzugriff bei Verletzung der Vertraulichkeit zu verweigern. Allerdings besteht die begründete Sorge, dass Verstöße oft erst erkannt werden, wenn der Schaden bereits eingetreten ist oder dass ein entsprechender Nachweis sehr schwer zu erbringen sein wird (*Schulz, 2024)*.

3.1.4.2 Das Spannungsfeld zwischen Datenzugang im Verhältnis zum Datenschutz

Zwar adressiert der Data Act sowohl personenbezogene als auch nicht-personenbezogene Daten, doch liegt der Schwerpunkt klar auf der Nutzung von maschinell erzeugten und industriellen Daten. Im Fall eines Konflikts zwischen Data Act und DSGVO gilt im Zweifel der **Anwendungsvorrang der DSGVO**. Daraus folgt auch, dass der Data Act keine eigenständige Erlaubnisnorm für eine Verarbeitung personenbezogener Daten darstellt *(Schemmel, 2024; Hennemann et al. 2025)*. Vor diesem Hintergrund ist es für die praktische Anwendung des Data Act wichtig zu klären, ob es sich bei dem jeweiligen Datensatz um personenbezogene oder nicht-personenbezogene Daten handelt. Der Data Act gilt gem. Art. 2 Nr. 1 Data Act grundsätzlich für alle Arten von Daten. Dennoch ist es erforderlich, den vermeintlichen Personenbezug zu bestimmen, um festzustellen, ob bei dem Zugang zu diesem Datensatz die Regelungsinhalte der DSGVO gelten, oder nicht. Eine eigene Definition personenbezogener Daten enthält der Data Act nicht, sondern verweist in Art. 2 Nr. 3 Data Act auf die Begriffsbestimmung der DSGVO (Art. 4 Nr. 1 DSGVO).

Im Rahmen des Data Act umfasst der Begriff der **personenbezogenen Daten** digitale Darstellungen von Informationen, die sich auf eine identifizierte natürliche Person beziehen. Ist die Person nicht benannt, ist ein Datum dennoch personenbezogen, wenn die betroffene Person anhand der vorliegenden Informationen identifizierbar ist, d. h. mit vertretbarem Aufwand bestimmt werden kann *(Art. 4 Nr. 1 DSGVO; Specht-*

Riemenschneider, 2023). **Nicht-personenbezogene Daten** hingegen werden im Data Act negativ abgegrenzt. Es handelt sich somit um alle Daten, die keine Informationen mit Bezug auf natürliche Personen enthalten (Art. 2 Nr. 4 Data Act). Ob diese Negativabgrenzung des Personenbezugs in der Praxis jedoch trennscharf vorgenommen werden kann, ist fraglich. In vielen Fällen ist die Grenze zwischen personenbezogenen und nicht-personenbezogenen Daten fließend, z.B. wenn ursprünglich anonym erscheinende Daten durch Kombination mit weiteren Informationen eine Re-Identifikation von Personen ermöglichen *(Antoine, 2024)*. Dies stellt Dateninhaber vor erhebliche Unsicherheiten hinsichtlich der datenschutzrechtlichen Einordnung und der damit verbundenen Pflichten, etwa im Hinblick auf den Datenschutz (*Specht-Riemenschneider, 2023)*. Gerade im Kontext vernetzter Geräte und IoT-Anwendungen besteht daher ein erhöhtes Risiko, dass vermeintlich nicht-personenbezogene Daten doch Rückschlüsse auf einzelne Personen zulassen.

Somit gilt: Wenn es sich bei den Daten auch um personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO handelt, ist der Anwendungsbereich des Datenschutzrechts eröffnet. In diesem Fall darf der Dateninhaber personenbezogene (IoT)-Daten nur unter Vorbehalt einer **datenschutzrechtlichen Erlaubnis** gem. Art. 6 DSGVO bzw. einer Ausnahme gem. Art. 9 DSGVO an den Nutzer oder einen von diesem bestimmten Datenempfänger übermitteln.

Da der Data Act die Persönlichkeitsrechte der betroffenen Personen nicht beeinträchtigen sollte, schlägt der Verordnungsgeber in Erwägungsgrund 7 vor, dass Dateninhaber den Datenzugang auf datenschutzkonforme Weise durch Anonymisierung oder Aussonderung personenbezogener Daten gewähren können *(Baumann & Brunnbauer, 2025).* Der Vorteil der Anonymisierung besteht darin, dass den Daten der Personenbezug entzogen wird und damit die Vorschriften der DSGVO nicht anwendbar sind. Im Unterschied zur Anonymisierung bleiben pseudonymisierte Daten grundsätzlich re-identifizierbar, sofern entsprechende Zusatzinformationen vorliegen. Zwar kann das Recht auf Datenzugang bei anerkannter Pseudonymisierung höher gewichtet werden, doch gelten solche Daten weiterhin als personenbezogen. Datenschutzrechtlich bietet daher nur die Anonymisierung eine sichere Option.

Wer im datenschutzrechtlichen Sinne als **Verantwortlicher** (Art. 4 Nr. 7 DSGVO) für die Übermittlung personenbezogener Daten anzusehen ist, hängt vom jeweiligen Einzelfall ab. In der Praxis kommen regelmäßig der Nutzer als auch der Dateninhaber als Verantwortliche in Betracht. Unter Umständen kann auch eine gemeinsame Verantwortlichkeit gem. Art. 26 DSGVO bestehen, welche in Erwägungsgrund 34 ausdrücklich erwähnt wird *(Specht-Riemenschneider et al. 2025).*

Im Kontext des Data Act gelten **Auftragsverarbeiter** (Art. 4 Nr. 8 DSGVO) nicht als Dateninhaber. Dies ist insofern nachvollziehbar, da der Auftragsverarbeiter nicht selbst über Zweck und Mittel der Datenverarbeitung entscheidet und somit keine eigenständige rechtliche Befugnis hat, den Zugang zu den Daten zu gewähren. Er handelt ausschließlich auf Weisung des Verantwortlichen im Sinne von Art. 4 Nr. 7 DSGVO und ist nur dann berechtigt, Zugang zu gewähren, wenn eine entsprechende Anweisung des Verantwortlichen vorliegt *(Specht-Riemenschneider et al. 2025).*

Vor diesem Hintergrund ist auch die in der Praxis relevante Konstellation zu beachten, dass ein Datenzugangsverlangen zugunsten eines Dritten zwar auf Grundlage des Data Act gestellt wird, der Dateninhaber dieses jedoch unter Berufung auf datenschutzrechtliche Schranken verweigern könnte. Dies könnte insbesondere dadurch erfolgen, dass Datensätze vorsätzlich mit personenbezogenen Daten kontaminiert werden, in dem Bewusstsein, dass gemischte Datensätze wie personenbezogene zu behandeln sind und somit den Datenzugangsanforderungen des Data Act entzogen werden *(Schemmel, 2024)*. Da die DSGVO Anwendungsvorrang genießt, stellt der Data Act keine eigene Rechtsgrundlage für die Übermittlung personenbezogener Daten dar. Fehlt es also an einer Erlaubnisnorm nach Art. 6 DSGVO, etwa in Form einer ausdrücklichen Einwilligung der betroffenen Person oder einer anderweitigen gesetzlichen Grundlage, ist der Dateninhaber nicht nur berechtigt, sondern sogar verpflichtet, den Datenzugang zu verweigern.

3.1.5 Im Überblick: Ansätze zur Data Governance des Dateninhabers

Nachfolgend werden im Überblick drei Ebenen der Data Governance im Hinblick auf die Verpflichtungen eines Dateninhabers im Sinne des Data Act vorgeschlagen.

1. Ebene: Dateninventur und Klassifizierung von Daten. Der erste Schritt zur Etablierung wirksamer Data-Governance-Strukturen (oder auch: zentrales Datenmanagement) besteht in der Durchführung einer Dateninventur, mit dem Ziel, einen systematischen Überblick über sämtliche im Unternehmen vorhandenen Daten zu gewinnen. Diese umfasst sowohl die strukturierte Bestandsaufnahme als auch die Klassifizierung der Daten nach definierten Kriterien, um deren Herkunft, Relevanz und potenzielle Nutzungsmöglichkeiten einordnen zu können *(Hennemann et al., 2025).*

Im Rahmen des Data Acts sind Dateninhaber dazu verpflichtet, bestimmte Daten unter festgelegten Bedingungen bereitzustellen. Ohne eine vorherige strukturierte Dateninventur ist es kaum möglich, diesen Pflichten rechtskonform und gezielt nachzukommen. Vor allem müssen Dateninhaber in der Lage sein, Daten aus vernetzten Produkten, verbundene Dienstdaten sowie **ohne Weiteres verfügbare Daten** zu identifizieren, zu klassifizieren und auf Anfrage bereitzustellen. Diese unterscheiden sich folgendermaßen (s. dazu schon ausführlich unter 2.2):

Produktdaten stellen einen Hauptanwendungsfall des Data Act dar, da sich das Zugangsregime primär auf sie (und auf verbundene Dienstdaten) bezieht. Sie entstehen bei der Nutzung vernetzter Produkte, sei es durch aktive Nutzerinteraktion oder passiv als Nebenprodukt. Bei **verbundenen Dienstdaten** handelt es sich dagegen um Daten, die bei der Erbringung verbundener Dienste entstehen und digitale Nutzerhandlungen im Zusammenhang mit dem vernetzten Produkt bilden. Beispiele hierfür sind Daten über die Umgebung oder Interaktionen des vernetzten Produkts, wie etwa Standortinformationen zu bestimmten Zeitpunkten bei einem vernetzten Navigationsgerät. **Ohne Weiteres verfügbare Daten** sind Produkt- und verbundene Dienstdaten, die der Dateninhaber rechtmäßig und ohne unverhältnismäßigen Aufwand aus dem vernetzten Produkt oder Dienst erhalten kann. Ein besonderes Augenmerk ist dabei auf die Herkunft der Daten zu richten: Nur wenn nachvollziehbar ist, woher die Daten stammen, etwa ob sie

intern generiert, von Dritten bereitgestellt oder aus vernetzten Geräten gewonnen wurden, kann eine systematische Einordnung im Sinne des Data Act erfolgen *(Schreiber et al., 2024).*

Diese erste Ebene, die Inventur der Datenbestände, bildet die Grundlage für eine differenzierte Datenkategorisierung entlang rechtlicher und wirtschaftlicher Kriterien. So lassen sich etwa Daten identifizieren, die unter Zugangspflichten nach dem Data Act fallen, aber auch solche, bei denen gegebenenfalls die Schranke des Geschäftsgeheimnisschutzes, geltend gemacht werden kann *(Hennemann et al., 2025; s. dazu auch 3.1.4.1).*

Darüber hinaus schafft eine solche Transparenz über Datenströme und -quellen nicht nur die Basis für rechtliche Einordung, sondern fördert auch das Bewusstsein für den wirtschaftlichen Wert der eigenen Datenbestände; ein Aspekt, der durch den Data Act erheblich an Bedeutung gewinnt (*s. dazu ergänzend Kapitel Datenbewertung 3.4).*

2. Ebene: Identifikation von besonderen Datensätzen und Handlungsbedarfen. Sobald durch eine gezielte Dateninventur Transparenz über die im Unternehmen vorhandenen Daten geschaffen wurde, stellt sich im nächsten Schritt die Frage nach deren rechtlichem Schutz. Der Data Act fordert nicht nur eine klare Zuordnung und Kategorisierung der Daten, sondern setzt auch voraus, dass Unternehmen wissen, ob und in welchem Umfang ihre Daten gegen unbefugte Nutzung geschützt sind und welche Abwehrinstrumente des Data Act zur Verfügung stehen.

Da **keine Eigentumsrechte an einzelnen Daten**, Datensätzen oder unstrukturierten Datensammlungen bestehen, kommt ein rechtlicher Schutz lediglich für strukturierte Datenbestände durch das Datenbankrecht gemäß der Richtlinie 96/9/EG oder als urheberrechtliches Datenbankwerk infrage. Für unstrukturierte Daten kommt allenfalls ein Schutz über das Geschäftsgeheimnisrecht in Betracht *(Antoine, 2024).* Dieser Schutz dient folglich primär dem **Zugangsschutz** und nicht der Zuerkennung eines Ausschließlichkeitsrechts *(Antoine, 2024).* Vor diesem Hintergrund ist es für Unternehmen essenziell, ihre Datenbestände nicht nur technisch zu erfassen, sondern auch juristisch zu bewerten: *Welche Daten könnten unter bestehende Schutzregime (wie das Datenbankrecht oder das Geschäftsgeheimnisrecht) fallen? Welche zusätzlichen Maßnahmen sind erforderlich, um überhaupt einen Schutzstatus zu begründen und aufrechtzuerhalten?*

Bereits im Vorfeld der Datenweitergabe im Rahmen des Data Act sollten Unternehmen ihre internen Spielräume bestmöglich durch eine systematische Einstufung schützenswerter Daten ausschöpfen. Gerade bei strategisch relevanten Daten, deren Bedeutung sich aus der zuvor erfolgten Dateninventur und -kategorisierung ergibt, ist im zweiten Schritt eine Einschätzung der potenziell bestehenden Spannungsverhältnisse notwendig *(Antoine, 2024; s. dazu bereits 3.1.4).* Nur wenn Klarheit besteht, lassen sich etwaige Zugriffsverlangen unter dem Data Act rechtlich begrenzen sogar oder verweigern. Die gewonnenen Erkenntnisse bilden zudem die Grundlage für die Ausgestaltung vertraglicher Regelungen sowie für mögliche Anpassungen unternehmensinterner Prozesse und Geschäftsmodelle im Lichte der neuen gesetzlichen Anforderungen.

Mit dem Inkrafttreten des Data Act wird das Bedürfnis für eine interne Datenklassifikation in Unternehmen deutlich ausgeweitet:

Neben den bereits durch die DSGVO etablierten Anforderungen zur Erfassung personenbezogener Daten müssen Unternehmen nun auch sämtliche produktbezogenen und dienstebezogenen IoT-Daten identifizieren, die potenziell unter die Datenzugangs- und -bereitstellungspflichten des Data Act fallen. Dies gilt unabhängig davon, ob es sich um strukturierte oder unstrukturierte, personenbezogene oder nicht-personenbezogene Daten handelt. Anhand der gewählten Schutzkategorie und Festlegung eines klaren Vorgehens, lassen sich dann konkrete Maßnahmen ableiten: von organisatorischen und technischen Vorkehrungen bis hin zu vertraglichen Schutzmechanismen gegenüber Nutzern und Dritten.

3. Ebene: Konzeption hinsichtlich der unterschiedlichen Datenzugangsarten. Im Zuge der Umsetzung des Data Act der Europäischen Union rückt die Frage nach dem Zugang zu Daten ins Zentrum unternehmerischer Verantwortung. Spätestens nach Anwendung des Data Act genügt die bloße Möglichkeit längst nicht mehr, Daten technisch bereitstellen zu können. Vielmehr bedarf es einer **organisatorischen, rechtlichen und strategischen** Einbettung der Anforderungen des Data Act in eine Data-Governance-Struktur *(Hennemann et al., 2025).* Auf der dritten konzeptionellen Ebene, der Ebene des tatsächlichen Datenzugangs, sollten sich Unternehmen entscheiden, wie sie den gesetzlichen Zugangsansprüchen gerecht werden und gleichzeitig legitime Schutzinteressen, etwa im Hinblick auf Geschäftsgeheimnisse, verfolgen können. Es steht ein Balanceakt zwischen Offenheit und Schutz, in dem sich moderne Data Governance Strukturen heute bewegen müssen *(Spießhofer, 2022; Ohly, 2019).*

Der Data Act differenziert dabei zwischen zwei zentralen Formen des Datenzugangs: dem unmittelbaren Zugriff durch den Nutzer **(„Access by Design“)** gem. Art. 3 Abs. 1 Data Act sowie der nachgelagerten **Bereitstellung** durch den Dateninhaber nach Art. 4 Abs. 1 DA. Beide Normen verpflichten Unternehmen, Nutzern die durch ein vernetztes Produkt oder einen verbundenen Dienst erzeugten Daten einfach, unentgeltlich, strukturiert und maschinenlesbar zugänglich zu machen. Art. 3 Data Act verlangt, dass der Zugang bereits im Produktdesign verankert wird. Für Unternehmen bedeutet dies eine Neuausrichtung ihrer Entwicklungs- und Designprozesse im Sinne eines „Data Access by Design“, das technologische, regulatorische und betriebliche Anforderungen miteinander verzahnt *(Bomhard et al. 2025).*

Ein zentraler Baustein in diesem Zusammenhang ist der sogenannte **In-situ-Datenzugang** – also der Zugriff auf Daten direkt am Ort ihrer Speicherung, ohne Übermittlung einer Datenkopie. In der juristischen Literatur wird vertreten, dass ein solches Leserecht auf einem vom Dateninhaber kontrollierten Server die Anforderungen des Data Act grundsätzlich erfüllen kann. Aus Sicht des Dateninhabers ist dies ein wertvolles Instrument zur Wahrung der Kontrolle über die relevanten Daten: Die Gefahr der Zusammenführung und Analyse sensibler Datenbestände durch Dritte wird reduziert, ebenso wie das Risiko des Abflusses von Geschäftsgeheimnissen.

Teilweise wird der In-situ-Zugang aber auch abgelehnt: Zwar wird er derzeit als zulässiger Mindeststandard angesehen, doch ist unklar, ob die reine Leseoption auf Dauer dem Grundgedanken eines effektiven und nutzerorientierten Datenzugangs genügt, insbesondere dann, wenn daraus faktisch keine

Weiterverarbeitung möglich ist. Unternehmen sollten daher eine flexible Architektur entwickeln: Während hochsensible Daten bevorzugt ausschließlich in-situ zugänglich gemacht werden könnten, kann für weniger kritische Datenarten eine Möglichkeit zur Datenkopie eingeräumt werden, z.B. nach erfolgreicher Verhandlung oder über ein digitales Vertragsverhältnis gem. Art. 4 Abs. 13 Data Act. Dies kann etwa über eine Registrierungspflicht oder die Akzeptanz von Online-Nutzungsbedingungen direkt in der Benutzeroberfläche oder im Nutzerkonto erfolgen.

Vor diesem Hintergrund ergibt sich eine doppelte Gestaltungsaufgabe: Einerseits müssen Unternehmen einen organisatorischen Rahmen schaffen, in dem berechtigte Zugangsverlangen bearbeitet und umgesetzt werden können. Andererseits ist ein technisches und vertragliches Instrumentarium zu entwickeln, das vorliegende Schutzinteressen wahrt.

3.1.6 Vorläufiges Fazit dieses Kapitel und weitere Forschungsfragen

Der aktuelle Stand in Unternehmen hinsichtlich der Vorbereitung und Umsetzung der Regelungsinhalte des Data Act ist unterschiedlich und teilweise geprägt von Unsicherheit, längerem Abwarten, teilweise geringem Bewusstsein, wenig Anpassungsbereitschaft und zurückhaltender Investitionslust *(Podszun, 2021).* Die Implementierung effizienter datenbezogener Prozesse wird maßgeblich durch die unklare rechtliche Entwicklung des Data Act erschwert, was auch an der bislang fehlenden einschlägigen Rechtsprechung sowie etablierten Best Practices, die als Orientierungshilfe für die praktische Umsetzung dienen könnten, liegt.

Vor diesem Hintergrund stellt sich die Frage, wie Unternehmen ihre **Vertrags- und Datenmanagementprozesse** so strukturieren können, dass die Erfüllung der rechtlichen Pflichten gewährleistet ist. Nach Art. 41 Data Act hat die EU-Kommission vor Inkrafttreten der Verordnung unverbindliche Mustervertragsklauseln für die in den Kapiteln II und III geregelten Datenbereitstellungspflichten sowie unverbindliche Standardvertragsklauseln für Cloud-Computing-Verträge nach Kapitel VI entwickelt. Zur Vorbereitung dieser Texte wurde die *Expert Group on B2B Data Sharing and Cloud Computing Contracts* eingesetzt, die am 2. April 2025 ihren Abschlussbericht vorlegte. Das 183 Seiten umfassende Dokument enthält die von der Expertengruppe erarbeiteten Klauselvorschläge *(der finale Bericht ist abrufbar unter:*
https://www2.morihamada.com/ss/uploads/files/Final%20Report_Expert%20Group_02.04.2025.pdf).
Ein relevanter Aspekt, der sich in der Praxis herauskristallisieren dürfte, ist die organisatorische Einbettung des Datenmanagements in Unternehmen: Wird die traditionell auf personenbezogene Daten fokussierte Datenschutzabteilung zukünftig um Einheiten für Datenzugang und Datenweitergabe erweitert, obwohl diese Bereiche oft divergierende Interessen vertreten? Oder werden stattdessen eigenständige Datenmanagement-Teams etabliert, die spezifisch auf die Anforderungen des Data Act zugeschnitten sind?

Ferner sind die Ausgestaltung der Ausnahmen und Vorrangregelungen im Zusammenspiel mit der DSGVO und dem Geschäftsgeheimnisschutz noch nicht abschließend geklärt. Hier bestehen taktische Spielräume, die Unternehmen im Spannungsfeld zwischen Compliance- und Vermeidungsstrategien nutzen können.

Wettbewerbsrechtliche Fragestellungen sind ebenfalls von Bedeutung, insbesondere hinsichtlich potenzieller Beschränkungen oder Chancen, die der Data Act für die Nutzung zugänglich gemachter Daten bietet.

Zudem rückt die strategische Ausrichtung von Unternehmen im Umgang mit dem Data Act in den Fokus. Eine **Strategieentscheidung** betrifft die generelle Positionierung als **Early Adopter** oder **Late Adopter**. Daraus ergeben sich unterschiedliche Handlungsoptionen zwischen einer vollständigen oder teilweisen Umsetzung, hin zu einem gezielten Ausweichen. Einige Unternehmen wählen bewusst eine **Vermeidungsstrategie**, indem sie versuchen, ihre Produkte oder Dienstleistungen so gestalten, dass der Anwendungsbereich des Data Act möglichst nicht berührt wird.

Ob das überhaupt gänzlich möglich ist, wird sich zeigen. Andere setzen auf eine **„Go-with-the-Flow"-Strategie**, bei der durch Beobachtung der Rechtsentwicklung, vorläufige Ordnung der Datenbestände und risikoorientierte Priorisierung von Umsetzungsmaßnahmen eine flexible Reaktion auf regulatorische Konkretisierungen ermöglicht wird. Eine dritte Gruppe entscheidet sich für eine **proaktive Umsetzung**, also für die frühzeitige systematische Implementierung aller Anforderungen; einschließlich umfassender Compliance-Strukturen und angepasster Lizenz- und Vertragsmodelle, denn Data-Act-Compliance kann gegebenenfalls ein Wettbewerbsvorteil und eventuell auch ein Verkaufsargument sein.

Welche strategische Option sinnvoll erscheint, hängt maßgeblich von der Rolle von Maschinen- und Gerätedaten im Geschäftsmodell, der allgemeinen Compliance-Kultur sowie der wettbewerblichen Positionierung und Reputationssensibilität des Unternehmens ab. Zudem kann die unvollständige und stark einzelfallabhängige rechtliche Absicherung nicht-personenbezogener Daten wie Maschinen- und Sensordaten zu beträchtlicher Rechtsunsicherheit für Unternehmen führen. Diese Unsicherheit kann sich negativ auf ihre Bereitschaft auswirken, Daten zu teilen *(Podszun, 2021).*

Vor diesem Hintergrund lassen sich folgende **Thesen** formulieren, aus denen sich zugleich weiterführende Forschungsfragen ergeben:

- **These 1:** Unternehmen mit robusten Data-Governance-Strukturen sind besser in der Lage, den gesetzlichen Anforderungen des Data Act zu entsprechen, Datenzugänge und Datenzugangsansprüche zu managen und Chancen des Data Act strategisch zu nutzen.
- **These 2:** Kleine und mittelständische Unternehmen stehen aufgrund begrenzter Ressourcen vor größeren Herausforderungen bei der Data-Act-Compliance als größere Unternehmen, trotz der im Data Act vorgesehenen Privilegien für KMU.
- **These 3:** Unternehmen, die sich für eine für sie passende Strategie entscheiden und verfolgen, können langfristig Wettbewerbsvorteile aus der Umsetzung des Data Act ziehen, wobei fehlgeschlagene oder fehlkalkulierte Vermeidungsstrategien das Risiko von Rechtsverstößen und damit verbundenen Sanktionen erhöhen.
- **These 4:** Die vagen Vorgaben zur Ausgestaltung der Datenlizenzen im Data Act sowie die sehr generellen Musterklauseln der EU-Kommission erschweren die Vertragsgestaltung und stellen eine Hürde für die schnelle praktische Umsetzung von Datenzugangs- und Nutzungsvereinbarungen dar.

Die derzeitigen Mustervertragsklauseln bieten in ihrer aktuellen Entwurfsform nur begrenzten Schutz für Geschäftsgeheimnisse und bedürfen wesentlicher Ergänzungen, um praktikabel zu sein.

3.2 Open Data Innovation

Einfluss des EU Data Act auf die Innovationsfähigkeit von Unternehmen: Chancen wahrnehmen, Risiken mildern

Zusammengefasst: Das Kapitel betrachtet die Wirkung des EU Data Acts auf den Innovationsprozess und die Innovationsfähigkeit von Unternehmen. Es fasst den aktuellen Stand dieser Projektperspektive im August 2025 zusammen.

Primäres Ziel des EU Data Acts ist es, die große Menge und das große Potenzial bislang ungenutzter Daten in Innovationen zu überführen. Dies ist möglich, da die neue Regulierung den Zugang zu bisher nicht oder kaum zugänglichen Daten neu geregelt wird und diese den Status von quasi offenen Daten einnehmen (anstelle eines de facto Eigentums über die Daten). Dies gilt insbesondere in einer spezifischen Form eines Ökosystems aus Dateninhaber, Nutzer und Datenempfänger (Dritter).

Doch werden aus Daten nicht automatisch Innovationen, vielmehr müssen ermöglichende Bedingungen geschaffen und potenzielle Hürden abgebaut werden. Dabei muss zunächst verstanden werden, wie der EU Data Act die Wertschöpfung im Ökosystem und in den Unternehmen verändert. Den Ausgangspunkt dazu bilden verschiedene Datenarten, die im Ökosystem geteilt werden, der neue Zugang zu diesen Daten im Ökosystem, wie diese Daten den Innovationsprozess verändern und welche Kompetenzen (Literacy) und organisationalen Rahmenbedingungen es im Umgang mit diesen Daten braucht. Diese Aspekte stehen aus der Perspektive «Open Data Innovation» im Zentrum des weiteren Projektverlaufs.

3.2.1 Ziel des EU Data Acts: Aus Daten werden Innovationen

Veränderung und Innovation als Chance begreifen. Primäres Ziel des EU Data Acts ist es, Unternehmen Zugang zu Daten ermöglichen, die bis anhin kaum oder gar nicht zugänglich waren. Meist geht es dabei um Maschinendaten, die über Sensorik gewonnen werden. Mithilfe dieser Daten und damit Zugang zu neuem Wissen und neuen Einsichten sollen letztlich Innovationen ermöglicht und angestossen werden, um neue Produkte, Services oder Geschäftsmodelle auf dem Markt zu etablieren *(European Commission 2022, 2024)*. Dies ist eine Möglichkeit, um in einer sich schnell verändernden Situation wettbewerbsfähig zu werden oder zu bleiben. Dabei ist der EU Data Act nicht nur eine Reaktion auf zahlreiche Veränderungen, denen Unternehmen aktuell begegnen müssen, sondern auch die damit neu einhergehenden rechtlichen Vorgaben stellen selbst eine solche (nicht immer einfach zu greifende) Veränderung für Unternehmen dar.

Unternehmen und Individuen sind heute mit zahlreichen Veränderungen und Unsicherheiten konfrontiert, die oft mit dem Begriff VUCA (volatil, uncertain, complex, ambiguous) oder ähnlichen Bezeichnungen umschrieben werden. Im Kern wird dabei eine Situation skizziert, die sich schnell entwickelt und (strategische) Planung nahezu verunmöglicht. Vielmehr braucht es in einer solchen

Situation Flexibilität und Unternehmergeist. Neue (oft digitale) Technologien spielen im Rahmen vieler Entwicklungen und neuer Trends eine zentrale Rolle, indem sie den Anstoß für diese Veränderungen geben, wie z.B. Künstliche Intelligenz. Denn innovative Technologien haben das Potenzial, sowohl etablierte Spielregeln auf Märkten als auch die Art und Weise wie Wertschöpfung stattfindet und konfiguriert ist, grundlegend zu verändern.

Für Unternehmen ist dies sowohl mit Chancen als auch **Herausforderungen** verbunden. Herausforderungen insofern, dass etablierte, funktionierende Prozesse, Kompetenzen, Geschäftsmodelle oder auch Geschäftsbeziehungen möglicherweise obsolet werden und neu verhandelt und gestaltet werden müssen. Chancen insofern, als dass sie Anstoß oder auch Inspirationsquelle für die Weiterentwicklung des eigenen Unternehmens und für neue Optionen auf dem Markt sein können, vorausgesetzt, sie werden rechtzeitig erkannt und ergriffen. Veränderungen und innovative Ideen können dann zu einer besseren Marktposition oder generell zu neuen Vorteilen im Wettbewerb führen.

Tendenziell fokussieren sich oft junge, kleine Unternehmen (Startups) proaktiv auf entstehende Chancen, während etablierte Unternehmen Veränderungen oft als Herausforderungen oder als Bedrohung des Etablierten interpretieren und sich eher defensiv verhalten. Junge Unternehmen haben wenig zu verlieren, aber viel zu gewinnen, etablierte Unternehmen gehen größere Risiken ein, eine gute Position im Wettbewerb zu verlassen. Aus strategischer Sicht lohnt es sich jedoch auch für etablierte Unternehmen, Veränderungen als Chance zu begreifen, um sich proaktiv neu (und besser) im Wettbewerb aufzustellen – denn defensive Verhaltensweisen zögern notwendige unternehmerische Veränderungen oft nur hinaus und nicht immer werden diese letztlich noch rechtzeitig ergriffen. Es ist daher zwar unbequemer, aber oft sinnvoll, Veränderungen frühzeitig aufzugreifen und auch als etabliertes Unternehmen proaktiv tätig zu werden. Dies gilt auch vor dem Hintergrund des EU Data Acts, der vor allem Innovationen anstoßen soll.

Künstliche Intelligenz und Daten: Zwei Seiten der gleichen Medaille. Verschiedene Arten von Innovationen spielen in diesem Prozess eine zentrale Rolle: Innovative Produkte, Prozesse und Services lösen Kundenbedürfnisse auf eine neue, oft bessere, intelligentere oder schnellere Art und Weise, als dies bisher der Fall war. Sie sind oft Bestandteil innovativer Geschäftsmodelle oder sie sind mit innovativen Management- und Arbeitsmethoden verbunden, welche durch sie erst möglich werden. Dabei entsteht eine paradoxe Situation: Je schneller Veränderungen stattfinden, umso mehr Innovation braucht es, um sich im Wettbewerb zu behaupten und je mehr Innovationen umgesetzt werden, umso schneller verändert sich die Situation wiederum, so dass noch mehr Unsicherheit entsteht *(Furr & Dyer, 2014).*

Spätestens seit November 2022 besteht mit der Öffnung des Open.AI Large Language Modells ChatGPT für die Öffentlichkeit kein Zweifel mehr daran, dass Künstliche Intelligenz ein erhebliches Potenzial hat, viele etablierte Prozesse, Produkte, Geschäftsmodelle grundlegend in Frage zu stellen. Auch wenn Unternehmen in den letzten Jahren kontinuierlich mit neuen Technologien oder sich wandelnden politischen Verhältnissen konfrontiert waren, so ist die aktuelle Situation doch anders. Denn Künstliche Intelligenz ist nicht nur eine komplexe Technologie, ihre Weiterentwicklung zeigt eine bisher noch nie dagewesene Geschwindigkeit und wirkt so (wie oben beschrieben) als Katalysator.

Künstliche Intelligenz entwickelt sich in rasantem Tempo während Unternehmen nach umsetzbaren Anwendungsfällen suchen, um von der Technologie zu profitieren. Jedoch ergeben sich geeignete Anwendungsfälle nicht automatisch, da sie grundlegend in bestehende Wertschöpfungssysteme eingreifen kön-

nen. Um deren Potenzial abzuschöpfen, braucht es dann auch grundlegende Modifikationen der Wertschöpfungskonfiguration (z.B. neue Geschäftsmodelle oder Ökosysteme), die erst noch definiert werden müssen. Daher sind zunächst (noch) viele Fragen unbeantwortet. Und doch ist klar, Künstliche Intelligenz hat das Potenzial, die etablierte Wertschöpfung ganz neu zu strukturieren und eine neue Logik zu etablieren. Künstliche Intelligenz gilt daher auch als ein typischer Fall von Disruption *(Christensen, 2016)*.

Daten und Künstliche Intelligenz sind dabei zwei Seiten der gleichen Medaille. Denn die blosse Anwendung von Künstlicher Intelligenz führt noch nicht zu Vorteilen im Wettbewerb. Vielmehr wird sich durch ihre Nutzung ein neuer Standard in zahlreichen Industrien etablieren, der den Einsatz der Technologie normalisiert, also mittelfristig voraussetzt. Es wird dann normal, Künstliche Intelligenz für bestimmte Tätigkeiten und Prozesse zu nutzen, z.B. um die Produktivität zu steigern. Zwar steht dann vielen Wettbewerbern die gleiche Technologie zur Verfügung (so dass dadurch kein Vorteil im Wettbewerb generiert wird). Es ist jedoch möglich, über die Menge und Qualität an verfügbaren Daten, die zum Training der Künstlichen Intelligenz eingesetzt werden, bessere Ergebnisse als Wettbewerber zu erzielen. Je mehr Daten verfügbar sind und je höher deren Qualität, umso besser das Ergebnis. Die Nutzung von Künstlicher Intelligenz bringt also einen grossen Datenhunger mit sich.

Um diesen zu stillen, müssen grosse Mengen an Daten nicht nur zugänglich sein, sondern sie müssen häufig auch mit anderen Unternehmen geteilt werden. Sie können dann eine Quelle darstellen, um Innovationen anzustossen *(z.B. Aaser et al., 2020)*. Oft entstehen Daten im industriellen Kontext gerade an der Schnittstelle zwischen verschiedenen Akteuren, z.B. wenn eine Maschine vom Hersteller an einen Kunden ausgeliefert und dann in Betrieb genommen wird. Der EU Data Act kann vor diesem Hintergrund als Anstoss für Veränderungen gesehen werden, die zwar einerseits mit zahlreichen Unwägbarkeiten und Unsicherheiten für Unternehmen verbunden sind. Andererseits aber auch als eine Möglichkeit, Zugang zu Daten (also neue Ressourcen) zu erhalten, die bisher nicht zugänglich waren. Im Sinne der Europäischen Kommission können diese Daten dann idealerweise in Innovationen transferiert werden. Doch ist es wirklich so einfach?

Aus Daten werden Innovationen: Voraussetzungen und Hürden. Jedoch unterscheidet sich dieser Innovationsprozess im Hinblick auf einige Charakteristika von einen traditionellen Innovationsprozess und Unternehmen sollten sich zunächst einen Überblick über die grundlegenden Zusammenhänge verschaffen. Diese Zusammenhänge zu verstehen ist Gegenstand des laufenden Forschungsprojektes «Data Act Pioneer» (Laufzeit 2024-2027) und Zielsetzung für die kommenden Monate.

Im Zentrum stehen dazu die in Abbildung 5 überblicksartig aufgezeigten Kernelemente und Zusammenhänge, die relevant für die Reise, die Daten auf dem Weg hin zu Innovationen sind: **(1) Charakteristika von Daten, (2) neuer Daten-Zugang & -Teilen, (3) veränderter Innovationsprozess; (4) notwendige Daten-Kompetenz (Literacy) & ermöglichende organisationale Rahmenbedingungen.**

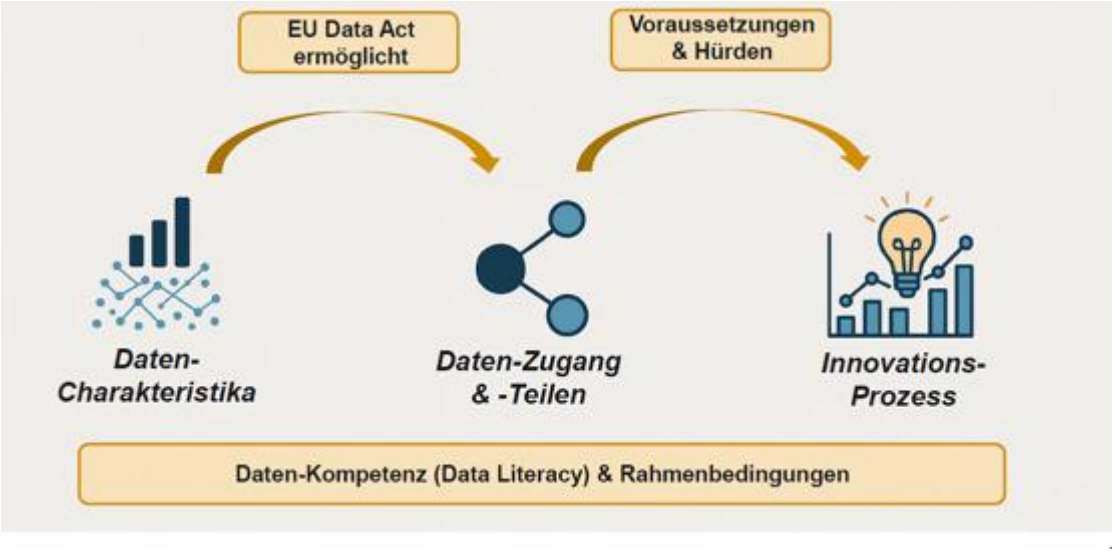


Abbildung 5

Aus Daten werden Innovationen: Vorrausetzungen und Hürden. Eigene Darstellung, Abbildung erstellt mithilfe von ChatGPT.

Den Ausgangspunkt bilden verschiedene **Datenarten**, aus denen anhand von Analysen Wissen gewonnen werden kann, welches unter anderem Auskunft über die Nutzung von Geräten, das Kundenverhalten oder andere Sachverhalte liefert. Oft müssen dazu Daten aus verschiedenen Quellen kombiniert analysiert werden. Doch welche Daten liegen vor, welche braucht es? Der EU Data Act ermöglicht neu den **Zugang zu Daten**, die bislang nicht oder nur in begrenztem Ausmaß verfügbar waren, da sie nur einem Akteur zugänglich waren. Zwischen den involvierten Akteuren (Dateninhaber, Nutzer, Datenempfänger (Dritter)) werden bestimmte Daten aufgrund der neuen Gesetzgebung nun offengelegt, sie werden innerhalb des Ökosystems zu **offenen Daten**. Diese können einerseits in den **Innovationsprozess** einfließen und diesen grundlegend neugestalten. Wie findet auf dieser Grundlage dann Innovation statt? Andererseits kommt es möglicherweise auch zu einer neuen Gestaltung der Beziehung zwischen den **Akteuren im Ökosystem**: Stehen diese in einer Beziehung des Wettbewerbs, der Kooperation, oder sowohl als auch, also Co-Opetition *(siehe z.B. Kugler & Plank, 2021)*? Und schließlich müssen die Mitarbeitenden in den Unternehmen befähigt werden, mit Daten im Alltag umzugehen, sie brauchen die notwendige **Daten-Kompetenz** (oder Data-Literacy) und die erforderlichen organisationalen Rahmenbedingungen, um dies zu tun.

Die nachfolgenden Abschnitte diskutieren diese Elemente genauer.

3.2.2 Wie ändert sich der Stage-Gate® Innovationsprozess durch den Datenzugang?

Zur Planung und Steuerung von Produktentwicklungsprojekten haben sich in Unternehmen prozessorientierte Strukturmodelle etabliert, die den zeitlichen Ablauf entlang definierter Entwicklungsphasen systematisieren *(Schuh, 2012).* Hierzu nutzen Unternehmen strukturierte Modelle wie das weit verbreitete Stage-Gate® Modell von R.G. Cooper (2008). Dieser Prozess stellt ein etabliertes Vorgehensmodell für die strukturierte Produktentwicklung dar. Er untergliedert den Innovationsprozess in eine Abfolge von Phasen (Stages), in denen definierte Aktivitäten durchgeführt werden, sowie in Entscheidungspunkte (Gates), an denen über die Fortführung des Projekts entschieden wird *(Cooper, 2008).* Im Verlauf jeder Phase des Stage-Gate®-Prozesses kommt der systematischen Erhebung, Verarbeitung und Auswertung von Daten eine zentrale Bedeutung zu. Unternehmen verfügen hierzu über vielfältige Datenquellen, die sich nach Strukturierungsgrad und Herkunft differenzieren lassen *(Babu et al., 2024).* Dazu zählen:

- **Unstrukturierte Daten** wie Texte aus Social-Media-Aktivitäten, audiovisuelle Inhalte oder Kundenfeedback;
- **strukturierte Daten** wie Transaktions- oder Stammdaten aus internen Datenbanken;
- sowie **maschinell generierte Daten**, die z. B. durch Sensoren im Rahmen von Industrie-4.0-Anwendungen gewonnen werden.

In industriellen Innovationsprozessen spielen zunehmend maschinell erzeugte Daten eine zentrale Rolle. Sie ermöglichen es Unternehmen, Echtzeitinformationen über physikalische und betriebliche Prozesse zu gewinnen, wodurch operative Effizienz gesteigert, Anomalien frühzeitig erkannt und Innovationspotenziale identifiziert werden können *(SECO, o.J., Stucki et al., 2024).* So werden in der industriellen Fertigung mittels Sensorik typischerweise folgende Daten erfasst:

- **akustische Signale** (z. B. zur Maschinenüberwachung);
- **visuelle Merkmale** (z. B. Bilddaten zur Qualitätskontrolle);
- sowie **prozessbezogene Daten** wie Energieverbrauch, Vibrationen, Druck, Temperatur und elektrische Spannung, um nur die wichtigsten zu nennen.

Die systematische Analyse dieser Daten liefert tiefgreifende Einsichten in die Funktionsweise und den Zustand technischer Systeme. Diese Erkenntnisse können sowohl zur Optimierung bestehender Anlagen als auch zur Entwicklung neuartiger Produkte und Prozesse genutzt werden *(Babu et al., 2024)*. Die zunehmende Integration des Internets der Dinge (IoT) sowie der breitere Zugang zu Maschinendaten verändern die Rolle von **Innovationsmanagern** fundamental. Mit dem geplanten Data Act verfolgt die Europäische Union das Ziel, diese Entwicklung gezielt zu fördern. Der Gesetzesentwurf soll den Zugang zu Maschinendaten, die durch die Nutzung vernetzter Produkte oder zugehöriger Dienstleistungen generiert werden, sowohl für Hersteller und Nutzer als auch für Drittparteien erleichtern *(Pliauskaite, o. J.; Strittmatter et al., 2025).*

Für das **Innovationsmanagement** ergeben sich daraus weitreichende Konsequenzen in drei zentralen Bereichen:

- **datengetriebene Entscheidungsprozesse;**
- **beschleunigte Innovationszyklen;**
- **kundenzentrierte Geschäftsmodellinnovation**

Mit dem verbesserten Zugang zu Maschinendaten im Zuge zunehmender IoT-Integration stehen auch etablierte **Innovationsprozesse** vor einem Wandel. Insbesondere der klassische Stage-Gate-Prozess, lange Zeit als Standardmodell für das Management von Innovationsvorhaben etabliert, muss neu gedacht werden *(Tesch et al., 2017; Trott et al., 2022; tntra.com, o. J.).* Durch die Verfügbarkeit von Echtzeitdaten und kontinuierlichem Feedback aus vernetzten Produkten ergeben sich neue Anforderungen – und neue Chancen – für das **Prozessdesign:**

- **agile und hybride Prozessmodelle;**
- **datengetriebene und dynamische Entscheidungspunkte;**
- **Iteration und Prototyping**

Der Innovationsprozess der Zukunft wird daher voraussichtlich nicht starr, sondern dynamisch, lernorientiert, daten- und KI-basiert sein. Aber nicht jedes Projekt profitiert vom gleichen Innovationsmodell. Während digitale, datengetriebene oder hochgradig unsichere Innovationsvorhaben einen flexiblen und adaptiven Prozessansatz benötigen, können Projekte mit klaren Anforderungen und geringer Komplexität weiterhin von der klassischen Stage-Gate®-Disziplin profitieren. Die Zukunft liegt in einer kontextsensitiven Prozessgestaltung. Innovationsmanager:innen stehen vor der Herausforderung, Strukturen zu schaffen, die sowohl eine zielgerichtete Steuerung als auch ein agiles Reagieren auf neue – insbesondere durch Echtzeitdaten gewonnene – Erkenntnisse ermöglichen. Eine zentrale Rolle nehmen dabei als Folge des EU Data Acts sowohl frei zugängliche Daten (Open Data) als auch die besondere Form eines Ökosystems mit den drei genannten Akteuren (Dateninhaber, Datennutzer, Datenempfänger (Dritter)) ein.

3.2.3 Die Bedeutung von Open Data

Hersteller sichern sich bislang durch technisches Design eine faktische Kontrolle über die von ihren Produkten generierten IoT-Daten. Dieses De-facto-Eigentum über diese Daten ermöglicht ihnen eine exklusive Position, obwohl keine formalen Eigentumsrechte bestehen *(Eckardt & Kerber, 2023).* Die daraus resultierenden Datensilos behindern Innovationen sowie den Wettbewerb und stehen der Entstehung offener Datenökosysteme entgegen. Dies ist ein möglicher Grund, warum ein Grossteil der erhobenen Daten (nach Schätzung der Europäischen Kommission, 2023, sind dies etwa 80%) nicht weiter genutzt werden).

Der Data Act zielt darauf ab, diese Strukturen aufzubrechen. Erwägungsgrund 32 greift auf, dass die Entscheidung gegen Exklusivität an Daten dem Ziel der Verordnung, Innovation im Bereich der

Datenwirtschaft anzuregen, dient. Durch regulierte Zugänge zu nicht-personenbezogenen IoT-Daten soll Innovation ermöglicht werden, die bislang durch exklusive Datenkontrolle blockiert war *(Strittmatter et al., 2025).* Gleichzeitig soll der Wettbewerb gestärkt werden, insbesondere auf sogenannten sekundären Märkten wie Wartung, Reparatur oder Datenanalyse, wo datenbasierte Dienste bislang kaum Fuss fassen konnten *(Ridgway et al., 2025).* Ein weiteres Ziel ist ein fairerer Ausgleich der Wertschöpfung zwischen Herstellern, Nutzern und datenverarbeitenden Dienstleistern *(Martens, 2023).*

IoT-Daten sind **nicht-rivalisierende Ressourcen** – ihre Nutzung durch einen Akteur schließt die gleichzeitige Verwendung durch andere nicht aus *(Bertschek et al., 2021).* Diese Eigenschaft verleiht ihnen ein besonderes Potenzial für die datengetriebene Wirtschaft, da dieselben Daten mehrfach verwendet und vielfältig kombiniert werden können. Vor diesem Hintergrund spielt der Data Act eine zentrale Rolle. Er zielt darauf ab, die Nutzung von Daten sektorübergreifend zu erleichtern und stellt klar, dass interoperable Daten aus verschiedenen Bereichen die Wettbewerbsfähigkeit der europäischen Wirtschaft steigern können. **Interoperabilität** bedeutet dabei, dass Daten aus unterschiedlichen Quellen – etwa aus Maschinen, digitalen Plattformen oder komplexen Lieferketten – technisch und semantisch kompatibel sind und sich somit effizient zusammenführen und nutzen lassen. Durch diese kombinierte Nutzung entstehen neue Analyse- und Wertschöpfungspotenziale, die wiederum einen Innovationsschub darstellen können.

In diesem Zusammenhang gewinnt das Konzept der **Open Data Innovation** zunehmend an Bedeutung. Es bezeichnet die gezielte Öffnung nicht-personenbezogener IoT-Daten für externe Akteure, um über einen regulierten Zugang neue Anwendungen, Services und datenbasierte Geschäftsmodelle zu ermöglichen. Damit wird ein Rahmen geschaffen, der das wirtschaftliche Potenzial interoperabler Daten systematisch erschließt. Dabei steht nicht die vollständige Offenheit im Sinne eines „Open Access" im Zentrum, sondern die strukturierte Teilbarkeit unter Berücksichtigung legitimer Interessen wie Datenschutz oder dem Schutz von Geschäftsgeheimnissen. Ziel ist es, durch die Förderung liquider Datenmärkte die Nutzung vorhandener Datenressourcen zu intensivieren.

3.2.4 Daten-Kompetenz (Literacy) und organisationale Voraussetzungen

Um Daten im skizzierten Innovationsprozess gezielt einzusetzen, müssen jedoch bestimmte Voraussetzungen im Unternehmen erfüllt sein bzw. Hürden abgebaut oder vermieden werden. Die größten Hürden, um Daten im Unternehmen in Werte zu transferieren, liegen interessanterweise weniger im Bereich sogenannter «harter Faktoren» (z.B. fehlende Ressourcen, Unternehmen ist zu klein, Technologie) oder im Bereich der Daten selbst (z.B. Menge an Daten, Qualität der Daten), sondern sind vor allem die sogenannten «weichen Faktoren» (z.B. Organisation, fehlende Vision, Kultur *(Kugler et al., 2020).*

Die nachfolgenden Ausführungen konzentrieren sich insbesondere auf zwei dieser Faktoren **(1) Daten-Kompetenz und (2) Daten-Kultur.** Denn um mit Daten im Unternehmen gezielt arbeiten zu können, insbesondere im Kontext des Innovationsprozesses, müssen Unternehmen und ihre Mitarbeitenden zunächst auch befähigt werden, dies zu tun. Denn Daten sind eine besondere Ressource, die sich grundlegend von physischen Produkten unterscheidet. Im Zentrum stehen dabei einerseits die Daten-

Kompetenz (Data Literacy) der Mitarbeitenden. Andererseits geht es um eine ermöglichende Daten-Kultur & Mindset im Unternehmen, also die implizit und explizit vorherrschenden Werte, Normen und selbstverständliche Annahmen *(Mindset, Logik; siehe hierzu auch zu Kultur: Kugler, 2025; Kugler et al., 2024; zu Mindset: Kugler, 2023; 2020).* Doch was verbirgt sich tatsächlich hinter diesem Ansatz?

Daten-Kompetenz, KI-Kompetenz. Je stärker Daten zu einem Bestandteil des Innovationsprozesses werden, umso mehr wird **Daten-Kompetenz (Data-Literacy)** zu einer Schlüsselqualifikation in Unternehmen. Darunter versteht man allgemein die Fähigkeit, Daten in ihrem Kontext zu verstehen, kritisch zu hinterfragen, zu analysieren und in Handlung überführen zu können *(Schüller, 2020).* Es geht also vor allem darum, auf der Grundlage von Daten Entscheide zu treffen und Mitarbeitende dazu befähigen, diesen Prozess zu verstehen und durchzuführen. In datengetriebenen Organisationen ist diese Kompetenz zunehmend für alle Mitarbeitenden, Hierarchieebenen und Fachbereiche relevant, von der Produktentwicklung über das Marketing bis hin zum strategischen Management. Daten treten daher aus einer Randposition in den Mittelpunkt der Wertschöpfung *(Kugler, 2020).*

Im Innovationsprozess spielen Daten dabei eine doppelte Rolle: Einerseits dienen sie der Identifikation neuer Bedürfnisse, Trends und Entwicklungen, andererseits können sie in der Umsetzung von Innovationen zur kontinuierlichen Ideengenerierung, Evaluation und Optimierung oder der kommunikativen Aufbereitung und Visualisierung von Ideen und Prototypen beitragen. Unternehmen, die über ein hohes Maß an Datenkompetenz verfügen, sind insgesamt besser in der Lage, datenbasierte Geschäftsmodelle zu entwickeln, Kundendaten sinnvoll zu interpretieren und datengetriebene Innovationen gezielt zu steuern. Verstärkt geschieht dies darüber hinaus durch den Einsatz von Machine Learning Modellen, generative Künstliche Intelligenz und KI-Agenten, die den Innovationsprozess zunehmend automatisieren *(z.B. Bouschery et al, 2023; Eapen et al., 2023).* Insofern ist häufig die mit der Daten-Kompetenz verwandte KI-Kompetenz (KI-Literacy) gleichermassen relevant für Unternehmen. Darunter versteht man die Fähigkeit, Künstliche Intelligenz kritisch zu reflektieren und kompetent anzuwenden. Es geht darum, die Funktionsweise von KI-Systemen nachvollziehen, ihre Potenziale und Risiken einzuschätzen und deren organisationale und gesellschaftliche Auswirkungen bewerten zu können. Dabei geht es nicht nur um technisches Wissen und technischen Grundkenntnisse, sondern darüber hinaus auch um ethische, rechtliche und soziale Aspekte des Einsatzes Künstlicher Intelligenz, z.B. im Hinblick auf den Datenschutz im Unternehmen oder in einem gesellschaftlichen Kontext *(z.B. Long & Magerko, 2020; Ng et al., 2021).*

Für Unternehmen ergibt sich daraus ein klarer Handlungsauftrag: Datenkompetenz muss strategisch als organisationsweite Schlüsselqualifikation verstanden und gezielt gefördert werden – etwa durch interne Weiterbildungsprogramme, die Integration datenbezogener Kompetenzen in Führungsrollen oder die Verankerung von Zielen zur Daten-Kompetenz in der Innovationsstrategie. Nur wenn Mitarbeitende befähigt sind, Daten souverän zu nutzen und kritisch zu reflektieren, können Daten ihr volles Potenzial im Innovationsprozess entfalten. (siehe hierzu auch Tabelle 2).

Kompetenzbereich	Datenkompetenz (Data Literacy)	KI-Kompetenz (AI Literacy)
Verstehen & Einordnen	Verständnis von Datentypen, -quellen, -qualität	Gundverständnis von KI, ML, Algorithmen und Trainingsdaten
Sammeln & Generieren	Daten erheben, kuratieren und strukturieren	Wissen über Datengrundlagen für KI-Modelle und deren Erhebung
Analysieren & Interpretieren	Datenanalyse, statistisches Denken, Mustererkennung	Interpretation von KI-Ergebnissen, Verstehen algorithmischer Prozesse
Bewerten & Reflektieren	Kritische Bewertung von Datenquellen, Bias, Kontext	Reflektion über Fairness, Verzerrungen (Bias), Transparenz von KI
Kommunizieren & Visualisieren	Aufbereitung und Präsentation von Daten (z. B. durch Visualisierungen)	Erklären von KI-Systemen und deren Entscheidungsfindung
Anwenden & Umsetzen	Nutzung datenbasierter Erkenntnisse zur Entscheidungsfindung	Anwendung von KI-Tools im Alltag/Beruf, z. B. Chatbots, Empfehlungssysteme
Ethische & Rechtliche Aspekte	Datenschutz, Datenethik, Urheberrechte, Datenrechte	KI-Ethik, DSGVO, Verantwortung für automatisierte Entscheidungen

Tabelle 2: Übersicht Daten-Kompetenz und KI-Kompetenz.

Daten-Kultur, Mindset und Organisation. Die Organisationskultur eines Unternehmens spielt eine zentrale – womöglich sogar die entscheidende – Rolle im Umgang mit Daten allgemein und insbesondere im Innovationsprozess. Denn das Arbeiten mit oder das Teilen von Daten folgt einer anderen Logik als der Umgang mit physischen Produkten oder klassischen Dienstleistungen: Es handelt sich um eine daten-dominante Logik *(Kugler, 2020).* In dieser rücken Daten ins Zentrum der Wertschöpfung, statt nur eine von vielen Ressourcen darzustellen. Doch was kennzeichnet eine solche Kultur, und worauf müssen Unternehmen gezielt achten?

Organisationskultur beschreibt allgemein die Werte, Normen und Überzeugungen, die das Denken und Handeln von Mitgliedern einer Organisation leiten – sowohl auf expliziter als auch auf impliziter Ebene *(Schein, 1992).* In datengetriebenen Unternehmen zeigt sich eine entsprechende Kultur etwa darin, dass Entscheidungen mithilfe der Daten-Kompetenz verstärkt auf Analysen und Daten basieren, weniger auf persönlicher Intuition oder Erfahrung. Daher wird in diesem Kontext häufig von einer Entscheidungskultur gesprochen *(Vidgen et al., 2017).* Doch eine datenorientierte Kultur greift weit über **Entscheidungsprozesse** hinaus – sie beeinflusst Strukturen, Rollen und das organisationale Selbstverständnis. Drei Charakteristika sind dabei zentral: **(1) Daten als besondere Ressource erkennen), (2) Organisationale Grenzen durchlässig gestalten, (3) Strukturen, Rollen und Prozesse anpassen** *(siehe auch Kugler, 2025; 2023; Kugler et al., 2024).*

(1) Daten als besondere Ressource erkennen

Eine datenorientierte Organisationskultur basiert zunächst auf der Anerkennung von Daten als besondere Ressource, die sich fundamental von physischen oder immateriellen Unternehmensressourcen unterscheidet. Nicht alle Daten sind gleichermaßen wertvoll. So unterscheiden sich etwa operative Daten, die Effizienz steigern, von strategischen Daten, die Innovation ermöglichen (Kugler & Plank, 2021). Zudem besitzen Rohdaten meist weniger Wert als aufbereitete Analysen und Interpretationen. Sofern Daten mit anderen Unternehmen geteilt werden sollen, kann dies einerseits Wettbewerbsvorteile ermöglichen, birgt andererseits aber das Risiko, diese Vorteile zu verlieren. Daher sind viele Unternehmen unsicher, wie sie das Potenzial von Daten nutzen können, ohne Kontrolle oder Exklusivität einzubüßen. Insofern geht es zunächst darum, den potenziellen Wert von Daten und ihrer geteilten Nutzung im Ökosystem überhaupt zu verstehen und anzuerkennen – sowohl innerhalb der eigenen Organisation als auch bei Partnerunternehmen. Denn oft erschließt sich der tatsächliche Nutzen von Daten erst dann, wenn durch sie neues Wissen generiert werden kann.

(2) Organisationale Grenzen durchlässig gestalten

Zudem ist das Selbstverständnis der Organisation und der Art, wie interne und externe Grenzen definiert werden, relevant. Unternehmen agieren häufig stark abteilungsorientiert oder fokussieren auf das eigene Unternehmen – datenbasierte Wertschöpfung erfordert jedoch ein erweitertes, ökosystemisches Denken. Denn erst durch die Kombination von (Roh-)Daten mit vorhandenem Wissen können neue Wertschöpfungspotenziale entstehen.

Innerhalb eines Unternehmens braucht es hierfür eine enge Verzahnung zwischen technologischer Datenanalyse und betriebswirtschaftlicher Perspektive, insbesondere bei der Entwicklung von datenbasierten Geschäftsmodellen oder Nutzenhypothesen. Zwischen Unternehmen im Ökosystem ist eine partnerschaftliche Zusammenarbeit erforderlich, um potenzielle Anwendungsfelder oder Synergien gemeinsam zu identifizieren. So können beispielsweise reale Nutzungsdaten von Produkten neue Einsichten in Kundenverhalten liefern, wenn sie mit technischem Wissen und Geschäftsmodellkenntnissen kombiniert werden – die Basis für neue Services, Innovationen oder Use Cases.

(3) Strukturen, Rollen und Prozesse anpassen

Schließlich geht es um notwendige Veränderungen in der organisatorischen Infrastruktur. Eine datenorientierte Kultur setzt voraus, dass Daten zugänglich sind – sowohl technisch als auch prozessual. Oft ist unklar, wer Zugriff auf welche Daten haben darf, insbesondere bei sensiblen Informationen wie Kundendaten. Datengetriebene Organisationen zeichnen sich durch transparente und niedrigschwellige Zugangsregelungen aus – quer durch Hierarchien und Funktionsbereiche. Dadurch verändern sich Rollen, Prozesse und Strukturen nachhaltig. Wertschöpfung mit Daten erfordert dabei sowohl das Erkennen des Datenwerts als auch die Fähigkeit, diesen abzuschöpfen – etwa durch Analyse, Interpretation und Visualisierung. Hierfür müssen unternehmensinterne Strukturen flexibel genug sein, um neue Rollen und Verantwortlichkeiten zu integrieren. Die organisationale Struktur spiegelt die Bedeutung von Themen wie Daten auch symbolisch wider.

Empfehlungen: Schrittweise kultureller Wandel. Die Entwicklung einer datenfreundlichen Organisationskultur ist ein langfristiger Prozess, der nicht verordnet werden kann. Es empfiehlt sich daher ein schrittweises Vorgehen, das an verschiedenen Hebeln ansetzt: Zunächst sollten Mitarbeitende für das Potenzial von Daten sensibilisiert werden – etwa durch interne Botschafter:innen, die das Thema greifbar machen. Darauf aufbauend gilt es, Kompetenzen im Umgang mit Daten gezielt zu fördern.
Im nächsten Schritt sollten Zugänge zu Daten geschaffen und bestehende Grenzen – sowohl intern als auch im Ökosystem – geöffnet werden. Schließlich ist es wichtig, erfolgreiche Praxisbeispiele und erste Use Cases aktiv zu verbreiten und zu skalieren. So kann über konkrete Erfahrungen eine nachhaltige Veränderung in der kulturellen Verankerung des Themas Daten angestoßen werden.

3.3 IKT-Sicherheit

Sicherheitsansätze und neue Risiken im Zeitalter des Data Act

Zusammengefasst:

IKT-Sicherheit ist vielschichtig und wird rund um den Data Act um ein Spezifikum reicher. Deshalb ist es wichtig, strategische Betrachtungen und das Bedrohungsmanagement zu beleuchten, typische Angriffsvektoren im industriellen Umfeld zu analysieren und effektive **technische sowie organisatorische Schutzmaßnahmen (TOMs)** zu diskutieren. Zudem werfen wir einen Blick auf die Entwicklung neuartiger Dienstleistungen und Geschäftsmodelle unter dem Aspekt Sicherheit.

Dieses Kapitel befasst sich mit den vielschichtigen Aspekten der Cybersicherheit. Es werden die strategische Beratung und das Bedrohungsmanagement beleuchtet, typische Angriffsvektoren im industriellen Umfeld analysiert und effektive technische sowie organisatorische Schutzmaßnahmen diskutiert. Ein Augenmerk liegt dabei auf der Reaktionsfähigkeit bei Sicherheitsvorfällen und der Schadensbegrenzung. Des Weiteren werden die Themen Lastmanagement und Compliance im Rahmen von IT-Sicherheitsstandards behandelt. Zudem werfen wir einen Blick auf die Entwicklung neuartiger Dienstleistungen und Geschäftsmodelle, die auf Sicherheitsanforderungen basieren.
Bei der Betrachtung von IKT-Sicherheitsaspekten gibt es verschiedene Ebenen von Sicherheitsanforderungen. Eine mögliche Unterscheidung könnte zwischen kritischen Infrastrukturen, angrenzenden kritischen Infrastrukturen und anderen Unternehmen getroffen werden. Zu den kritischen Infrastrukturen gehören in der Regel die öffentliche Sicherheit, die elektrische Energieversorgung, die Kernenergie, die chemische Produktion, die landwirtschaftliche und pharmazeutische Produktion sowie der Vertrieb und in einigen Fällen auch das Bank- und Finanzwesen *(Knapp, 2024).* Die gemeinsame Wertschöpfung und die Entwicklung innovativer Dienstleistungen auf dieser Ebene können durch die Einhaltung von Vorschriften und Standardisierungsrahmen und deren strenge Ansätze in Bezug auf Datenintegrität und Datenaustausch behindert werden. Zu den an kritische Infrastrukturen angrenzenden Branchen gehören Sektoren, die von Regulierungsbehörden - wie Regierungen oder supranationalen Blöcken wie der EU - zwar nicht ausdrücklich als kritische Infrastrukturen eingestuft werden, aber dennoch eine entscheidende Rolle bei der Aufrechterhaltung der gesellschaftlichen Funktionalität und

Kontinuität spielen. Beispiele hierfür sind die Lebensmittelindustrie *(Hetzenauer et al., 2023)* oder Zulieferer von Anbietern Kritischer Infrastrukturen sowie Anbieter von Software und Lösungen für das Lieferkettenmanagement *(Topping et al., 2021).*

Bei der gemeinsamen Entwicklung neuer Dienste müssen, die von jeder Ebene vorgeschriebenen Auswirkungen berücksichtigt, werden. Es ist zu beachten, dass ein Unternehmen (oder insbesondere ein KMU) zwar nicht als kritische Infrastruktur oder als an kritische Infrastrukturen angrenzend eingestuft werden kann, aber möglicherweise ein Lieferant oder Dienstleister für kritische Infrastrukturen ist.

Im Folgenden werden primär Betrachtungen vorgestellt, welche für alle Unternehmen relevant sind. Im Falle von kritischen oder systemerhaltenden Infrastrukturen können zusätzliche Maßnahmen erforderlich sein.

Zudem ist anzumerken, dass folgende Betrachtungen sich nur auf Spezifika im Zusammenhang mit dem Data Act beziehen. Eine eingehende Beschäftigung und Implementierung von etablierten IT-Sicherheitsstandards (insb. ANSI/ISO Standards sowie Schutzmaßnahmen des BSI oder des österreichischen Informationssicherheitshandbuchs) wird empfohlen.

Allgemein kann es auch helfen, sich vor Augen zu führen, dass laut Data Act Dateninhaber und Inhaber eines Geschäftsgeheimnisses nicht dieselbe Person sein muss.

3.3.1 Strategische Cybersicherheitsbetrachtung & Bedrohungsmanagement im Kontext des Data Act

Die gemeinsame Wertschöpfung kann durch die Entwicklung von Dienstleistungen erreicht werden, indem die Sicherheit der IKT gewährleistet wird. Obgleich des Erfolgs der digitalen Transformation bleibt die IKT-Sicherheit oft ein zweitrangiger Aspekt. Aus einer ganzheitlichen strategischen Betrachtung, bleibt festzuhalten, dass der Data Act im Bereich Cybersicherheit neben den zusätzlichen Anforderungen im fortlaufenden IKT-Betrieb, zugleich eine Chance für eine ganzheitliche Wertschöpfung bieten kann. Die Einführung des Data Acts unterstreicht primär die Bedeutung der Implementierung von automatisiertem Datenaustausch unter Einhaltung der gesetzlichen Anforderungen. Diese Entwicklung hat abseits der technologischen und verwaltungstechnischen Auswirkungen ein Potential als Steigerung des Co-Creation Value genutzt werden zu können. Zu den spezifischen strategischen Überlegungen zur Informationssicherheit gehören die Verwaltung des Datenabrufs gemäß dem Data Act, die Vorschriften für Zwischenfälle sowie das Betriebsmanagement von IKT-Sicherheitsüberlegungen. Übergeordnet muss eine Abwägung zu Kosten- & Nutzen sowie der Risikotoleranz des Unternehmens stehen *(Meier & Burda, 2019).*

Auf der strategischen Ebene der Klassifikation von Gefahren, engl. ‚Threats', *(Jouini & Rabai, 2016)* für ein Risiko- und Bedrohungsmanagements *(Al-Mhiqani et al., 2019)* müssen mindestens folgende Gefahrenklassen betrachtet werden:

- **Lokale operative Gefahren**, welchen den laufenden Betrieb gefährden (Beispiel: Maschinenverfügbarkeit ist aufgrund vieler Anfragen oder aufgrund einer Infiltration der Maschine gefährdet)

- Operative **Gefährdung von Unternehmen** (Beispiel: Schnittstellen für automatisierte Data Act-Abfragen werden für Infiltration genutzt)
- **Datenabfluss** (Beispiel: Unbeabsichtigter Abfluss sicherheits-relevanter oder unternehmenskritischer (Meta-)Daten als Teil von Maschinendaten)
- **Datenintegrität** (Beispiel: Gefährdung von Reputation oder Folgeschäden, welche aus Datenmanipulation unter Nutzung von Schwachstellen in Schnittstellen resultiert)
- **Reconnaissance** (Beispiel: Nutzung von (Meta-)Daten um Reconnaissance von Unternehmensinterna oder der IKT-Sicherheitsmaßnahmen zu betreiben)

Alle Gefahrenklassen können sowohl aus Sicht des bereitstellenden Unternehmens / Dateninhabers oder betreibenden Unternehmens / Datenutzer getroffen werden.
Abschließend ist es wichtig zu verstehen, dass oben genannte Gefahrenklassen nicht neu sind, jedoch potenziell neue Angriffsvektoren für diese Klassen in der Umsetzung des Data Acts geschaffen werden. Insbesondere die Gefahrenklassen des Datenabfluss sowie Reconnaissance sind aufgrund der Natur der Anforderungen des Data Act als kritisch zu betrachten.

3.3.2 Kritische, gängige Angriffsvektoren im maschinellen industriellen Kontext

Im maschinellen industriellen Kontext stehen die Angriffsvektoren Datenabfluss und Reconnaissance im Fokus, da der Data Act den Austausch von maschinengenerierten Daten explizit fördert.
Datenabfluss als Angriffsvektor. Der Datenabfluss (engl.: Data Exfiltration) bezeichnet das unerlaubte Kopieren, Verschieben oder Übertragen von sensiblen Daten von einem geschützten Netzwerk. Im industriellen Kontext können dies beispielsweise Betriebsgeheimnisse, geistiges Eigentum, Produktionsdaten oder personenbezogene Informationen sein. Es können Einfallstore geschaffen werden, da Schnittstellen für den Datenabruf, die für legitime Zwecke geschaffen wurden, auch von böswilligen Akteuren missbraucht werden können. Ein typischer Angriffsvektor ist die Ausnutzung von Schwachstellen in den APIs (Application Programming Interfaces) oder in den Protokollen, die für den Datenaustausch genutzt werden. Wichtig ist dabei zu beachten, dass sowohl Daten als auch Meta-Daten (bspw. Datenbank-Schema, Domänenmodelle, Prozessschritte, o.ä.) abfließen können.
Reconnaissance technischer Infrastruktur als Angriffsvektor. Reconnaissance oder Aufklärungsmaßnahmen sind oft der erste Schritt in Cyberangriffen, bei dem böswillige Akteure Informationen über das Zielsystem sammeln, um Schwachstellen zu identifizieren. Im Kontext des Data Act ist dieser Vektor besonders kritisch, da die bereitgestellten Daten – auch Metadaten – wertvolle Einblicke in die Systemarchitektur, die genutzte Software und die Sicherheitsmaßnahmen eines Unternehmens geben können. Angreifer können diese Informationen nutzen, um eine Landkarte der IT-Infrastruktur zu erstellen, potenziell verwundbare Systeme zu lokalisieren und maßgeschneiderte Angriffe vorzubereiten. Die über den Data Act zugänglichen Daten könnten beispielsweise Aufschluss darüber geben, welche Maschinentypen oder Softwareversionen im Einsatz sind, welche Kommunikationspfade existieren und wie das Lastmanagement (bspw. Content Delivery Networks, CDN) funktioniert. Diese Informationen erleichtern das Auffinden von Zero-Day-Exploits oder bekannten Schwachstellen, um gezielte Angriffe durchzuführen.

Reconnaissance unter Nutzung von Daten. Die Reconnaissance im Kontext des Data Act kann zudem eine neue Dimension erhalten, wenn frei verfügbare oder leicht zugängliche maschinengenerierten Daten eine Fülle von ableitbaren Informationen erhalten. Böswillige Akteure können mithilfe von Methoden aus der Data Science und statistischen Werkzeugen wertvolle, sicherheitskritische Erkenntnisse gewinnen. So kann ein böswilliger Akteur bspw. die über eine Schnittstelle abrufbaren Betriebsdaten einer Maschine analysieren. Allein durch die statistische Auswertung von Metadaten wie der Datenerhebungsfrequenz, dem Datenvolumen oder Zeitstempeln lassen sich Rückschlüsse auf Auslastung, Produktionszyklen, Wartungsintervalle, Schichtintervalle oder geographischer Ort, u.a. ziehen. Auch Anomalien in den Datenströmen können Aufschluss über Schwachstellen oder ungewöhnliche Konfigurationen geben. Solche aus den Daten gewonnenen Informationen können als Grundlage für Cyberattacken dienen, die speziell auf die Schwachstellen des Unternehmens zugeschnitten sind.

Wirksame Beispiele einer Cyberattacke basierend auf der Nutzung dieser statistisch ermittelten Information sind Social Engineering Angriffe. So kann bspw. mittels des Wissens um Schichtwechsel gezielt die verringerte Aufmerksamkeit genutzt werden; Phishing-Mails können gezielt vor oder nach einem Wartungsintervall gesendet werden; Spear-Phishing-Angriffe können gezielt auf relevante Personen basierend auf Echtzeitdaten erfolgen; böswillige Akteure können sich telefonisch oder in der Produktionsstätte glaubwürdig als Wartungspersonal ausgeben; u.v.a.

Allgemein können alle Maßnahmen der Reconnaissance auch genutzt werden, um öffentlich vorhandene Information ohne Sicherheitsbezug zu sammeln, um so einen betriebswirtschaftlichen Vorteil zu schaffen.

3.3.3 Reaktion auf Sicherheitsvorfälle & Schadensbegrenzung

Ein proaktiver Ansatz in der Cybersicherheit ist unerlässlich, jedoch ist die vollständige Prävention aller Sicherheitsvorfälle meist praktisch unmöglich. Daher ist ein effektives Incident Management und eine schnelle Schadensbe- oder -eingrenzung von entscheidender Bedeutung, um die Auswirkungen von Angriffen zu minimieren und die Geschäftskontinuität sicherzustellen.

Das Incident Management ist ein strukturierter Prozess zur Erkennung, Analyse, Behebung und Dokumentation von Sicherheitsvorfällen. Im Rahmen der (technischen) Implementierung des Data Acts macht es Sinn, Maßnahmen etablierter IT-Sicherheitsstandards (insb. Verantwortlichkeiten, Richtlinien, Verfahren, Check-Listen) für den Umgang mit Zwischenfällen abzugleichen. Organisatorisch umfassen diese Erkennung des Vorfalls, Isolierung betroffener Systeme, sowie die anschließende Beseitigung der Ursache des Problems. Eine detaillierte Dokumentation des Vorfalls ist entscheidend, um Gegenmaßnahmen treffen zu können, zukünftige Angriffe zu verhindern und Compliance-Anforderungen gerecht zu werden. Die Sicherstellung der Geschäftskontinuität (Business Continuity) im Schadensfall wird in der Regel über die Schaffung von Notallplänen umgesetzt. Es kann Sinn machen, diese Notfallpläne für den Data Act anzupassen, insb. um die notwendige Sorgfaltspflicht der Datenherausgabe zu gewährleisten. Jeder Sicherheitsvorfall muss einer gründlichen Risikobewertung unterzogen werden, um die tatsächlichen Auswirkungen auf das Unternehmen und seine Partner zu verstehen.

Dabei ist eine ganzheitliche Betrachtung notwendig, die über die eigenen Infrastrukturen hinausgeht. Mögliche Auswirkungen beziehen sich in komplexen Datenökosystemen wie dem Data Act in der Regel auf

die direkte, eigene Infrastruktur, angrenzende Infrastruktur (insb. Zulieferer, Partner) und andere Unternehmen. Um Schäden resultierend aus einer **Sorgfaltspflicht** und der Reputation zu minimieren, empfiehlt es sich, Kommunikationspläne der Business Continuity um Spezifika resultierend aus dem Data Act zu ergänzen. Kommunikationspläne sollten Teilbereiche und etwaige Kontaktstellen für die interne, externe als auch Behördenkommunikation (insb. bei Meldepflichten) beinhalten.

3.3.4 Technische & organisatorische Schutzmaßnahmen

Technische und organisatorische Maßnahmen (**TOMs**, vgl. engl.: **T**echnical-**O**rganisational **M**easures) sind bereits aus der Datenschutz-Grundverordnung (DSGVO) aus dessen Art. 32 bekannt.
Technische und Organisatorische Maßnahmen im Kontext des Data Act sind jedoch weit mehr als nur eine Compliance-Anforderung. Sie entwickeln sich zu einem **strategischen Instrument**, das eine Diskrepanz zwischen der geforderten Datenweitergabe und dem Schutz sensibler Informationen beinhaltet *(von Ditfurth, 2024).* Die zentrale Frage lautet: Wie können TOMs genutzt werden, um das eigene Sicherheitsniveau zu schützen, ohne die Verpflichtungen des Data Act zu verletzen? Oder anders ausgedrückt: Wie hoch darf der *Abwehr-Zaun* um einen sensiblen Datencontainer sein?
Es entsteht dadurch ein Spannungsfeld zwischen Datensicherheit und Datenzugang. Der Data Act verpflichtet Dateninhaber, Daten unter bestimmten Voraussetzungen an Dritte weiterzugeben. Gleichzeitig fordert der Gesetzgeber eine angemessene Cybersicherheit. Aus diesem Konflikt ergibt sich eine potenzielle *Not-Handbremse*, (*engl.: safety and security handbrake*), die in den FAQs zum Data Act (Frage 25) explizit angesprochen wird. Dateninhaber können die Weitergabe von Daten einschränken oder ablehnen, wenn das Risiko besteht, dass die Sicherheitsanforderungen untergraben werden könnten. Dies kann die Nutzung von hohen Sicherheitsstandards als Argument gegen eine unkontrollierte Datenweitergabe legitimieren.

Die Herausforderung besteht darin, ein Gleichgewicht zu finden:

- Ablehnung aufgrund hoher Sicherheitsanforderungen: Ein Dateninhaber könnte die Weitergabe an einen Dritten mit dem Argument ablehnen, dass die eigenen TOMs – die das hohe Sicherheitsniveau gewährleisten – durch die Weitergabe kompromittiert würden.
- Sicherstellung eines angemessenen Sicherheitsniveaus: Der Data Act erfordert, dass ein angemessenes Sicherheitsniveau über die gesamte Weitergabekette hinweg erhalten bleibt. Dies wirft die Frage auf, wie der Dateninhaber die Sicherheitsstandards des Datenempfängers überprüfen und sicherstellen kann, dass diese seinen eigenen Standards entsprechen.

Die rechtlichen Grundlagen für dieses Spannungsfeld finden sich an verschiedenen Stellen im Data Act:

- Artikel 4 Abs. 2 und Abs. 6: Hier werden Nutzung und Weitergabebeschränkungen basierend auf Sicherheitsanforderungen (Abs. 2) und dem Schutz von Geschäftsgeheimnissen (Abs. 6) behandelt.

- Artikel 11: Ein eigener Artikel 11 im Data Act widmet sich den technischen Schutzmaßnahmen gegen unbefugte Nutzung oder Offenlegung von Daten. Hier wird die Bedeutung von Technologien wie intelligenten Verträgen (*engl.:* Smart Contracts) und Verschlüsselung hervorgehoben. Diese können als essenzielle TOMs dienen, um die Datenintegrität und Vertraulichkeit während des gesamten Datenaustauschprozesses zu gewährleisten.
- Erwägungsgründe 31, 42, 82 und 83: Diese betonen die Wichtigkeit des Schutzes von Geschäftsgeheimnissen und beleuchten die Auswirkungen auf die Cybersicherheit.
- Erwägungsgründe 8, 20, 35 und 46: Diese legen die Bedeutung von technischen und organisatorischen Maßnahmen dar.

3.3.5 Design neuartiger Dienstleistungen & Geschäftsmodelle im Kontext der Sicherheit

Die gemeinsame Wertschöpfung bei der Entwicklung von Services kann durch die Bereitstellung und Gewährleistung von IKT-Sicherheit erreicht werden. In den letzten zehn Jahren wurde das Wachstum digitaler Lösungen hauptsächlich durch die digitale Transformation vorangetrieben, was zu einer Vielzahl von Strategien führte, die alle versuchen, multidisziplinäre Ansätze zur Schaffung von Geschäftswert zu kombinieren und sich von rein technischen Überlegungen zu lösen *(Verhoef et al., 2021).* Die IKT-Sicherheit, die häufig nicht im Mittelpunkt der Bemühungen um die digitale Transformation steht, bietet nach wie vor beträchtliche Möglichkeiten für die Entwicklung einer ganzheitlichen gemeinsamen Wertschöpfung *(Stewart, 2023).* Das Inkrafttreten des Data Act unterstreicht diese Behauptung noch, wenn man die technologischen und verwaltungstechnischen Implikationen für die Umsetzung der gesetzlich vorgeschriebenen automatischen Datenweitergabe und des Datenaustauschs betrachtet.
Aufgrund der Einführung des Data Act sehen wir die folgenden Bereiche voraus, in denen neue, gemeinsam geschaffene Dienste gedeihen könnten - alle in verschiedenen Formen, je nach den Anforderungen, die sich aus Überlegungen zur Einhaltung von Vorschriften oder der Einbeziehung von Infrastrukturen ergeben.

Services der Planung und des Betriebsmanagements:

- Beratung & Schulungen zur Cybersicherheit: Beratungsunternehmen oder Dienstleistungsanbieter können strategische Sicherheitsrichtlinien für Datendienste anbieten, die aufgrund des Datengesetzes veröffentlicht werden. Darüber hinaus können auf technischer Ebene fortgeschrittene automatisierte Tools zur Erkennung von Bedrohungen bereitgestellt werden, die es den Kunden ermöglichen, Risiken zu erkennen und zu mindern. Diese Aktivitäten können auf Unternehmensnetzwerke oder Lieferketten mit mehreren Beteiligten ausgeweitet werden.
- Reaktion auf Zwischenfälle und Schadensbegrenzung: Im Falle von Sicherheitsvorfällen können schnelle Reaktionen und Abhilfemaßnahmen erforderlich werden. Spezifische Vorfälle im Zusammenhang mit Data-Act können unbeabsichtigte oder erzwungene Datenverletzungen und

böswillig veranlasste hohe Zahlen von Datenabrufanfragen einschließlich (verteilter) Denial-of-Service-Angriffe ((D)DoS) sein. Ein weiterer gängiger Angriffsvektor ist der absichtliche oder unabsichtliche Abruf von Daten Dritter, die für Industriespionage oder Reconnaissance genutzt werden können.

- Entwurf und Dienstleistungen zur Einhaltung von Vorschriften: Zu den Dienstleistungen können spezialisierte Compliance-Services gehören, die den Kunden helfen, die gesetzlichen Datenschutzanforderungen zu erfüllen oder IKT-Infrastrukturen zu entwerfen, die sowohl den Standards als auch den gesetzlichen Rahmenbedingungen entsprechen.
- Resilienz / Business Continuity Design & Dienstleistungen: Diese Dienstleistungen können Strategien, Beratung oder technische Lösungen zur Gewährleistung eines kontinuierlichen Betriebs von Data-Act-bezogenen Diensten oder zur Wiederherstellung nach einem Cyberangriff umfassen.

Technische Services:

- Managed On-Premises Secured Services: Ein Dienstleister kann Lösungen für das Hosting der Serverinfrastruktur entwickeln, einschließlich automatisierter Softwarelösungen am Standort des Kunden, um auf Anfragen zum Data Act zu reagieren. Diese Kategorie kann durch Wartungslösungen (d. h. geschultes Personal) erweitert werden.
- Gesicherte Managed Cloud-Dienste: Ähnlich wie bei den gesicherten Vor-Ort-Diensten könnte man eine Cloud-Software-Infrastruktur entwickeln, die Lösungen für Data Act-Anfragen bereitstellt. Diese Kategorie kann durch Wartungslösungen (bspw. geschultes Personal) erweitert werden.
- Bedrohungsdaten: Threat Intelligence kann Datenbanken mit bekannten Schwachstellen oder eine Echtzeitbewertung von Sicherheitsbedrohungen gegen veröffentlichte Data-Act-Lösungen umfassen.
- Penetrationstests: Penetrationstests können die Bewertung von datenschutzspezifischen Sicherheitsmaßnahmen und die Prüfung auf Schwachstellen beinhalten.
- (Automatisierte) Counter-Intelligence: Frühzeitiges Erkennen von koordinierten Angriffen oder Reconnaissance-Operation von Dritten oder böswilligen Akteuren.

3.4 Datenbewertung, Monetarisierung und Modelle

Neue Datenflüsse und neue Chancen

Zusammengefasst:

Der EU Data Act verändert die industrielle Datenwertschöpfung grundlegend: Kunden erhalten neue Rechte zur Nutzung und Weitergabe ihrer Anlagendaten. Dies eröffnet Chancen für effizientere Services durch Drittparteien, birgt aber auch Risiken für Hersteller. Das Projekt „Data Act Pioneer" analysiert diese neuen Werteströme und entwickelt Modelle zur Bewertung wirtschaftlicher Effekte und fairer Vergütungen.

3.4.1 Datenbasierte Wertschöpfung in industriellen Kontexten vor dem Data Act

In industriellen B2B-Märkten erfolgt die datenbasierte Wertschöpfung bislang typischerweise entlang folgender Werteströme: Maschinenhersteller entwickeln, produzieren und verkaufen Anlagen an Geschäftskunden (entspricht „Nutzern" in der Data Act Terminologie). Geschäftskunden nutzen diese Anlagen zur Herstellung eigener Produkte. Im Zuge der Digitalisierung sind moderne Maschinen mit Sensorik, Aktorik und digitaler Steuerung ausgestattet. Durch die Vernetzung via IoT können zusätzliche Services wie Fernüberwachung, zustandsabhängige oder vorausschauende Wartung angeboten werden. Die Anbindung an IoT-Plattformen führt dazu, dass Kunden ihre Anlagendaten mit dem Hersteller teilen. Der Hersteller wird dadurch zum Dateninhaber.

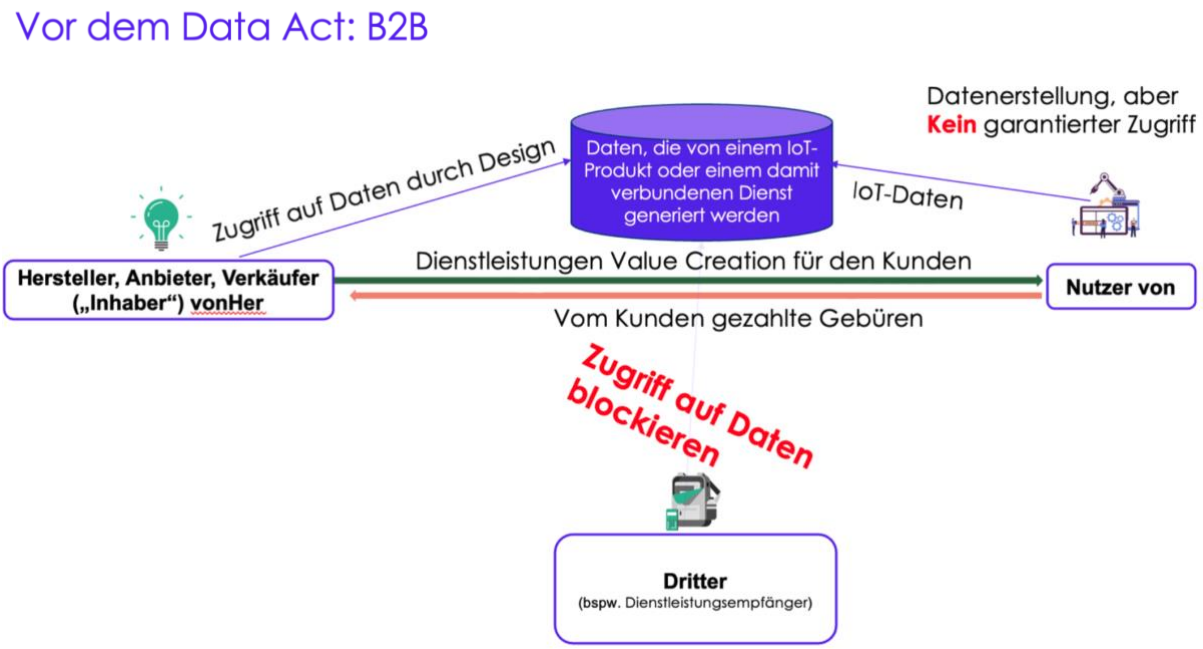


Abbildung 6

Vereinfachte Darstellung der unausgewogenen Daten- und Werteflüsse, vor Anwendbarkeit des Data Act

Diese Konstellation bringt sowohl Nutzen als auch Herausforderungen mit sich. Potenzielle Nachteile für Kunden umfassen einen unausgewogenen Wertefluss: Kunden geben ihre Produktionsdaten auf breiter Basis weiter an die Hersteller.

Daraus lassen sich auf verschiedene Weisen Nutzen für die Hersteller ableiten:

- Sie können mit den Daten Mehrwertservices für die Kunden anbieten, was Kundenbindung und Zusatzumsatz bewirken kann.
- Sie erhalten wertvolle Einsichten in die Nutzung ihrer Anlagen und können daraus Verbesserungen oder Anforderungen an eine nächste Produktgeneration ableiten.
- Die Hersteller können aus den Daten auch ableiten, welche Verwendungsmuster ihrer Anlagen effizienter sind oder zu längeren Standzeiten der Anlagen führen, und diese Muster im Sinne einer Beratungsdienstleistung für andere Kunden nutzen.
- Die Kunden geben dem Hersteller auch Einsicht in ihren betriebswirtschaftlichen Zustand. Die Anbieter können z.B. wirtschaftliche Auf- oder Abschwungphasen vorwegnehmen und darauf mit gezielten Zusatzangeboten reagieren.
- Potenziell geben die Kunden sogar geistiges Eigentum preis, wenn z.B. aus den Produktionsdaten Informationen über das Design von Endprodukten ersichtlich werden.
- Hinzu kommt, dass sich die Hersteller für den daraus resultierenden Servicenutzen nach Möglichkeit über Servicegebühren vergüten lassen.

Der Nutzen für die Kunden besteht im Wesentlichen in verbesserter Leistung mit den eingesetzten Anlagen, z.B. durch:

- optimierten Betrieb, z.B. mehr Output pro Zeit, weniger Rohmaterial- und Energieverbrauch pro Output.
- Verbesserte Qualität des Outputs, weniger produzierte Fehlteile inklusive des nachgelagerten Nutzens infolge weniger Beschwerden durch die Endkunden.
- Höhere Standzeiten, z.B. durch vermiedene Ausfälle und optimierte Wartung der Anlagen.
- Passgenaue Angebote und innovative Produkte, da der Hersteller die Bedürfnisse anhand der Daten genau kennt.

Auch wenn beide Seiten wesentlichen Nutzen aus den geteilten Daten erhalten, besteht doch in einigen Fällen ein Missverhältnis, insbesondere, weil die Hersteller den von einem Kunden abgeleiteten Nutzen auf viele andere Kunden ausbreiten und somit skalieren kann. Der Effekt verstärkt sich, wenn der Hersteller zwar die Daten von den Kunden bezieht und für sich einen Nutzen erzeugt, aber daraus für die Kunden nur einen sub-optimalen Service generiert. Dieser Umstand eröffnet die Opportunität, dass Drittanbieter in die Bresche springen und aus den Daten gesteigerten Mehrwert für die Kunden erzeugt.

3.4.2 Veränderungen im Wertschöpfungsökosystem durch den Data Act

Der EU Data Act verändert diese Datenströme grundlegend. Kunden (Nutzer) erhalten das Recht, ihre Anlagendaten selbst zu nutzen oder an Dritte weiterzugeben.

Nutzung der Daten durch die Kunden selbst: Die Kunden sollen mit dem Data Act durch den Hersteller dazu befähigt werden, die Daten aus ihren Anlagen selbst zu beziehen und weiter zu nutzen, z.B. für eine Integration in ihre Produktionssteuerungssysteme (wie z.B. MES, Scada etc.) oder für ihre eigenen Auswertungen (z.B. ihre eigenen Management Dashboards). Die Kunden sind auch berechtigt, diese Daten an Dritteweiterzugeben, die daraus einen Mehrwert erzeugen und z.B. den Kunden als externe Serviceanbieter für den Anlagenunterhalt oder für Betriebsanalysen.

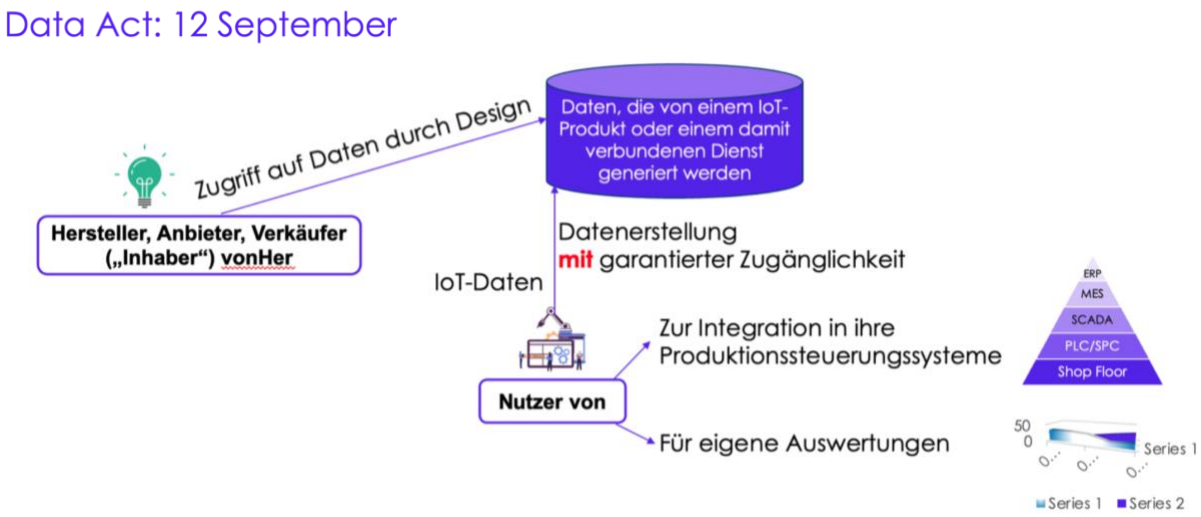


Abbildung 7

Vereinfachte Darstellung des Datenzugangs und Möglichkeiten des Nutzers durch den Data Act

Diese Form der Datennutzung durch die Kunden wird nicht an die Hersteller vergütet *[European Parliament, 2023]*. Diese Form der Nutzung der Daten für eigene Zwecke oder zur Weitergabe an Dritte erfordert, dass die Kunden über eigene Kompetenzen in der Datenverarbeitung verfügen oder dann in ihrem Namen externe Zulieferer damit beauftragen (z.B. IT-Dienstleister). Selbst für die Weitergabe an Dritte müssen zumindest Schnittstellen und Übertragungsverfahren angelegt werden, wobei relevante Fragen des Datenschutzes und der IT-Sicherheit auftreten. Entwicklung und Betrieb dieser Schnittstellen bedeuten für die Kunden Zusatzaufwand oder sogar schwer überwindbare Hürden, gerade für KMU. Wenn Kunden das vermeiden möchten, steht ihnen die Möglichkeit der Weitergabe an Dritte direkt durch den Hersteller offen.

Weitergabe der Daten durch die Hersteller an Drittparteien: Die Kunden können die Hersteller verpflichten, die Daten an von ihnen bestimmte Drittparteien zu übermitteln. Diese sind typischerweise Dienstleistungsanbieter, welche die Daten aufwerten und daraus ein neues Geschäft erzeugen:

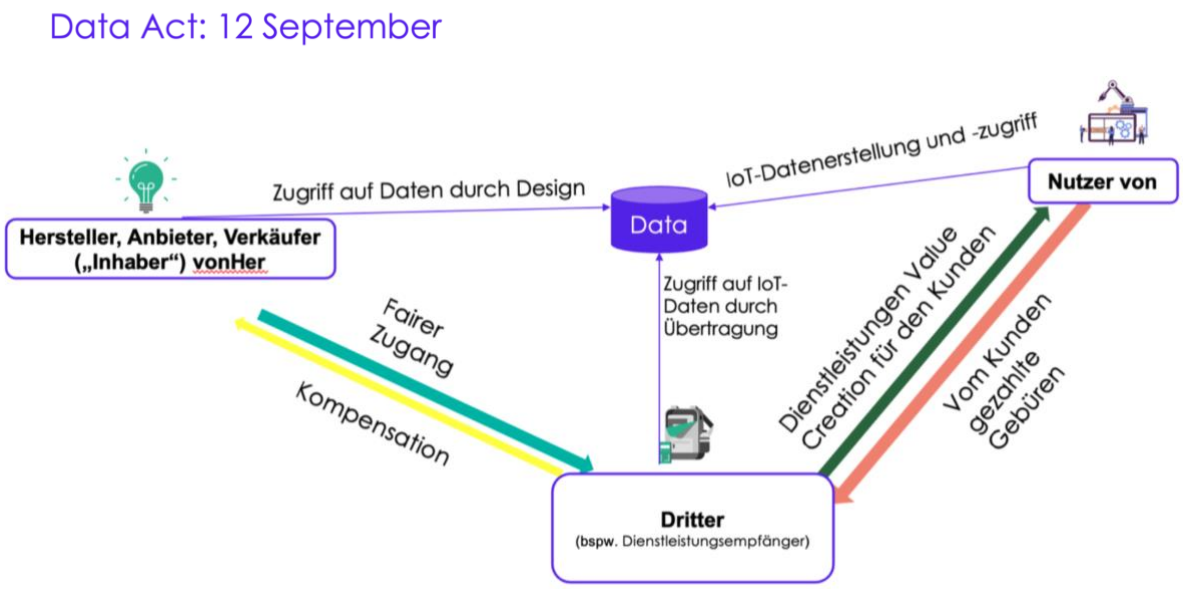


Abbildung 8

Vereinfachte Darstellung des Datenzugang und Möglichkeiten des Dritten durch den Data Act

Eine auch für die Kunden sehr interessante und naheliegende Form liegt dann vor, wenn diese Drittpartei für einen besseren Service sorgt. Dies umfasst Möglichkeiten, wie sie weiter oben im Text unter „Nutzen für die Kunden“ aufgeführt sind. Das kann zum Beispiel der Fall sein, wenn die Drittpartei darauf spezialisiert ist, aus den produktiven Daten besonders effektive oder effiziente Wartungstätigkeiten abzuleiten. Häufige Beispiele in diesem Zusammenhang sind Fernüberwachung und –wartung *(“remote service”)* oder auch zustandsabhängige oder vorausschauende Wartung *(“condition based“* oder *„predictive maintenance“).* Besonders letztere Form basiert auf fortgeschrittenen Verfahren des maschinellen Lernens und der künstlichen Intelligenz, was beides Kompetenzen sind, die gerade für KMU-Kunden schwer zu erschließen sind. Auf diese Art von Analytik spezialisierte Drittparteien können dann deutlich mehr Nutzen aus den Daten ziehen und damit zum Beispiel Ausfallzeiten der Anlagen bei den Kunden signifikant reduzieren, was direkten wirtschaftlichen Nutzen stiften kann. Ebenso können damit die Ressourceneffizienz und Lebensdauer der Anlagen erhöht werden, was nebst dem wirtschaftlichen auch umweltbezogenen Nutzen schafft. Wenn Dritte ihre Kernkompetenz in der Analyse von Daten aus industriellen Anlagen haben, können sie aus breit gefächerten Typen von Produktionsstätten, Kundensituationen und Anlagen lernen und ihre Datenmodelle optimieren. Daraus kann eine Servicequalität entstehen, wie sei in einer Hersteller-Kunden-Beziehung nicht erreicht werden kann.

In der Sprache der industriellen Dienstleistungen werden durch diese Nutzung der Daten Problempunkte *(“pains”)* bei den Kunden abgeschwächt oder vermieden. **Typische Pains sind:** Ausfallzeiten, tiefe Anlageneffizienz, geringe Qualität, hoher Energieverbrauch. Der wirtschaftliche und umweltbezogene Nutzen aus der Abschwächung oder Behebung dieser Pains kann mit dem *“value-of-pains"-Framework* quantitiativ bestimmt werden, welches in *(Meierhofer et al. 2024)* beschrieben ist und hier kurz zusammengefasst wird:

- Durch die ungelösten Pains entsteht für die Kunden messbarer betriebswirtschaftlicher Schaden („impact“), z.B. reduzierte Stückzahl an Endprodukten, Überzeitschichten, Nacharbeit, Energieverschwendung.
- Die Pains haben eine Häufigkeit („frequency“), mit der sie auftreten (z.B. täglich, wöchentlich, …).
- Durch die Multiplikation von Schaden und Häufigkeit erhalten wir den Erwartungswert des Pains in einer Zeitperiode.
- Mit einem datengetriebenen Service kann ein Anteil dieser Ausfälle vermieden werden. Dadurch wird der finanzielle Wert des Pains um diesen Anteil reduziert.

  Beispiel:
  - Eine Produktionsanlage mit Maschinenkosten von 200 Euro pro Stund steht bei einem Ausfall typisch während 5 Stunden still, d.h. ein Ausfall kosten +1.000 Euro.
  - Derartige Ausfälle kommen im Mittel viermal pro Jahr vor. Damit ergibt sich der Erwartungswert dieses Pains zu 4‘000 Euro pro Jahr.
  - Durch Predicitive Maintenance und Remote Monitoring können ca. 50% der Ausfälle vermieden werden.
  - Damit ergibt sich der betriebswirtschaftliche Nutzen dieser Services zu 2'000 Euro pro Jahr.
  - Aus diesem Nutzen kann im Sinne von «value-based pricing» die maximale Zahlungsbereitschaft der Kunden abgeleitet werden: sie zahlen einen Teil des erhaltenen Nutzens, d.h. ihre Zahlungsbereitschaft in Form von Servicegebühren beträgt im Beispiel <= 2'000 Euro pro Jahr.
- Zum finanziellen Nutzen hinzu kommt ein potenzieller umweltbezogener Nutzen, wenn durch die Services z.B. Reisen, Energieverschwendung oder Ausschussmaterial vermieden wird. Dieser kann in CO2 Äquivalenten ausgedrückt mit derselben Methodik berechnet werden.

Aus den vorangestellten Überlegungen kann auch abgeleitet werden, dass die Kunden der Drittpartei potenziell höhere Servicegebühren bezahlen, wenn sie von dieser höheren Servicenutzen erhalten.

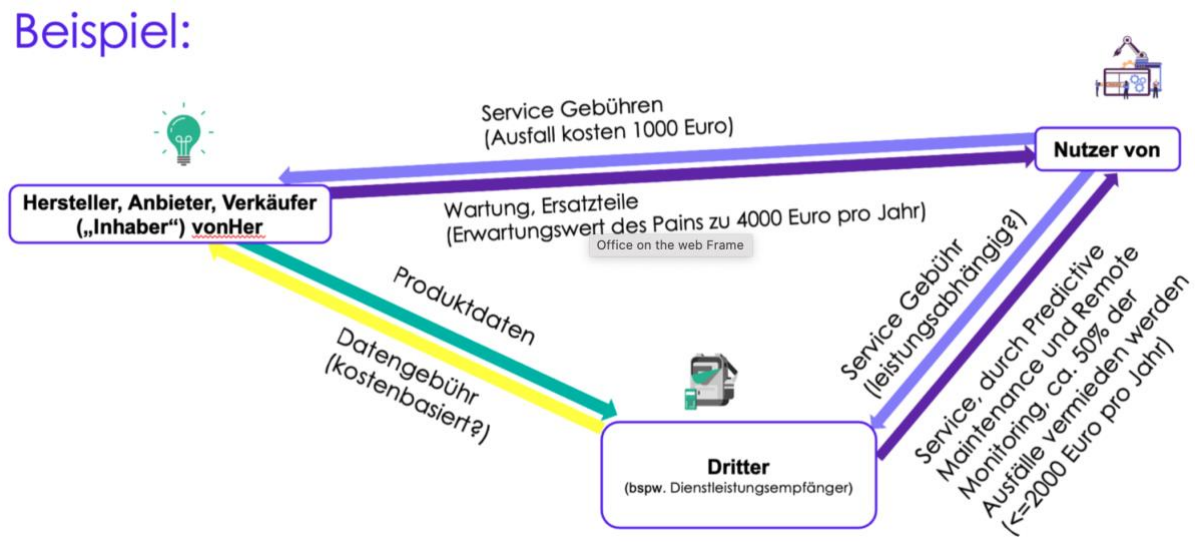


Abbildung 9

Vereinfachte Darstellung des Beispiels: Höhere Servicegebühren

Zusammenfassend kann festgehalten werden, dass die Kunden entweder vom Anbieter oder der Drittpartei einen Service-Nutzen zur Behebung von Pains wie Leistungseinbussen oder Unterbruchszeiten der Anlage erhalten. Sie sind im Gegenzug bereit, dafür eine Servicegebühr zu entrichten, entweder an den Anbieter oder an die Drittpartei. Entweder erbringt der Hersteller den Service für die Kunden selbst durch Nutzung der Produktionsdaten aus den Anlagen. Alternativ bezieht die Drittpartei Daten vom Hersteller und erbringt damit den Service für die Kunden. Für diese Datenweitergabe an Dritte steht dem Hersteller eine angemessene Vergütung zu. Die Höhe dieser Vergütung ist derzeit Gegenstand regulatorischer und wirtschaftlicher Klärungen. Diese Services durch die Drittparteien können bestehende Hersteller-Services substituieren oder ergänzen.
Ob es für die Kunden interessanter ist, die Services von der Drittpartei statt vom Hersteller zu beziehen, hängt wesentlich davon ab, ob die Drittpartei eine bessere **Service-Performance** erreicht (z.B. weniger Downtime, mehr Leistung für die Kunden) als der Hersteller oder ob sie eine Service-Performance effizienter (d.h. zu geringeren Kosten) und somit für die Kunden zu einer tieferen Servicegebühr erbringen kann. D.h. der Hersteller kann verhindern, dass Kunden die Daten an Dritte geben wollen, wenn er bereits selbst effizient eine gute Service-Performance erbringt. Damit zeigt sich auch das Potenzial des Data Acts, die effiziente und innovative Nutzung der Daten zur fördern.

3.4.3 Chancen und Risiken für Akteure im Ökosystem

Die neuen Regelungen schaffen sowohl Risiken als auch Chancen für alle Beteiligten. **Für Hersteller besteht das Risiko**, Daten gegen möglicherweise geringe Vergütung abgeben zu müssen. Gleichzeitig haben die **Hersteller folgende Chancen:**

- Sie können ihre eigene Servicekompetenz auszubauen und ihre Kunden binden.
- Zudem können sie als Drittpartei im Markt anderer Hersteller auftreten und datengetriebene Services anbieten. Diese Opportunität wird in der Praxis noch sehr selten erkannt und genutzt, birgt aber grosses Potenzial, denn Entwicklung und Betrieb industrieller Dienstleistungen profitieren stark von Skaleneffekten. Wenn z.B. Service- oder Daten-Plattformen eines Herstellers auch für die Kunden anderer Anbieter genutzt werden, können die Fixkosten für Entwicklung und Betrieb besser gedeckt werden.
- Eine interessante Möglichkeit liegt auch vor, wenn ein Anbieter in der Geographie verteilte Feldtechnikressourcen mit stark fluktuierender Auslastung hat, welche durch eine vergrösserte Kundenbasis geglättet werden kann.
- Zudem kann sich auch die Situation ergeben, dass ein Hersteller strategisch kein Gewicht auf den Service legen will und auf der Basis des Data Acts eine Drittpartei in diese Lücke springen kann.

Für Dritte ergeben sich Chancen, effizientere oder kundenorientiertere Services zu entwickeln und neue Kunden zu gewinnen. Allerdings besteht für **Dritte das Risiko,** dass Hersteller nachziehen und Kunden zurückgewinnen, was zu nicht amortisierten Investitionen führen kann.
Kunden profitieren von besseren oder günstigeren Services, tragen jedoch das Risiko von Lock-in-Effekten bei Anbieterwechsel und Unsicherheit über die langfristige Servicequalität.

3.4.4 Beitrag des Projekts „Data Act Pioneer“

Im Rahmen des Projekts „Data Act Pioneer“ werden die neuen Wertetröme systematisch analysiert und mathematisch modelliert. Ziel ist es, Entscheidungsgrundlagen für die beteiligten Akteure zu schaffen. Zentrale Projektinhalte umfassen die Modellierung von Wertetrömen im Business-Ökosystem, Szenarienanalysen zur Bewertung der Auswirkungen datenbasierter Geschäftsmodelle und die quantitative Bewertung der wirtschaftlichen Effekte für Hersteller, Kunden und Drittparteien.
Erste Erkenntnisse aus Fallstudien zeigen, dass eine Datenweitergabe an Drittparteien unter folgenden Bedingungen wirtschaftlich vorteilhaft ist, wenn auch zulasten des Herstellers: Wenn die Drittpartei den gleichen Servicenutzen effizienter (kostengünstiger) erbringen kann oder einen höheren Servicenutzen generieren kann. Erfolgsfaktoren für Drittparteien umfassen überlegene Datenanalysefähigkeiten und effiziente Servicebereitstellung.
Die im Projekt erarbeiteten Bewertungsmodelle können bei der Festlegung fairer Vergütungen und der Schaffung von Transparenz in regulatorischen und wirtschaftlichen Entscheidungsprozessen unterstützen.

4 Schlussbetrachtung

Die bevorstehende Umsetzung des EU Data Acts markiert einen wichtigen Wendepunkt für die industrielle Datenökonomie. Unternehmen sind gefordert, ihre Rolle innerhalb des neuen regulatorischen Rahmens zu analysieren und die sich daraus ergebenden Pflichten frühzeitig in Produkt- und Dienstleistungsdesign zu integrieren. Insbesondere die Ansprüche auf Datenzugang, Vorgaben zur Datenweitergabe und Interoperabilität erfordern eine konsequente Berücksichtigung bereits in der Planungs- und Entwicklungsphase. Hierbei gewinnt das Prinzip „Data Access by Design“ an Bedeutung. Die Vielzahl der Pflichten und die Tragweite möglicher Sanktionen lassen die Auswirkungen mit den Erfahrungen zur DSGVO jedenfalls vergleichbar erscheinen, sodass eine rechtzeitige Auseinandersetzung mit dem Regelungsgehalt und passenden Implementierungsstrategien geboten ist. Neben der technischen Umsetzung gewinnen auch vertragliche Regelungen als zentrales Instrument des Data Act an Bedeutung: Bestehende Kunden- und Partnervereinbarungen sollten auf ihre Übereinstimmung mit den Anforderungen des Data Act überprüft und bei Bedarf angepasst werden. Auch die in diesem Paper vorgeschlagenen Instrumente und Modelle zur Bewertung des Datennutzens und der Monetarisierung sollten in ihrer Relevanz nicht unterschätzt werden.

Aus der Perspektive des Innovationsprozesses und der dazu erforderlichen Kompetenzen schafft die neue Regulierung dafür im Ökosystem einen geregelten Zugang zu bisher kaum zugänglichen Daten, die nun den Status quasi offener Daten erhalten. Da aus Daten jedoch nicht automatisch Innovationen entstehen, müssen geeignete Rahmenbedingungen geschaffen und Hürden abgebaut werden. Zentral ist dabei, wie der EU Data Act die Wertschöpfung im Ökosystem und in Unternehmen verändert. Im Fokus stehen die geteilten Datenarten, der neue Datenzugang, ihre Wirkung auf den Innovationsprozess sowie die nötigen Kompetenzen und organisatorischen Voraussetzungen.

In der praktischen Umsetzung bleiben zahlreiche Unsicherheiten bestehen. Zwar verschafft die klare Zuordnung von Produkt- und Dienstdaten dem Nutzer eine starke Ausgangsposition, gleichzeitig eröffnet der Data Act dem Dateninhaber bei adäquater Vorbereitung Handlungsspielräume. Wesentliche Schritte umfassen dabei die systematische Analyse und Klassifizierung von Daten, die Einrichtung eines Nutzer- und Drittparteienmanagements sowie die Festlegung von eigenen Nutzungszwecken und Verfahren zur Bearbeitung von Datenzugangsansprüchen. Es mangelt im Rahmen dieser Forschung also nicht an offenen Fragen z.B. auch die nach der fairen Vergütung bei Datenweitergabe, die Entwicklung der Servicequalität über einen längeren zeitlichen Horizont sowie die Bewertung von Technologieplattformen, welche für die Serviceerbringung genutzt werden.

Angesichts der direkten Anwendbarkeit des Data Acts ab dem **12. September 2025** bleibt nur eine begrenzte Vorbereitungszeit, weshalb frühzeitige Maßnahmen nicht nur zur Risikominimierung, sondern auch zur Ausschöpfung der neuen wirtschaftlichen Potenziale entscheidend sind. Die Umsetzung des EU Data Acts wird die industrielle Datenökonomie nachhaltig verändern. Unternehmen sollten sich daher frühzeitig mit den neuen Pflichten auseinandersetzen, um sachverhaltsbezogene technische und organisatorische Schutzmaßnahmen einzurichten, die regemäßig überprüft und angepasst werden. Gleichzeitig gilt es, die Chancen zu erkennen, die der Data Act insbesondere für kleinere Unternehmen eröffnet.

Diese Aspekte des Papiers bieten wertvolle Anknüpfungspunkte für weiterführende Forschungsarbeiten und Kooperationen. Gleichzeitig liefern die Ergebnisse des Forschungsprojekts **“Data Act Pioneer”** praxisnahe Ansätze, von denen sowohl die assoziierten Partnerunternehmen als auch weitere interessierte Unternehmen unmittelbar profitieren sollen.

Literaturverzeichnis

Zitierte und weiterführende Quellen:

Aaser, M., Kanagasabai, K., Roth, M., & Tavakoli, A. 2020. Four ways to accelerate the Creation of Data Ecosystems. McKinsey Analytics, November.

Al-Mhiqani, M. N., Ahmad, R., Abidin, Z. Z., Ali, N. S., & Abdulkareem, K. H. 2019. Review of cyber attacks classifications and threats analysis in cyber-physical systems. International Journal of Internet Technology and Secured Transactions, 9(3), 282-298.

Antoine, L. (2024). Datenzugang im Spannungsfeld zwischen DSGVO, Geschäftsgeheimnisschutz und Datenbankherstellerrecht, Computer und Recht, 73 ff.

Babu, M. M., Rahman, M., Alam, A., & Dey, B. L. 2024. Exploring Big Data-driven Innovation in the Manufacturing Sector: Evidence from UK Firms. Annals of Operations Research, 333(2), 689-716.

Baumann, J.; Brunnbauer, J. (2025). Datenschutzrechtliche Anforderungen bei der Bereitstellung von IoT-Daten nach dem Data Act, Herausforderung für Dateninhaber im Spannungsfeld zwischen DS-GVO und DA. Zeitschrift für Datenschutz, (3), 131-137.

Bertschek, I., H. Bonin, J. Kühling, J., G. Thüsing & Wenzel, T., 2021. Entwicklung eines Konzepts zur Datenallmende: IZA Research Report No. 119. Expertise im Auftrag des Bundesministeriums für Arbeit und Soziales.

Bomhard, D.; Siglmüller, J. (2025), Das Verhältnis von Access by design und Datenzugangsanspruch nach dem Data Act. Recht Digital, (7), 353-357.

Bouschery, S.G.; V. Blazevic & F.T. Piller, 2023. Augmenting human innovation teams with artificialintelligence: Exploring transformer-based language models. Journal of Product Innovation Management 40(2): 139–153. https://doi.org/10.1111/jpim.12656

Christensen, C., 2016. The Innovator's Dilemma: When new Technologies cause great Firms to fail. Harvard Business Review Press.

Cooper, R. G. 2008 Perspective: The Stage-Gate® idea-to-launch Process—update, what's new, and nexgen systems. Journal of Product Innovation Management, 25(3), 213-232.

Denga, M. (2024). Verträge über digitale Produkte zwischen Unternehmen. Zeitschrift für die gesamte Privatrechtswissenschaft, (4), 427-464.

Eapen, T.T.; D.J. Finkenstadt; J. Folk; L. Venkataswamy, 2023. How generative AI can augment Human Creativity. Harvard Business Review, July-August.

Eckardt, M., & Kerber, W. 2023. The EU Data Act and the Re-Allocation of Data Rights in the IoT Ecosystem. European Journal of Law and Economics, 56(3), 405–433. https://doi.org/10.1007/s10657-023-09791-8

Ehlen, T.; Sebulke, P. (2024). Der Data Act: Zwischen Markt- und Vertragsgestaltung. Computer und Recht, (2), 84-90.

EU-Kommission, COM(2020) 66 final v. 19.02.2020, Brüssel: Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Eine europäische Datenstrategie, abrufbar unter: https://eurlex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52020DC0066.

Europäische Kommission, 2022. Proposal for a Regulation on harmonised Rules on fair Access to and use of Data (Data Act). COM(2022) 68 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0068

European Commission 2023. Boosting data sharing in the EU: what are the benefits? https://www.europarl.europa.eu/topics/en/article/20220331STO26411/boostingdata-sharing-in-the-eu-what-are-the-benefits

European Commission, “Frequently Asked Questions Data Act.” European Union, Feb. 03, 2025. Accessed: Apr. 14, 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act

European Commission, 2022. Data Act: Commission proposes Measures for a fair and innovative Data Economy. Press Release, 23 February, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.

European Commission, 2024. Data Act. Shaping Europe’s digital Future. https://digital-strategy.ec.europa.eu/en/policies/data-act

European Parliament, “Data Act: MEPs back new rules for fair access to and use of industrial data.” EP_Industry, Mar. 14, 2023. Accessed: Nov. 03, 2023. [Online]. https://www.europarl.europa.eu/news/en/press-room/20230310IPR77226/data-act-meps-back-new-rules-for-fair-access-to-and-use-of-industrial-data

European Union, 2025. European Data: Open Data as a Catalyst for Innovation. https://data.europa.eu/en/academy/open-data-catalyst-innovation.

Furr, N., & J. Dyer, 2014. The Innovator's Method: Bringing the Lean Start-up into Your Organization. Boston: Harvard Business Review Press.

Götz, M., Blöink, S. (2024). Datenvertrag: Lösungsansatz für das Spannungsfeld zwischen Data Act und DS-GVO. Multimedia und Recht, (6), 451-456.

Grützmacher, M. (2024). Data Act: Datenzugang und Geschäftsgeheimnisschutz, Computer und Recht, (5), 281-292.

Hartmann, B., McGuire, M. & Schulte-Nölke, H. (2023). Datenzugang bei smarten Produkten nach dem Entwurf für ein Datengesetz (Data Act). Recht Digital, (2), 49-59.

Heinzke, P.; Herbers, B.; Kraus, M. (2024). Datenzugangsansprüche nach dem Data Act. Betriebs-Berater, (12), 649-655.

Hennemann, M., Specht-Riemenschneider, L. (2025). Data Act – Data Governance Act – Handkommentar, 2. Auflage, Nomos Verlagsgesellschaft, Baden-Baden.

Hennemann, M., Steinrötter, B. (2022). Data Act – Fundament eines neuen EU-Datenwirtschaftsrechts? Neue Juristische Wochenschrift, (21), 1481-1486.

Hennemann, M., Steinrötter, B. (2024). Der Data Act – Neue Instrumente, alte Friktionen, strukturelle Weichenstellungen. Neue Juristische Wochenschrift (1), 1 – 8.

Hennemann, M., Steinrötter, B. (2024). Der Data Act – Neue Instrumente, alte Friktionen, strukturelle Weichenstellungen. Neue Juristische Wochenschrift (1), 1 – 8.

Hetzenauer, C., Dobler, M., & Simma, A. (2023, June). Information security chal-lenges in the digitalisation of the austrian food industry: Assessment of food Suppli-ers and implications. In 2023 IEEE International Conference on Engineering, Tech-nology and Innovation (ICE/ITMC) (pp. 1-7).

Jouini, M., & Rabai, L. B. A. (2016). Threats classification: state of the art. Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security, 368-392.

Knapp, E. D. (2024). Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems. Elsevier.

Kugler, P., & T. Plank, 2021. Coping with the double-edged Sword of data sharing in Ecosystems. Technology Innovation Management Review, 11(11/12), 5-16. https://www.timreview.ca/article/1470.

Kugler, P., 2020. Approaching a Data-Dominant Logic. Technology Innovation Management Review, Vol. 10(10), 16-28. http://doi.org/10.22215/timreview/1393.

Kugler, P., 2023. Aus Big Data wird Big Value: Warum es eine Daten-dominante Logik braucht. Schallmo, D.R.A.; K. Lang; T. Werani; B. Krumay (Hrsg.): Digitalisierung: Fallstudien, Tools und Erkenntnisse für das digitale Zeitalter. Wiesbaden: Springer Fachmedien, 553-568. https://doi.org/10.1007/978-3-658-36634-6

Kugler, P., 2025. Datengetriebene Organisationskultur: Unternehmen neu denken und Daten im Ökosystem teilen. In: Kugler et al. (Hrsg.): Data Sharing für KMU: Voraussetzungen und Instrumente für die gemeinsame Nutzung von Daten. Berlin, Heidelberg: Springer Gabler, 27-49.

Kugler, P.; H. Vogt; J. Meierhofer; M. Dobler; M. Strittmatter; M. Treiterer; & S. Schick, 2024. Daten im B2B-Ökosystem teilen und nutzen: Wie KMU Voraussetzungen schaffen und Hürden überwinden. In: Schallmo, D., S. Kundisch, K. Lang, D. Hasler (Hrsg.): Digitale Plattformen und Ökosysteme im B2B-Bereich: Fallstudien, Ansätze, Technologien und Tools. Springer Nature, Schwerpunkt Business Model Innovation, 209-240. ISBN 978-3-658-43129-7, DOI 10.1007/978-3-658-43130-3.

Kugler, P.; M. Dobler, J. Meierhofer, M. Strittmatter, M. Treiterer, H. Vogt (2025). Data Sharing für KMU - Voraussetzungen und Instrumente für die gemeinsame Nutzung von Daten, Wiesbaden: Springer Nature.

Long, D., & B. Magerko, 2020. What is AI Literacy? Competencies and Design Considerations. In: CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, https://doi.org/10.1145/3313831.3376727

Martens, B., 2023. Pro-and anti-competitive Provisions in the proposed European Union Data Act (No. 01/2023). Bruegel Working Paper.

Meier, D. A., & Burda, D. (2019). Cybersicherheit als Führungsaufgabe in Schweizer KMU: Herausforderungen und Chancen im Zuge der Digitalisierung. In Digitale Transformation und Unternehmensführung: Trends und Perspektiven für die Praxis (pp. 83-104). Wiesbaden: Springer Fachmedien Wiesbaden.

Müller, J. (2024). Der Schutz faktischer Kontrolle durch die Rechtsordnung, Recht Digital, (7), 297 – 304.

Ng, D.T.K.; J.K.L. Leung; S.K.W. Chu; M.S. Qiao, 2021. Conceptualizing AI literacy: An exploratory review. Computers and Education: Artificial Intelligence, 2, 2021, 100041, https://doi.org/10.1016/j.caeai.2021.100041

Ohly, A. (2019). Das neue Geschäftsgeheimnisgesetz im Überblick, Gewerblicher Rechtsschutz und Urheberrecht, 441 ff.

Pauly, D., Wichert, F., Baumann, J. (2024). Schutz von Geschäftsgeheimnissen nach dem Data Act. Multimedia und Recht, (3), 211-216.

Pliauskaite, L. o.J. EU Data Act: 101. https://iapp.org/media/pdf/resource_center/eu-data-act-101-chart.pdf

Podszun, R. (2021). Handwerk in der digitalen Ökonomie – Rechtlicher Rahmen für den Zugang zu Daten, Software und Plattformen (Bd. 5). Nomos Verlag.

Podszun, R.,Pfeifer, C. 2023. Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission, Gewerblicher Rechtsschutz und Urheberrecht, (13), 953 – 961.

Ridgway, W. E., Simon, D. A., Kerr-Shaw, N., Werry, S., Aleksiev, A. J., & Éles, K., 2025. EU Data Act: Three months to go before new rules on data access and sharing take effect [PDF]. Skadden, Arps, Slate, Meagher & Flom LLP. https://www.skadden.com/-/media/files/publications/2025/06/eu_data_act_three-months_to_go_before_new_rules_on_data_access_and_sharing_take_effect.pdf?rev=19bad942e61b4d14b647c54e05456151

Schein, E.H., 1992. Organizational Culture and Leadership, 2nd edition. Jossey-Bass Publishers.

Schemmel, F. (2024). Data Act und DS-GVO: ziemlich beste Feinde? Spannungsfeld und Wechselbeziehung in der Praxis. Compliance-Berater, (8), 301-308.

Schmidt-Kessel, M. (2024). Heraus- und Weitergabe von IoT-Gerätedaten. Multimedia und Recht, 75-82.

Schreiber, K., Pommerening, P., /Schoel, P. (2024). Der neue Data Act – mit Data Governance Act, 2. Auflage, Nomos Verlagsgesellschaft, Köln.

Schuh, G. (Ed.), 2012. Innovationsmanagement: Handbuch Produktion und Management 3. Springer-Verlag.

Schüller, K. 2020. Future Skills: A Framework for Data Literacy. Stifterverband & Hochschulforum Digitalisierung. https://hochschulforumdigitalisierung.de/wp-content/uploads/2023/09/HFD_AP_Nr_53_Data_Literacy_Framework.pdf

Schulz, M. (2024). Datenzugang nach dem Data Act - Überblick und Schnittstellen zum Kartellrecht. Neue Zeitschrift für Kartellrecht, (8), 426-433.

Schwamberger, S. (2024). Die Klauselkontrolle in Art. 13 Data Act. Multimedia und Recht, 96-101.

Seco.com, o.J.. Industrial innovation, how an OEM evolves thanks to AI and IIOT. https://www.seco.com/blog/details/industrial-innovation-how-an-oem-evolves-thanks-to-ai-and-iiot

Specht-Riemenschneider, L. (2023). Datennutz und Datenschutz: Zum Verhältnis zwischen Daten-wirtschaftsrecht und DSGVO, Zeitschrift für Europäisches Privatrecht, S. 638 ff.

Spießhofer, B. (2022). Sustainable Corporate Governance, Neue Zeitschrift für Gesellschaftsrecht, S. 435 ff.

Steinrötter, B. (2021). Gegenstand und Bausteine eines EU-Datenwirtschaftsrechts. Recht Digital, (10), 480-486.

Stewart, H. (2023). Digital transformation security challenges. Journal of Comput-er Information Systems, 63(4), 919-936.

Strittmatter, M., Meyer, J., Meierhofer, J., Vogt, H., Kugler, P., Dobler, M. 2025. The EU Data Act: Opportunities and Research Perspectives for Data-Driven Companies. In: West, S., Meierhofer, J., Buecheler, T., Wally Scurati, G. (eds) Smart Services Summit. SMSESU 2024. Progress in IS. Springer, Cham. https://doi.org/10.1007/978-3-031-86958-7_2

Stucki, M., Meierhofer, J., Gal, B., Gallina, V., & Eisl, S. 2024. Data driven value creation in industrial services including remanufacturing. Procedia Computer Science, 232, 2240-2248.

Tesch, J. F., Brillinger, A. S., & Bilgeri, D. 2017. Internet of things business model innovation and the stage-gate process: An exploratory analysis. International Journal of Innovation Management, 21(05).

The European Parlament, “MODEL CONTRACTUAL TERMS for contracts between data holders and data recipients on making data available at the request of a user.” Dec. 2024.

The European Parlament, “REGULATION (EU) 2023/2854 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act),” 2023/2854, p. 71, Dec. 2023, [Online]. Available: https://eur-lex.europa.eu/eli/reg/2023/2854/oj

Tntra.com. o.J. The Future of Work: IoT-Driven Innovations in Manufacturing Industries. https://www.tntra.io/blog/future-of-work-iot-driven-innovations-in-manufacturing-industries/

Topping, C., Dwyer, A., Michalec, O., Craggs, B. and Rashid, A., 2021. Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks. Computers & Securi-ty, 108, p.102324.

Trott, P., Baxter, D., Ellwood, P., & van der Duin, P. (2022). The changing context of innovation management. Prometheus, 38(2), 207-227.

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. Journal of business research, 122, 889-901.

Verordnung (EU) 2023/2084, Erwägungsgrund 32, https://data-act-law.eu/de/erwg/32/

Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung) v. 13.12.2023, abrufbar unter: http://data.europa.eu/eli/reg/2023/2854/oj.

Verordnung (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act), OJ L, 2023/2854, 22.12.2023, p. 1–65. https://eur-lex.europa.eu/eli/reg/2023/2854/oj

Vidgen, R., Shaw, S., & Grant, D.B. 2017. Management challenges of creating value from business analytics. European Journal of Operational Research, 261: 626-639. https://doi.org/101016/j.ejor.2017.02.023

Von Ditfurth, L. (2024). Datenmärkte, Datenintermediäre und der Data Governance Act – Eine Analyse der europäischen Regulierung von B2B-Datenvermittlungsdiensten (Bd. 4). Verlang De Gruyter.

Weiden, H. (2022). EU Data Act und Tool zur Visualisierung von Datenströmen öffentlich. Gewerblicher Rechtsschutz und Urheberrecht, 16(5), 313–315.

Weinhold, R.; Schröder, C. (2024). Data Act - (R)Evolution oder vergebene Chance?. Zeitschrift für Datenschutz, (6), 306-311.

Wiebe, A (2023). Der Data Act als vertragsrechtlicher Rahmen für Datennutzungsverträge, Computer und Recht, S. 777 ff.

Wiebe, A. (2023). Der Data Act – Innovation oder Illusion? Gewerblicher Rechtsschutz und Urheberrecht, (22), 1569-1578.

Prof. Dr. Marc Strittmatter hält an der HTWG Konstanz eine Professur für Wirtschaftsrecht, insbesondere zu den Themen IT- und Datenschutzrecht inne. Er forscht im Bereich Rechtsfragen der Datenökonomie und der Künstlichen Intelligenz (KI). Vor seiner Berufung an die HTWG Konstanz war er Leiter Recht der IBM Deutschland und in einer spezialisierten IT-Rechtskanzlei als Rechtsanwalt tätig. Seine Schwerpunkte in der Lehre sind Datenrecht, Rechtsfragen der KI, Fragen der Verhandlungstheorie, Kartellrecht und das IT- und Datenschutzrecht.

Johanna Meyer hat Wirtschaftsrecht an der HTWG Konstanz mit dem Abschluss Bachelor of Laws (LL.B.) studiert. Sie wirkte bereits während ihres Studiums an verschiedenen Forschungsprojekten mit und war Teil des Teams der Datenschutzstelle der Hochschule. Parallel zu ihrer Tätigkeit als wissenschaftliche Mitarbeiterin für das Forschungsprojekt “Data Act Pioneer”, arbeitet sie seit 2021 in freier Mitarbeit für eine Boutiquekanzlei, die auf Technologie, IP und Medien spezialisiert ist. Ihr Schwerpunkt liegt dort vor allem im Bereich IT-Recht und EU-Regulatorik.

Eileen Gladis absolviert derzeit ihren LL.B. an der HTWG Konstanz. Seit September 2024 ist sie als studentische Mitarbeiterin am Lehrstuhl von Marc Strittmatter tätig und arbeitet dort intensiv im Interreg-geförderten Projekt „Data Act Pioneer“ mit. Ihr besonderes Interesse gilt dem Datenwirtschafts-, IP- und Wettbewerbsrecht, dem sie sich auch in ihrer Abschlussarbeit am Lehrstuhl widmete.

Data Act Pioneer

Zürcher Hochschule für Angewandte Wissenschaften

zh aw

Dr. Jürg Meierhofer ist Leiter der Expert Group «Smart Services» der Data Innovation Alliance und Studienleiter Industrie 4.0 (MAS) und Smart Services (CAS) an der ZHAW Zürcher Hochschule für Angewandte Wissenschaften. Die Gestaltung datengetriebener Service-Wertschöpfung zieht sich als roter Faden durch seine Tätigkeit. Nach verschiedenen Führungspositionen im Dienstleistungsbereich lehrt und forscht er seit 2014 an der ZHAW. Er hat an der ETH Zürich promoviert und an der Universität Fribourg einen EMBA erworben.

Dr. Helen Vogt ist Dozentin für Innovations- und Produktmanagement an der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) in Winterthur. Die ausgebildete Materialwissenschaftlerin verfügt über umfangreiche Erfahrungen im Business Development und im industriellen Produktmanagement von Schweizer und internationalen Unternehmen. An der ZHAW leitet sie den Studiengang Master in Product Management und engagiert sich in der Weiterbildung im Bereich des Innovationsmanagements. Ihre Forschungsschwerpunkte sind Kreislaufwirtschaft und Entrepreneurship mit Fokus auf die Entwicklung von nachhaltigen Geschäftsmodellen.

Susana Soriano Ramirez ist seit 2022 wissenschaftliche Mitarbeiterin an der ZHAW. Sie hat einen Master in Wirtschaftsinformatik an der ZHAW und einen Master of Advanced Studies in Angewandter Technologie an der ETH Zürich absolviert. Ihre Forschung umfasst nachhaltige und automatisierte Softwareentwicklung, empirische Studien zu deren Herausforderungen sowie datengesteuerte Wertschöpfung. Zuvor war sie als Systemingenieurin in Mexiko, den USA und der Schweiz tätig und gründete in Mexiko ihr eigenes IT-Unternehmen.

Interreg Alpenrhein-Bodensee-Hochrhein

Kofinanziert von der Europäischen Union

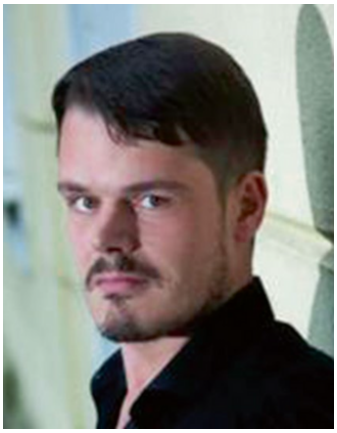
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Data Act Pioneer

OST Ostschweizer Fachhochschule

Prof. Dr. Petra Kugler ist Professorin für Strategie und Management am Institut für Unternehmensführung. Ihre Arbeit konzentriert sich auf die Schnittstelle von Innovation, Strategie und Management und darauf, wie Unternehmen in turbulenten Zeiten nachhaltige Wettbewerbsvorteile generieren und schützen können. Sie promovierte an der Universität St. Gallen (HSG), war in der Werbung tätig und sammelte internationale akademische Erfahrung durch verschiedene Stipendien, unter anderem ein Stipendium des Schweizerischen Nationalfonds für ein Forschungsjahr an der University of California, Berkeley.

FHV Vorarlberg University of Applied Sciences



Martin Dobler hat an der Fachhochschule Vorarlberg (FHV) im Forschungszentrum Business Informatics über 20 nationale, Interreg und EU-geförderte (Forschungs-)Projekte umgesetzt. Nach dem Studium der Informatik war er zuerst als Softwareentwickler und später in der Simulation und Modellierung von digitalen, automatisierten Supply Chain Ökosystemen tätig. Neben der Lehrtätigkeit im Bereich an der FHV und in Schloss Hofen sind seine Forschungsschwerpunkte Informationssicherheit, autonome Systeme sowie digitales Innovationsmanagement.

Interreg Alpenrhein-Bodensee-Hochrhein
Kofinanziert von der Europäischen Union
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra